



Fakultas Hukum
Universitas Djuanda

MODUL

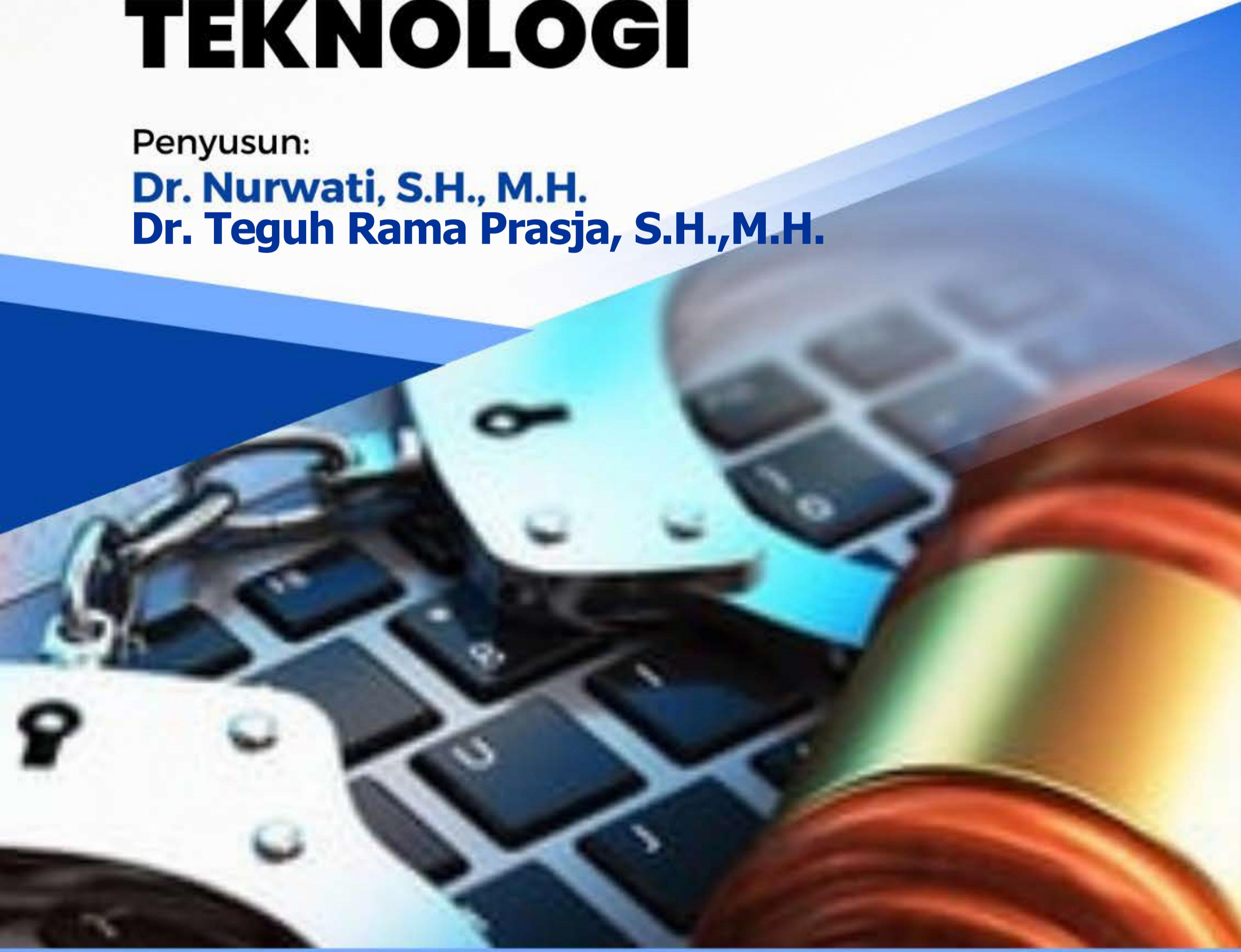
Tahun Akademik
2024/2025

HUKUM INFORMASI DAN TRANSFORMASI TEKNOLOGI

Penyusun:

Dr. Nurwati, S.H., M.H.

Dr. Teguh Rama Prasja, S.H.,M.H.



0852-1994-7320



fh.unida.ac.id



ilmu.hukum@unida.ac.id

KATA PENGANTAR

Segala puji dan syukur ke kehadiran Allah SWT yang telah memberikan rahmat, dan hidayah-Nya, akhirnya Buku “Hukum Transaksi Elektronik di Indonesia (sebagai pedoman dalam menghadapi era digital bisnis *e-commerce* di Indonesia)” dapat diselesaikan.

Perkembangan Transaksi elektronik membawa banyak perubahan terhadap sektor aktivitas bisnis yang selama ini dijalankan di dunia nyata. Perubahan tersebut ditandai dengan adanya sejumlah upaya dari sektor aktivitas bisnis yang semula berbasis di dunia nyata (*real*), kemudian mengembangkannya ke dunia maya (*virtual*).

Penggunaan internet dalam Transaksi elektronik ini memberikan dampak yang sangat positif yakni dalam kecepatan dan kemudahan serta kecanggihan dalam melakukan interaksi global tanpa batasan tempat dan waktu yang kini menjadi hal yang biasa.

Pengaturan di Indonesia diatur dalam Undang-Undang Nomor 11 Tahun 2008, Kemudian direvisi dengan Undang-undang No. 19 Tahun 2016 dan diperbaharui lagi yang ketiga yaitu Undang-undang No.1 Tahun 2024 tentang Informasi dan Transaksi Elektronik atau dapat disingkat UU ITE ini disebut juga oleh banyak kalangan sebagai *cyber law* atau Hukum Siber Indonesia. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai *cyber law* Indonesia dibentuk karena adanya suatu kebutuhan yang mendesak bagi masyarakat, bangsa dan Negara Republik Indonesia saat ini dan di masa datang supaya dapat berdaya saing pada era global atau pasar bebas atau perdagangan bebas dalam lingkup dunia internasional.

Materi muatan dalam modul aja ini memuat pokok-pokok pikiran tentang keterkaitan antara hukum dengan dunia teknologi informasi, dengan beberapa konten pendekatan kasus dari *cyber law* sebagai perkembangan hukum telematika.

Kami mengucapkan terima kasih kepada semua pihak yang telah membantu penulisan modul ajar hukum dan informasi teknologi elektronik ini. Kami menyadari bahwa penulisan modul ajar ini sangat penting untuk khasanah pegangan bagi para mahasiswa di era milenial, untuk itu kami mengharapkan saran serta masukan guna perbaikan dari modul ajar kedepannya.

Bogor, 17 September 2024

Penulis

Dr.Nurwati.,S.H.,M.H

DAFTAR ISI

KATA PENGANTAR	i
DAFTAR ISI	ii
BAB I PENGATURAN HUKUM TERHADAP PERKEMBANGAN TEKNOLOGI INFORMASI DAN TRANSAKSI ELEKTRONIK DI INDONESIA	1
A. Pengaruh Perkembangan Teknologi Terhadap Pembentukan Hukum	1
B. Pengaturan Hukum tentang Transaksi Elektronik	4
C. Urgensi Pengaturan Hukum dalam Transaksi di Internet... ..	13
D. Peristilahan dan Pengertian Informasi Elektronik	22
BAB II KONSEPSI HUKUM TELEMATIKA.....	27
A. Konsepsi Hukum Telematika	27
B. pengertian hukum telematika	31
C. sumber-sumber hukum telematika	37
D. kedudukan hukum telematika dalam Ilmu Hukum.....	37
E. hubungan hukum telematika dengan hukum administrasi negara ..	38
F. hubungan hukum telematika dengan hukum pidana.....	42
G. hubungan hukum telematika dengan hukum tata negara ..	49
H. hubungan hukum telematika dengan hukum perikatan	50
I. hubungan hukum telematika dengan hukum perlindungan konsumen	52
J. Konvergensi Bidang Telematika dengan Undang-Undang Informasi dan Transaksi Elektronik (ITE) di Indonesia	56

BAB III TINDAK PIDANA CYBER CRIME DI INDONESIA	61
A. Pengertian Cyber Crime.....	61
B. Dasar Hukum Cyber Crime.....	64
C. Bentuk-Bentuk Tindak Pidana Cyber Crime.....	71
D. Tindak Pidana Carding	72
1. Pengertian Carding.....	72
2. Dasar Hukum Carding.....	75
3. Penindakan Hukum Pidana terhadap Carding	76
 BAB IV MEKANISME SANKSI DAN PENYELESAIAN SENGKETA TRANSAKSI ELEKTRONIK.....	78
A. Bentuk – bentuk sengketa dalam transaksi elektronik	78
B. Perbuatan yang dilarang dalam UU ITE	80
C. Alternatif Penyelesaian Sengketa (Alternative Dispute Resolution (ADR)	83
D. Online Dispute Resolution (ODR).....	87
 BAB V CYBER CRIME SEBAGAI KEJAHATAN TRANSNASIONAL SERTA PEMBERANTASAN DAN PENANGANAN CYBERCRIME MELALUI PERLUASAN ALAT BUKTI	89
A. Pengertian Kejahatan Transnasional	89
B. Yurisdiksi Suatu Negara dalam Kejahatan Transnasional... ..	90
C. Yurisdiksi Hukum Pidana Indonesia dalam Cyber Crime ..	94
D. Penegakan Hukum Tindak Pidana Cyber Crime.....	96
E. Alat Bukti dalam Sistem Hukum Pembuktian di Indonesia	103
F. Asas-Asas dalam Pembuktian.....	111
G. Alat Bukti Elektronik dalam Cyber Crime	114

BAB VI KAJIAN UMUM TENTANG DATA PRIBADI DAN PERLINDUNGAN HUKUMNYA.....	122
A. Pengertian Data Pribadi	122
B. Dasar Hukum Perlindungan Data Pribadi.....	124
1. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi	124
2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah kedalam Undang-Undang Nomor 19 Tahun 2016 Informasi dan Transaksi Elektronik	124
C. Prinsip Perlindungan Data Pribadi	127
D. Penindakan terhadap Pelanggaran Data Pribadi	129
 BAB VII SISTEM TEKNOLOGI INFORMASI DALAM TRANSAKSI E-COMMERCE	132
A. Syarat sahnya jual beli dalam KUHPerdata	132
B. Keabsahan Kontrak Transaksi Elektronik	138
C. Kontrak Jual Beli Transaksi Elektronik	147
D. Pengaturan UU ITE Terhadap Kontrak Jual Beli e-Commerce.....	170
E. Aspek Pengaturan Penyelenggaraan Sertifikasi Elektronik dan Tanda tangan Elektronik	174
F. Sistem Pembayaran Transaksi Elektronik	187
 DAFTAR PUSTAKA.....	204

BAB I

PENGATURAN HUKUM TERHADAP PERKEMBANGAN TEKNOLOGI INFORMASI DAN TRANSAKSI ELEKTRONIK DI INDONESIA

A. Pengaruh Perkembangan Teknologi Terhadap Pembentukan Hukum

Pada era globalisasi penggunaan media telekomunikasi dan teknologi informasi menempati kedudukan yang penting dalam memudahkan proses transaksi bisnis secara umum dan perdagangan bebas.

Selain itu, Jack Febrian berpendapat¹ Evolusi teknologi telekomunikasi dan teknologi informasi dimulai dari inovasi teknologi sistem informasi yang berbasis pada integrasi antara teknologi komunikasi dengan teknologi komputer, yang disebut *Interconnection Networking* atau disingkat dengan INTERNET, yang dapat diartikan sebagai *global network of computer networks* atau sebuah jaringan komputer dalam skala global dan mendunia. Hadirnya teknologi komputer yang diproduksi untuk konsumsi masyarakat, dan munculnya jaringan internet yang menghubungkan dunia tanpa mengenal batas-batas negara bermaksud untuk mempermudah terpenuhinya segala aktivitas dan kebutuhan manusia di dunia. Inovasi di bidang teknologi informasi diyakini akan membawa keuntungan dan kemudahan dalam berbagai kepentingan yang besar bagi masyarakat dan negara-negara di dunia.

¹ Jack Febrian, *Menggunakan Internet*, Informatika, Bandung 2003, hlm. 3.

Data Perkembangan Internet di Dunia Global

Top 25 Countries, Ranked by Internet Users, 2013-2018 millions						
	2013	2014	2015	2016	2017	2018
1. China*	620.7	643.6	669.8	700.1	736.2	777.0
2. US**	246.0	252.9	259.3	264.9	269.7	274.1
3. India	167.2	215.6	252.3	283.8	313.8	346.3
4. Brazil	99.2	107.7	113.7	119.8	123.3	125.9
5. Japan	100.0	102.1	103.6	104.5	105.0	105.4
6. Indonesia	72.8	83.7	93.4	102.8	112.6	123.0
7. Russia	77.5	82.9	87.3	91.4	94.3	96.6
8. Germany	59.5	61.6	62.2	62.5	62.7	62.7
9. Mexico	53.1	59.4	65.1	70.7	75.7	80.4
10. Nigeria	51.8	57.7	63.2	69.1	76.2	84.3
11. UK**	48.8	50.1	51.3	52.4	53.4	54.3
12. France	48.8	49.7	50.5	51.2	51.9	52.5
13. Philippines	42.3	48.0	53.7	59.1	64.5	69.3
14. Turkey	36.6	41.0	44.7	47.7	50.7	53.5
15. Vietnam	36.6	40.5	44.4	48.2	52.1	55.8
16. South Korea	40.1	40.4	40.6	40.7	40.9	41.0
17. Egypt	34.1	36.0	38.3	40.9	43.9	47.4
18. Italy	34.5	35.8	36.2	37.2	37.5	37.7
19. Spain	30.5	31.6	32.3	33.0	33.5	33.9
20. Canada	27.7	28.3	28.8	29.4	29.9	30.4
21. Argentina	25.0	27.1	29.0	29.8	30.5	31.1
22. Colombia	24.2	26.5	28.6	29.4	30.5	31.3
23. Thailand	22.7	24.3	26.0	27.6	29.1	30.6
24. Poland	22.6	22.9	23.3	23.7	24.0	24.3
25. South Africa	20.1	22.7	25.0	27.2	29.2	30.9
Worldwide*** 2,692.9 2,892.7 3,072.6 3,246.3 3,419.9 3,600.2						

Note: individuals of any age who use the internet from any location via any device at least once per month; *excludes Hong Kong; **forecast from Aug 2014; ***includes countries not listed
Source: eMarketer, Nov 2014

181948 www.eMarketer.com

Sumber:

<http://tekno.kompas.com/read/2014/11/24/07430087/Pengguna.Internet.Indonesia.Nomor.Enam.Dunia.Tahun.2017>

Melalui teknologi informasi, segala kegiatan telekomunikasi memungkinkan untuk dilakukan, tidak terbatas hanya pada suara saja. Hudson, Heather E. juga berpendapat²: Lewat satelit, kejadian monumental di berbagai belahan bumi dapat dilihat dalam waktu yang bersamaan di berbagai tempat. Selain itu, telepon, *facsimile*, dan surat elektronik atau *e-mail* dapat menghubungkan individu, organisasi dan usahawan di seluruh dunia. Sistem telekomunikasi akan melengkapi infrastruktur setiap industri dan perusahaan yang bersaing dalam pasar global. Bisnis telekomunikasi akan berkembang ke arah interkoneksi global.

Perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang, termasuk di Indonesia yang secara langsung telah memengaruhi lahirnya bentuk-bentuk perbuatan hukum baru yang harus diantisipasi oleh pemerintah dengan

² Terperik dalam, *Global Connection: International Telecommunications Infrastructure and Policy*, Thomson Publishing Company, New York, 1997, hlm. 3.

diimbangi pembentukan peraturan perundang- undangan sebagai hukum positif yang harus dilaksanakan dan dipatuhi oleh seluruh lapisan masyarakat.

Penggunaan dan pemanfaatan Teknologi Informasi harus terus dikembangkan untuk menjaga, memelihara, dan memperkuat persatuan dan kesatuan nasional berdasarkan Peraturan Perundang- undangan demi kepentingan nasional. Jika tidak maka negara dan bangsa Indonesia akan tertinggal dari kemajuan ilmu pengetahuan dan teknologi di dunia yang terus berkembang dengan pesat sekali, sehingga negara Indonesia akan selamanya terus menjadi berkembang bahkan bukan tidak mungkin akan menjadi “negara gagal”.

Di abad yang serba maju ini pemanfaatan Teknologi Informasi dan Transaksi Elektrik mutlak harus dilakukan karena sangat berperan penting dalam menunjang dunia perdagangan dan untuk akselerasi pertumbuhan perekonomian nasional guna mewujudkan kesejahteraan masyarakat, karena dengan memanfaatkan teknologi informasi dan transaksi elektrik berarti telah menerapkan ekonomi biaya murah (*low cost economic*).

Perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.³ Misalnya Penipuan, pelanggaran terhadap hak atas kekayaan intelektual, eksplorasi anak-anak atau pornografi, *hecking*,

³ Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia* (Bandung: Refika Aditama, 2004), hlm 1.

pelanggaran terhadap kehidupan pribadi (*privacy*) seseorang, penyebaran virus komputer, dan pencemaran nama baik yang sudah tidak asing lagi di alam maya.

Dalam perspektif masa depan, dunia akan menjadi sebuah perkampungan besar, sehingga batas-batas negara menjadi sangat kabur. Sementara itu, ekonomi global⁴ mengikuti logikanya sendiri. Dalam proses tersebut, terjadi intensifikasi kesadaran terhadap dunia sebagai satu kesatuan utuh. Namun demikian, proses globalisasi yang memungkinkan adanya arus informasi bebas hambatan melalui internet, peningkatan lalu lintas arus barang dan personalia secara internasional serta keanggotaan di dalam berbagai organisasi dunia, secara potensial memunculkan persoalan-persoalan hukum yang berdampak bagi masyarakat, yang mau tidak mau harus ditangani oleh para ahli hukum.⁵ Berbagai permasalahan yang dimunculkan oleh teknologi informasi dan harus dihadapi oleh hukum semestinya telah cukup jelas dan dapat diduga.⁶

B. Pengaturan Hukum tentang Transaksi Elektronik

Undang-Undang Informasi dan Transaksi Elektronik atau dapat disingkat UU ITE ini disebut juga oleh banyak kalangan sebagai *cyber law* atau Hukum Siber Indonesia. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai *cyber law* Indonesia dibentuk karena adanya suatu kebutuhan yang mendesak bagi masyarakat, bangsa dan Negara Republik Indonesia saat ini dan di masa datang

⁴ Samuel P. Huntington, *The Thad Wave: Democratization in the Late Twentieth Century*, Alih bahasa, Asril Marjohan (Jakarta: Midas Surya Grafindo)

⁵ E.K.M. Masinambow, ed., *Hukum dan Kemajemukan Budaya, Sumbangan Karangan Untuk Menyambut Hari Ulang Tahun ke-70 Prof. Dr. T.O. Ihromi* (Jakarta: Yayasan Obor Indonesia, 2000), hlm 3.

⁶ David Bainbridge, *Introduction to Computer Law*, 3rd Edition (London: Pitman Publishing, 1996), hlm 1.

supaya dapat berdaya saing pada era global atau pasar bebas atau perdagangan bebas dalam lingkup dunia internasional.

Lebih lanjut mengenai dasar pertimbangan terbentuknya Undang- Undang tentang Informasi dan Transaksi Elektronik (ITE) dapat ditemukan dalam bagian konsideransnya, khususnya pada bagian “Menimbang” yang menyatakan sebagai berikut:

1. Bahwa pembangunan nasional adalah suatu proses yang berkelanjutan yang harus senantiasa tanggap terhadap berbagai dinamika yang terjadi di masyarakat;
2. Bahwa globalisasi informasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia sehingga mengharuskan dibentuknya pengaturan mengenai pengelolaan Informasi dan Transaksi Elektronik di tingkat nasional sehingga pembangunan Teknologi Informasi dapat dilakukan secara optimal, merata, dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa;
3. Bahwa perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah mempengaruhi lahirnya bentuk-bentuk perbuatan hukum baru;
4. Bahwa penggunaan dan pemanfaatan Teknologi Informasi harus terus dikembangkan untuk menjaga, memelihara, dan memperkokoh persatuan dan kesatuan nasional berdasarkan peraturan perundang- undangan demi kepentingan nasional;
5. Bahwa pemanfaatan Teknologi Informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat;

6. Bahwa pemerintah perlu mendukung pengembangan Teknologi Informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan Teknologi Informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia⁷.

Selanjutnya, dalam Penjelasan umum Undang-Undang Nomor 1 Tahun 2014 atas perubahan kedua Undang-undang 11 Tahun 2008 (UU ITE) dijelaskan, bahwa pemanfaatan teknologi informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi Informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi teknologi yang sangat rawan dalam mengakomodasi perbuatan kriminal dan perbuatan melawan hukum yang dilakukan oleh orang-orang yang menguasai teknologi informasi.

Selanjutnya dalam alinea berikutnya dijelaskan bahwa telah lahir suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika. Hukum siber atau *cyber law*, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum

⁷ Anonymous, terpetik dalam bagian “Konsideran Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik”, Kesindo Utama, Surabaya, 2008, hlm. 1.

telekomunikasi, hukum media, dan hukum informatika. Istilah lain yang juga digunakan adalah hukum teknologi informasi (*law of information technology*), hukum dunia maya (*virtual world law*) dan hukum mayantara. Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global (internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual. Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.⁸

Sehubungan dengan itu, dunia hukum sebenarnya sudah sejak lama telah memperluas penafsiran asas dan normanya ketika menghadapi persoalan kebendaan yang tidak berwujud, misalnya dalam kasus pencurian listrik sebagai perbuatan pidana. Dalam kenyataan kegiatan siber tidak lagi sederhana karena kegiatannya tidak lagi dibatasi oleh teritorial suatu negara, yang mudah diakses kapan saja dan dari mana saja. Kerugian dapat terjadi baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi, misalnya pencurian dana kartu kredit melalui pembelanjaan di internet. Di samping itu, pembuktian merupakan faktor yang sangat penting, mengingat informasi elektronik bukan saja belum terakomodasi dalam sistem hukum acara Indonesia secara komprehensif, melainkan juga ternyata sangat rentan untuk diubah, disadap, dipalsukan, dan dikirim ke berbagai penjuru dunia dalam

⁸ Penjelasan Umum UU No. 1/2024 (UUITE).

waktu hitungan detik. Dengan demikian, dampak yang diakibatkannya pun bisa demikian kompleks dan rumit.

Permasalahan yang lebih luas terjadi pada bidang keperdataan karena transaksi elektronik untuk kegiatan perdagangan melalui sistem elektronik (*electronic commerce*) telah menjadi bagian dari perniagaan nasional dan internasional. Kenyataan ini menunjukkan bahwa konvergensi di bidang teknologi informasi, media, dan informatika (*telematika*) berkembang terus tanpa dapat dibendung, seiring dengan ditemukannya perkembangan baru di bidang teknologi informasi, media, dan komunikasi. Kegiatan melalui media sistem elektronik, yang disebut juga ruang siber (*cyber space*), meskipun bersifat virtual dapat dikategorikan sebagai tindakan atau perbuatan hukum yang nyata.

Berkaitan dengan hal itu, perlu diperhatikan sisi keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, komunikasi agar dapat berkembang secara optimal. Oleh karena itu, terdapat tiga pendekatan untuk menjaga keamanan pada ranah hukum siber (*cyberlaw space*), yaitu pendekatan aspek hukum, aspek sosial, budaya, dan etika. Untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal.

Setelah mencermati penjelasan UU ITE seperti yang dikemukakan di atas, khususnya alinea terakhir; dapat disimpulkan bahwa pemikiran yang dituangkan dalam penjelasan tersebut merupakan suatu gagasan dasar yang melandasi terbentuknya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Oleh karena itu UU ITE yang berlaku saat ini, di samping berfungsi sebagai suatu pendekatan terhadap perkembangan telekomunikasi, teknologi

informasi dan transaksi elektronik, tetapi yang paling penting adalah berfungsi dan bertujuan sebagai sarana tolok ukur yang dapat menjamin perlindungan hukum, kepastian hukum dan keadilan bagi para pihak, baik perseorangan, pengguna, masyarakat, lembaga-lembaga non pemerintah, pelaku bisnis, penyelenggara, instansi pemerintah dalam penyelenggaraan informasi dan transaksi elektronik.

Sehubungan dengan itu, dalam upaya untuk tetap menjamin konsistensi dari penguraian materi muatan UU ITE, maka terlebih dahulu dipaparkan mengenai sistematika UU ITE yaitu sebagai berikut; Bab I Ketentuan Pendahuluan (Pasal 1 dan Pasal); Bab II Asas dan Tujuan (Pasal 3 dan Pasal 4); Bab III Informasi Dokumen dan Tanda Tangan Elektronik (Pasal 5-Pasal 12); Bab IV Penyelenggaraan Sertifikasi Elektronik dan Sistem Elektronik, yaitu Bagian Kesatu: Penyelenggaraan Sertifikasi Elektronik (Pasal 13- Pasal 114); Bagian Kedua: Penyelenggaraan Sistem Elektronik, (Pasal 15-Pasal 16); Bab V Transaksi Elektronik, (Pasal 17- Pasal 22); Bab VI Nama Domain, Hak Kekayaan Intelektual dan Perlindungan Hak Pribadi, (Pasal 23-Pasal 26); Bab VII Perbuatan Yang Dilarang, (Pasal 27- Pasal 37); Bab VIII Penyelesaian Sengketa, (Pasal 38-Pasal 39); Bab IX Peran Pemerintah dan Peran Masyarakat, (Pasal 40-Pasal 41); Bab X Penyidikan (Pasal 42-Pasal 44); Bab XI Ketentuan Pidana (Pasal 45-Pasal 52); Bab XII Ketentuan Peralihan (Pasal 53); Bab XIII Ketentuan Penutup (Pasal 54).

Berdasarkan pada sistematika di atas, maka dalam uraian selanjutnya akan dibagi atas beberapa materi bahasan yaitu sebagai berikut;

1. Beberapa Peristilahan/Pengertian dan Ruang Lingkup Serta Asas dan Tujuan.
2. Beberapa Ketentuan Material Dalam UU ITE.

3. Beberapa Ketentuan Hukum Formal Dalam UU ITE

Pada tahun 2016 disahkan perubahan terhadap UU ITE Tahun 2011, menjadi UU Nomor 19 Tahun 2016 tentang Perubahan Atas UU ITE Nomor 11 Tahun 2008. Naskah Undang-Undang tersebut tercatat dalam Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251 dan Tambahan Lembaran Negara Nomor 5952. UU ITE perubahan ini berisi tujuh poin penting yang merevisi UU ITE, terutama melalui UU baru ini Pemerintah juga berwenang memutus akses dan/atau memerintahkan penyelenggara sistem elektronik untuk memutus akses terhadap informasi elektronik yang bermuatan melanggar hukum. UU baru ini diharapkan dapat memberikan kepastian hukum bagi masyarakat, sehingga mereka dapat lebih cerdas dan beretika dalam menggunakan Internet. Dengan demikian konten berunsur SARA, radikalisme, dan pornografi dapat diminimalisir.

Awalnya UU ITE disusun untuk mendukung pertumbuhan ekonomi di Indonesia melalui ekonomi digital dan perdagangan di dunia maya (*ecommerce*) di Indonesia. Kemudian di tengah perjalanan terjadi banyak polemik dan kasus yang menimbulkan pro kontra terhadap pasal-pasal di UU ITE, terutama terkait dengan penggunaan media sosial. Pasal-pasal tersebut dianggap mengancam kebebasan berekspresi pengguna Internet.

Ada beberapa perubahan di UU ITE yang baru yaitu sebagai berikut:

1. Untuk menghindari multitafsir terhadap ketentuan larangan mendistribusikan, mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik bermuatan penghinaan dan/atau pencemaran nama baik pada ketentuan Pasal 27 ayat (3), dilakukan 3 (tiga) perubahan sebagai berikut:

- a. Menambahkan penjelasan atas istilah “mendistribusikan, mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik”. - Yang dimaksud dengan “mendistribusikan” adalah mengirimkan dan/atau menyebarkan Informasi Elektronik dan/atau Dokumen Eletronik kepada banyak orang atau berbagai pihak melalui Sistem Elektronik. - Yang dimaksud dengan “mentransmisikan” adalah mengirimkan Informasi Elektronik dan/atau Dokumen Eletronik yang ditujukan kepada satu pihak lain melalui Sistem Elektronik. - Yang dimaksud dengan “membuat dapat diakses” adalah semua perbuatan lain selain mendistribusikan dan mentransmisikan melalui Sistem Elektronik yang menyebabkan Informasi Elektronik dan/atau Dokumen Elektronik dapat diketahui pihak lain atau publik.
 - b. Menegaskan bahwa ketentuan tersebut adalah delik aduan bukan delik umum.
 - c. Menegaskan bahwa unsur pidana pada ketentuan tersebut mengacu pada ketentuan pencemaran nama baik dan fitnah yang diatur dalam KUHP.
2. Menurunkan ancaman pidana pada 2 (dua) ketentuan pada Pasal 29 sebagai berikut:
 - a. Ancaman pidana penghinaan dan/atau pencemaran nama baik diturunkan dari pidana penjara paling lama 6 (enam) tahun menjadi paling lama 4 (tahun) dan/atau denda dari paling banyak Rp 1 miliar menjadi paling banyak Rp 750 juta.
 - b. Ancaman pidana pengiriman informasi elektronik berisi ancaman kekerasan atau menakut-nakuti dari pidana

penjara paling lama 12 (dua belas) tahun menjadi paling lama 4 (empat) tahun dan/ atau denda dari paling banyak Rp 2 miliar menjadi paling banyak Rp 750 juta.

3. Melaksanakan putusan Mahkamah Konstitusi terhadap 2 (dua) ketentuan sebagai berikut:
 - a. Mengubah ketentuan Pasal 31 ayat (4) yang semula mengamanatkan pengaturan tata cara intersepsi atau penyadapan dalam Peraturan Pemerintah menjadi dalam Undang-Undang.
 - b. Menambahkan penjelasan pada ketentuan Pasal 5 ayat (1) dan ayat (2) mengenai keberadaan Informasi Elektronik dan/atau Dokumen Elektronik sebagai alat bukti hukum yang sah.
4. Melakukan sinkronisasi ketentuan hukum acara pada Pasal 43 ayat (5) dan ayat (6) dengan ketentuan hukum acara pada KUHAP, sebagai berikut:
 - a. Penggeledahan dan/atau penyitaan yang semula harus mendapatkan izin Ketua Pengadilan Negeri setempat, disesuaikan kembali dengan ketentuan KUHAP.
 - b. Penangkapan penahanan yang semula harus meminta penetapan Ketua Pengadilan Negeri setempat dalam waktu 1×24 jam, disesuaikan kembali dengan ketentuan KUHAP.
5. Memperkuat peran Penyidik Pegawai Negeri Sipil (PPNS) dalam UU ITE pada ketentuan Pasal 43 ayat (5):
 - a. Kewenangan membatasi atau memutuskan akses terkait dengan tindak pidana teknologi informasi;

- b. Kewenangan meminta informasi dari Penyelenggara Sistem Elektronik terkait tindak pidana teknologi informasi.
6. Menambahkan ketentuan mengenai "*right to be forgotten*" atau "hak untuk dilupakan" pada ketentuan Pasal 26, sebagai berikut:
 - a. Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan.
 - b. Setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan Informasi Elektronik yang sudah tidak relevan. (Menambahkan ketentuan atau kewajiban menghapus konten yang tidak relevan bagi penyelenggara sistem elektronik sebagai jaminan pemenuhan atas perlindungan data pribadi. Pelaksanaan ketentuan ini dilakukan atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan).
7. Memperkuat peran Pemerintah dalam memberikan perlindungan dari segala jenis gangguan akibat penyalahgunaan informasi dan transaksi elektronik (Memberikan landasan yang kuat bagi pemerintah untuk mencegah penyebarluasan konten negatif di internet) dengan menyisipkan kewenangan tambahan pada ketentuan Pasal 40:
 - a. Pemerintah wajib melakukan pencegahan penyebarluasan Informasi Elektronik yang memiliki muatan yang dilarang;
 - b. Pemerintah berwenang melakukan pemutusan akses dan/atau memerintahkan kepada Penyelenggara Sistem Elektronik untuk melakukan pemutusan akses terhadap

Informasi Elektronik yang memiliki muatan yang melanggar hukum.

C. Urgensi Pengaturan Hukum dalam Transaksi di Internet

Dengan demikian teknologi yang diciptakan oleh manusia tidak selalu menghasilkan hal-hal yang positif tetapi dapat juga menghasilkan berbagai dampak negatif. Disinilah salah satu arti penting perlunya peraturan perundang-undangan dibidang teknologi informasi.

Banyak pihak yang mengatakan bahwa hukum selalu tertinggal dengan teknologi. Kritikan tersebut tidak terlalu salah. Memang demikianlah sifat dari hukum apabila dikaitkan dengan teknologi. Hukum tidak mungkin berada didepan perkembangan teknologi informasi. Tidak mungkin orang memprediksikan teknologi apa yang akan diketemukan dimasa depan kemudian mengurnya dalam suatu produk hukum. Hukum sudah sewajarnya berada dibelakang mengikuti perkembangan teknologi. Apabila hukum berada didepan maka teknologi tidak dapat berkembang secara leluasa. Hal terpenting untuk diperhatikan adalah berapa lama waktu yang dibutuhkan untuk pada akhirnya hukum terbentuk setelah muncul yang dibutuhkan untuk pada akhirnya hukum terbentuk setelah muncul teknologi baru. Cepat lambatnya pembentukan hukum akan berpengaruh pada kestabilan masyarakat, kedamaian dan ketertiban yang hendak dituju oleh hukum dengan adanya perkembangan teknologi baru. Pembentukan hukum yang dapat diselesaikan karena tidak ada hukum yang mengatur.

Dalam era globalisasi, tak dapat dipungkiri bahwa penggunaan telekomunikasi dan teknologi informasi yang

semakin terpadu (*global communication network*) dengan semakin populernya Internet seakan- akan telah membuat dunia semakin mencuat (*shrinking the world*) dan semakin memudarkan batas-batas negara berikut kedaulatan dan tatanan masyarakatnya. Ironisnya, dinamika masyarakat Indonesia yang masih baru tumbuh dan berkembang sebagai masyarakat industri dan masyarakat Informasi, seolah masih tampak prematur untuk mengiringi perkembangan teknologi tersebut. Adanya internet hal ini sangat berpengaruh besar (juga bagi masyarakat Indonesia) sebagai suatu negara berkembang, yang langsung tidak langsung berpengaruh bagi kehidupan nyata manusia itu sendiri.

Dalam pada itu, tentunya akan mempengaruhi berkembangnya pemahaman manusia terhadap pengertian *cyber space* yang tidak lain ada dalam komunikasi melalui jaringan Internet sering disebut sebagai "*a network of net works*", maka dari karakteristik ini kemudian ada yang menyebut *cyber space* dengan istilah *virtual-community* atau *virtual-world*. Dalam pada itu, netter bernganggapan seolah-olah sudah tidak ada lagi kekuasaan hukum yang mengendalikan aktivitas manusia atau pelaku dunia usaha. Sebab tidak ada kedaulatan dalam jaringan komputer yang maha besar (*gigantic network*), delain telekomunikasi dan teknologi informasi. Para netter beranggapan bahwa tidak ada satu pun hukum suatu negara yang berlaku, karena hukum network tumbuh dari kalangan mayarakat global penggunanya.

Era baru yang menglobal seakan-akan menjadi jawaban dari impian untuk melampiaskan kebebasan berkomunikasi (*free flow of information*) dan kebebasan mengemukakan pendapat (*freedom of speech*), tanpa perlu mengindahkan norma yang berlaku sebagaimana dalam kehidupan di dunia nyata.

Dalam perkembangan teknologi informasi, suatu hal yang harus disadari secara cermat dengan pikiran dan iman yang teguh bahwa setinggi dan secanggih apa pun perkembangan telekomunikasi dan teknologi informasi, maka harus tetap memperhatikan rambu-rambu dan prinsip-prinsip universal dalam kehidupan manusia, bermasyarakat, berbangsa dan bernegara. Prinsip-prinsip tersebut yaitu antara lain; kepentingan umum, ketentuan peraturan perundang-undangan yang berlaku, hak asasi manusia orang lain, agama, kesusilaan, dan kesopanan.

Dalam pandangan Hamad Steven, Internet merupakan *big bang* kedua setelah *big bang* pertama yaitu *material big bang* menurut versi Stephen Hawking – yang merupakan *knowledge big bang* dan ditandai dengan komunikasi elektromagentoopis via satelit maupun kabel, didukung oleh eksistensi jaringan teleponi yang telah ada dan akan segera didukung oleh ratusan satelit yang sedang dan akan diluncurkan.⁹

Internet merupakan simbol material embrio masyarakat global di era perkembangan teknologi informasi saat ini yang semakin pesat. Era informasi ditandai dengan aksesibilitas informasi yang amat tinggi. Dalam era global, informasi merupakan komoditi utama yang diperjualbelikan sehingga akan muncul berbagai *network & information company* yang akan memperjualbelikan berbagai fasilitas bermacam jaringan dan berbagai basis data informasi tentang berbagai hal yang dapat diakses oleh pengguna dan pelanggan. Bidang-bidangnya pun kian meluas. Misalnya di bidang transportasi, perindustrian dan

⁹ Harnad, Steven, *Post-Gutenberg Galaxy: The Fourth Revolution in the Means of Production of Knowledge*, Public-Access Computer System Review 2 (1): 39-53, versi elektronik dapat dibaca pada <http://cogprints.org/1580/00/> harnad91.postgutenberg.html

bidang-bidang lainnya yang termasuk vital, semua itu membawa masyarakat ke dalam suasana yang disebut sebagai *Zona Mabuk Teknologi*.¹⁰

Istilah teknologi informasi (TI), telematika, multimedia ataupun *information & communication technologies* (ICT) tidak jauh berbeda maknanya, namun sebagai suatu definisi sangat tergantung kepada lingkup dan sudut pandang pengkajiannya. Dengan semakin populernya internet sebagai *the network of the networks*, masyarakat penggunanya (*internet global community*) seakan-akan mendapati suatu dunia baru yang dinamakan *cyberspace*. Istilah *cyberspace* pertama kali diperkenalkan oleh William Gibson seorang penulis fiksi ilmiah (*science fiction*) dalam novel yang berjudul *Neuromancer*¹¹, istilah yang sama kemudian diulangi dalam novelnya yang lain berjudul *Virtual Light*.¹²

Pola dinamika masyarakat Indonesia seakan masih bergerak tak beraturan ditenga keinginan untuk mereformasi semua bidang kehidupannya ketimbang suatu pemikiran yang handal untuk merumuskan suatu kebijakan ataupun pengaturan yang tepat untuk itu. Meskipun masyarakat telah banyak menggunakan produk-produk teknologi informasi dan jasa telekomunikasi dalam kehidupannya, namun bangsa Indonesia secara garis besar masih

¹⁰ Naisbitt, John; Nasibitt, Nana; dan Douglas Philips, *High Tech, High Touch, Pencarian Makna di Tengah Perkembangan Pesat Teknologi*, Bandung: Mizan, Bandung, 2001, hlm. 14.

¹¹ Atip Latipulhayat, "Cyber Law Dan Urgensinya Bagi Indonesia", Makalah disampaikan pada Seminar, yang diselenggarakan oleh Yayasan Cipta Bangsa di Bandung pada tanggal 29 Juli 2000, Bandung, 2000, hlm. 5.

¹² William Gibson: *cyberspace....was a consensual hallucination that felt and looked like a physical space but actually was a computer generated construct representing abstract data*", yang menghayalkan adanya alam lain pada saat teknologi telekomunikasi dan informatika bertemu. Pun menurut Menurut Cavazos dan Morin yang menyatakan: "...represents a vast array of computer systems accessible from remote physical locations".

meraba-raba dalam mencari suatu kebijakan publik dalam membangun suatu infrastruktur yang handal (*National Information Infrastructure*) dalam menghadapi infrastruktur informasi global (*Global Information Infrastructure*).

Dunia hukum sebenarnya sudah sejak lama memperluas penafsiran asas dan normanya ketika menghadapi persoalan yang bersifat tidak berwujud, misalnya dalam kasus pencurian listrik yang pada awalnya sulit dikategorikan sebagai delik pencurian tetapi akhirnya dapat diterima sebagai perbuatan pidana. Kenyataan saat ini yang berkaitan dengan kegiatan siber tidak lagi sesederhana itu, mengingat kegiatannya tidak lagi bisa dibatasi oleh teritori suatu negara, aksesnya dengan mudah dapat dilakukan dari belahan dunia manapun, kerugian dapat terjadi baik pada pelaku internet maupun orang lain yang tidak pernah berhubungan sekalipun misalnya dalam pencurian dana kartu kredit melalui pembelanjaan di internet.

Bidang-bidang yang menggunakan peralatan komputer erat kaitannya dengan data, maka hal ini tersangkut paut dengan kepentingan integritas (data harus dipercaya), kerahasiaan (data yang dimaksudkan untuk tidak diketahui oleh umum), eksklusivitas (kemungkinan untuk menolak orang yang berminat menggunakan data tanpa imbalan), dan keharusan selalu siap tersedia data-data komputer (data harus senantiasa dapat dicapai oleh pemakai komputer).¹³ Tindak pidana yang berkaitan dengan komputer adalah salah satu kejahatan modern yaitu kejahatan yang dilakukan oleh para intelektual dan para pelaku kejahatan dalam lingkup “*white collar crime*”.

¹³ Karlinah P. A. Soebroto, *Kejahatan Komputer dalam Perbankan, Temu Karya Ilmiah Tindak Pidana Perbankan*, Majalah Hukum Varia Peradilan, Mei 1991, hlm. 82-83.

Kejahatan tersebut tidak dilakukan dengan kekerasan atau menggunakan sarana yang rumit, misalnya bom atau nuklir tetapi hanya menggunakan perangkat telekomunikasi dan teknologi informasi berupa komputer. Melalui komputer dapat memproses jutaan data setiap detiknya dan juga dapat pula digunakan untuk merusak data informasi yang berakibat timbulnya kerugian yang besar atau dapat menimbulkan bahaya bagi keamanan masyarakat atau negara.

Tindak pidana tersebut dapat menimbulnya kerugian finansial dalam jumlah yang sangat besar sebagai akibat langsung dari penggunaan sarana atau perangkat telekomunikasi dan teknologi informasi yang tidak bertanggungjawab dan terkadang sulit dilacak keberadaannya. Para *netter* beranggapan bahwa aspek kerugian yang potensial ini sebagai ciri yang paling penting dalam tindak pidana ini, misalnya dalam kegiatan lalu lintas keuangan dalam dunia perbankan, rahasia dan keamanan negara serta di bidang-bidang vital lainnya. Di samping kerugian finansial, ada kepentingan lain yang perlu mendapat pengamanan, misalnya data pribadi warga, data ilmu pengetahuan, data keamanan negara dan rahasia yang menyangkut administrasi Pemerintah dan dokumen-dokumen penting.

Sehubungan dengan tindak pidana ini adalah bahwa perbuatan tersebut dapat dilakukan dengan cepat dan otomatis, perbuatan dilakukan tanpa campur tangan manusia dan dapat diulang-ulang secara tanpa batas, tidak kelihatan dan semua berkas dapat dihapus secara otomatis, dapat pula dilakukan melampaui geografis karena penggunaan telekomunikasi dan informatika dan perbuatan tersebut merupakan ancaman bagi

perusahaan- perusahaan, organisasi-organisasi, dan lembaga yang merupakan tonggak dari masyarakat modern.¹⁴

Terdapat tiga pendekatan untuk mempertahankan keamanan di *cyberspace*¹⁵: *pertama* adalah pendekatan teknologi; *kedua*, adalah pendekatan sosial budaya-etika; dan *ketiga*, adalah pendekatan hukum. Dalam kaitannya dengan penentuan hukum yang berlaku dikenal beberapa asas yang biasa digunakan, yaitu:

1. *Subjective territoriality*, yang menekankan bahwa keberlakuan hukum ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan dinegara lain.
2. *Objective territoriality*, yang menyatakan bahwa hukum yang berlaku adalah hukum dimana akibat utama perbuatan itu terjadi dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan.
3. *Nationality*, yang menentukan bahwa negara mempunyai jurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku.
4. *Passive Nationality*, yang menekankan jurisdiksi berdasarkan kewarganegaraan korban.
5. *Protective Principle*, yang menyatakan berlakunya hukum didasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahanan yang dilakukan di luar wilayahnya, yang umumnya digunakan apabila korban adalah negara atau pemerintah.
6. *Universality*, asas ini disebut juga sebagai “*universal interest jurisdiction*”. Asas ini menentukan bahwa setiap negara

¹⁴ Ny. Karlinah P.A. Soebroto, *Kejahatan Komputer dalam Perbankan, Temu Karya Ilmiah Tindak Pidana Perbankan*, Majalah Hukum Varia Peradilan, Mei 1991, hal.

¹⁵ Ahmad M. Ramli, *Cyber Law ...*, Op. cit., hlm. 4-6.

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 dimasa mendatang asas yurisdiksi universal ini mungkin dikembangkan untuk *internet piracy*, seperti *computer, cracking, carding, hacking*, dan, namun perlu dipertimbangkan bahwa penggunaan asas ini hanya diberlakukan untuk kejahatan sangat serius berdasarkan pada perkembangan dalam hukum internasional.

Berdasarkan karakteristik yang disebutkan diatas, maka dapat dikemukakan beberapa teori sebagai berikut¹⁶: Pertama, *The theory of the uploader and the downloader*. Berdasar teori ini, suatu negara dapat melarang dalam wilayahnya, kegiatan *uploading* dan *downloading* yang diperkirakan dapat bertentangan dengan kepentingannya. Misalnya, suatu negara dapat melarang setiap orang untuk *uploading* kegiatan perjudian atau kegiatan perusakan lainnya dalam wilayah negara, dan melarang setiap orang dalam setiap wilayahnya untuk *downloading* kegiatan perjudian tersebut. Minnesota adalah salah satu negara bagian pertama yang menggunakan jurisdiksi ini.

Kedua, teori *The Law of the server*. Pendekatan ini memperlakukan *server* dimana *webpages* secara fisik berlokasi, yaitu dimana mereka dicatat sebagai data elektronik. Menurut teori ini sebuah *webpages* yang berlokasi di *server* pada *Stanford University*

¹⁶ Anonymous, *Pendekatan Hukum untuk Keamanan Dunia Cyber serta Urgensi Cyberlaw bagi Indonesia*, Makalah mahasiswa teknologi informasi, Teknik Komputer, Universitas Indonesia, 2005.

tunduk pada hukum California. Namun teori ini akan sulit digunakan apabila *uploader* berada dalam jurisdiksi asing.

Ketiga, *The Theory of International Spaces*. Ruang *cyber* dianggap sebagai *the fourth spaces*. Yang menjadi analogi adalah tidak terletak pada keamanan fisik, melainkan pada sifat internasional, yakni *sovereignless quality*.

Berdasarkan karakteristik khusus yang terdapat dalam ruang *cyber* di mana pengaturan dan penegakan hukumnya tidak dapat menggunakan cara-cara tradisional, beberapa ahli berpandangan bahwa sebaiknya memang kegiatan dalam *cyberspace* diatur oleh hukum sendiri. Oleh karena itu, untuk ruang *cyber* dibutuhkan hukum baru yang menggunakan pendekatan yang berbeda dengan hukum yang dibuat berdasarkan batas-batas wilayah. Ruang *cyber* diibaratkan sebagai suatu tempat yang hanya dibatasi oleh *screens* dan *passwords*. Secara radikal, ruang *cyber* telah mengubah hubungan antara *legally significant (online) phenomena* dan *physical location*.

Respon hukum terhadap teknologi informasi telah menjadi kebutuhan dan tuntutan yang mendesak. Ketertinggalan Indonesia dalam hal pengembangan perangkat hukum di bidang teknologi informasi, yang diukur dari belum adanya hukum yang mengatur tentang teknologi informasi ini menyebabkan keyakinan masyarakat bahwa bagi para pengguna teknologi informasi berlaku hukum rimba. Persepsi demikian timbul karena adanya kevakuman dan ketidak pastian hukum dalam tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843)

D. Peristilahan dan Pengertian Informasi Elektronik

Istilah informasi elektronik pada dasarnya dibentuk dari dua kata yaitu kata informasi dan kata elektronik. Istilah informasi dalam bahasa Inggris yaitu *information*. Menurut Shanon dan Weaver sebagaimana terpetik dalam Edmon Makarim mengemukakan *Information* adalah *the amount of uncertainty that is reduced when a received*¹⁷. Lalu Gordon B. Davis mendefenisikannya sebagai: *Information is data that has been processed into a form that is meaningful to the recipient and is used of real or perceived value in current or prospective action or decision*¹⁸.

Bertumpu pada peristilahan dan pandangan di atas dapat dikemukakan bahwa informasi adalah suatu data atau keterangan dan pesan yang diterima atau diperoleh tentang segala sesuatu baik menyangkut data pribadi seseorang, keluarga, masyarakat maupun suatu lembaga tertentu baik yang disampaikan secara lisan maupun tertulis atau tersimpan dalam suatu dokumen tertentu yang telah ditata, diolah dan diproses secara sistematik serta disimpan secara nyaman dan dijamin kerahasiaannya sebagai dasar dalam pengambilan suatu tindakan atau keputusan.

Secara yuridis istilah atau pengertian informasi elektronik telah diatur dalam Pasal 1 butir 1 yang secara tegas ditentukan bahwa informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, Kode akses, simbol atau perforasi yang telah diolah yang

¹⁷ Edmon Makarim, *Kompilasi Hukum ...*, Op. cit., hlm. 29.

¹⁸ Ibid., hlm. 29

memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Lalu dalam Pasal 1 butir 2 ditentukan juga bahwa transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya, (Pasal 1 butir 2). Lalu, teknologi informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, manganalisis, dan/ atau menyebarkan informasi. Demikian pula dalam Pasal 1 butir 17 ditentukan bahwa kontrak elektronik adalah perjanjian para pihak yang dibuat melalui sistem elektronik.

Atas dasar ketentuan Pasal 1 butir 1, 2 dan 17 tersebut dapat diketahui bahwa ruang lingkup materi yang diatur dalam UU ITE adalah sangat luas dan saling terkait dengan bidang hukum yang lainnya, misalnya hukum telekomunikasi, hukum penyiaran, hukum kontrak/perjanjian, hukum administrasi, hukum bisnis/ perdagangan, hukum perdata, dan hukum pidana, baik secara nasional maupun dalam lingkup dunia internasional, serta berbagai peraturan perundang-undangan lainnya.

Pengertian lain yang terkait erat dengan transaksi *e-commerce* ini adalah:

1. Internet berasal dari kata *Interconnection Networking*. Artinya hubungan berbagai komputer dengan berbagai tipe yang membentuk sistem jaringan mencakup seruruh dunia (jaringan komputer global) dengan memalui jalur telekomunikasi seperti kabel telepon dan satelit.
2. E-Mail adalah pengiriman surat melalui media elektronik misalnya melalui media komputer.

3. *World wide web* adalah jaringan luas (jaringan yang dimiliki oleh setiap perusahaan yang melayani jasa internet).
4. *Cardholder* adalah orang yang menggunakan kartu pembayaran yang dikeluarkan oleh sebuah *issuer*. Dalam sistem pembayaran SET, informasi nomor rekening yang dikirimkan *cardholder* dijamin kerahasiaannya.
5. *Issuer* adalah suatu institusi ekonomi (bank) yang membuat rekening dan mengeluarkan kartu pembayaran bagi *cardholder*. *Issuer* menjamin pembayaran untuk transaksi yang terotorisasi menggunakan kartu pembayaran yang dikeluarkannya, sesuai dengan regulasi yang dikeluarkan oleh pemegang merek dan pemerintah setempat. Contoh *issuer* adalah bank-bank yang mengeluarkan kartu kredit seperti Bank BCA, Bank Bali, Bank Lippo, BII dsb.
6. *Merchant* adalah orang yang menyediakan barang atau jasa untuk dipertukarkan dengan pembayaran, dalam hal ini pembayaran dilakukan melalui internet. Dalam SET, *merchant* dapat menyediakan transaksi yang aman bagi *cardholder*. *Merchant* terlebih dahulu harus memiliki relasi dengan *acquirer*.
7. *Acquirer* adalah suatu institusi ekonomi yang membuat rekening bagi *merchant* dan melakukan proses otorisasi kartu pembayaran yang diterima oleh *merchant* dari *cardholder*. Contoh *acquirer* adalah bank-bank yang menyediakan layanan otorisasi bagi toko-toko yang menerima pembayaran dengan kartu kredit seperti Bank BCA, Bank Bali, City Bank, BII dsb.
8. *Payment gateway* adalah suatu pihak ketiga yang merupakan perangkat yang dioperasikan oleh *acquirer* atau pihak ketiga untuk memproses pesan pembayaran termasuk instruksi pembayaran dari *cardholder*.

9. Pemegang merek adalah suatu badan usaha yang mengembangkan sistem kartu pembayaran, yang melindungi, mempromosikan dan menciptakan aturan-aturan penggunaannya. Ada beberapa pemegang merek yang merupakan institusi ekonomi dan berperan sebagai *issuer* maupun *acquirer*. Contoh pemegang merek yaitu Visa, Master Card, Amex, dsb.
10. Pihak Ketiga Terkadang *acquirer* maupun *issuer* memilih pihak ketiga untuk menjalankan *payment gateway*.
11. Web Site (Situs web), merupakan tempat penyimpanan data dan informasi dengan topik tertentu.
12. Web adalah fasilitas hipertaks untuk menampilkan data berupa taks, gambar, suara, animasi dan multimedia lainnya. Di antara data tersebut saling berhubungan satu sama lain. Untuk membaca data dan informasi pada web dapat menggunakan *web browser microsoft internet exploler atau netscape communicator*.
13. Web Server merupakan komputer yang selalu hidup 24 jam di internet yang berfungsi untuk mengolah sb page atau devisi lain adalah server penyedia web di internet.
14. *Browser*, merupakan program aplikasi yang digunakan untuk memudahkan melakukan navigasi (penelusuran) berbagai data dan informasi pada www. Browser yang terkenal adalah internet explorer dan netscape navigator.
15. URL (*Universal Resource Locator*), adalah alamat absolut suatu web di internet. Meskipun koneksinya berbeda sering diartikan sama dengan alamat web site.
16. HTTP (*Hypertext transfer protocol*), merupakan suatu teknologi format protokol yang berfungsi menampilkan dan mengelola halamat web di dalam web server.

BAB II

KONSEPSI HUKUM TELEMATIKA

A. Konsepsi Hukum Telematika

Pada mulanya, istilah Telematika dikenal dalam bahasa Perancis yaitu *Telematique*, yang kemudian berkembang menjadi istilah umum di Eropa. Selanjutnya, Telematika diartikan untuk memperlihatkan pertemuan jaringan komunikasi dengan teknologi informasi. Perkembangan makna telematics menjadi singkatan dari “Telecommunications and Informatics”, yang merupakan perpaduan konsep Computing and Communication. Dewasa ini, istilah Telematika memperlihatkan konvergensi antara Telekomunikasi, Media dan Informatika. Konvergensi pada telematika merupakan penyelenggaraan sistem elektronik yang berbasis teknologi digital. Akibat dari perkembangan yang luar biasa, istilah telematika berkembang menjadi istilah Teknologi Informatika (TI), Information & Communication Technologies (ICT)

Keberadaan Telematika, berkaitan dengan perkembangan internet yang pada awalnya memberikan dunia baru bagi masyarakat dunia. Dunia baru yang seakan-akan ditemukan tersebut bernama *Cyberspace*. Istilah *Cyberspace* menjadi populer setelah istilah tersebut digunakan dalam novel *science fiction*, karya William Gibson. *Cyberspace* menggambarkan suatu halusinasi adanya alam lain yang mempertemukan teknologi telekomunikasi dan informatika, yang seakan-akan terdapat ruang dalam medium *Cyber*. Asal usul kata *Cyber* diartikan sebagai kawat listrik. *Cyberspace* dapat diartikan sebagai jaringan komputer mahabesar (*gigantic network*) tanpa adanya penguasa tunggal mutlak, tanpa ada satu pun hukum suatu negara

yang berlaku. *Cyberspace* merupakan medium komunikasi global yang didasarkan atas kebebasan berinformasi (*freedom of information*) dan kebebasan berkomunikasi (*free flow of information*), keberadaan alam yang baru ini seakan-akan menjadi jawaban dari impian untuk melampiaskan kebebasan mengemukakan pendapat (*free of speech*).

Howard Rheingold menyatakan bahwa, *Cyberspace* adalah sebuah ‘ruang imajiner’ atau ‘maya’ yang bersifat *artificial*, dimana setiap orang melakukan apa saja yang biasa dilakukan dalam kehidupan sosial sehari-hari dengan cara yang baru. Hal senada disampaikan oleh Ahmad Ramli dkk bahwa², “Setiap kegiatan siber meskipun bersifat *virtual* tetapi dikategorikan sebagai tindakan dan perbuatan yang nyata.” Sebuah kenyataan sosial bahwa internet menawarkan ruang publik yang maya, namun nyata terjadi dan nyata akibat-akibatnya.³ Lebih jelasnya diuraikan oleh Barda Nawawi Arief sebagai berikut:

Dunia nyata dan maya (*cyberspace*) tidak terpisah secara tegas. Artinya aktifitas di internet walaupun dianggap sebagai suatu aktifitas maya, dalam pengaturannya tidak dapat dilepaskan dari manusia dalam dunia nyata. Ini dikarenakan internet sebagai sebuah teknologi menuntut peran manusia dalam pengoperasiannya. Manusia dalam alam nyatalah yang bertanggung jawab atas akibat dari perbuatannya.¹⁹

Seiring dengan perkembangan *Cyberspace* sebagai medium komunikasi global antar subjek yang dapat berkomunikasi, memunculkan pula hak dan kewajiban dari tiap-tiap subjek. Hal tersebut membuat banyak negara yang mencoba mengatur

¹⁹ Barda Nawawi Arief, *Tindak Pidana Mayantara Op. Cit.*, hlm. 113.

keberadaan alam baru tersebut. Beberapa negara dikenal istilah *Cyberlaw* atau *Cyberspace law*. Kedua istilah tersebut, secara sekilas memiliki makna yang sama. Namun, apabila ditelaah lebih lanjut, muncul perbedaan yang berpengaruh dari penggunaan kedua istilah tersebut. Menurut Edmon Makarim, istilah yang cocok adalah *Cyberspace Law* karena hukum yang berlaku adalah hukum yang dilaksanakan pada medium *Cyberspace*, sedangkan penggunaan istilah *Cyberlaw*, lebih cocok digunakan untuk hukum-hukum ilmu fisika yang berkaitan dengan arus listrik dalam kawat. Hal tersebut dikaitkan dengan arti istilah *cyber*, yang sudah disebutkan sebelumnya, yaitu kawat listrik. Namun demikian, apabila ditelaah lebih lanjut, istilah *Cyberspace Law* juga tidak begitu tepat, karena istilah ini hanya berbicara tentang halusinasi alam *virtual*. Istilah yang tepat adalah Hukum Telematika, karena makna dari Telematika dikaitkan dengan *Cyberspace* yaitu pada hakikatnya merupakan suatu sistem elektronika yang lahir dari hasil perkembangan dan konvergensi telekomunikasi, media dan informatika itu sendiri.

Hukum Telematika diartikan pula sebagai suatu hukum yang mengembangkan konvergensi telematika yang berwujud dalam penyelenggaraan suatu sistem elektronik, baik yang terkoneksi melalui internet atau tidak. Meskipun demikian istilah yang digunakan untuk hukum yang mengatur di dunia *Cyber* belum seragam, karena seperti yang diuraikan oleh Ahmad M. Ramli²⁰ yang lebih memilih istilah *Cyberlaw* atau Hukum Siber. Hal tersebut dikaitkan dengan makna *Cyberlaw* yang dilandasi dengan pemikiran bahwa istilah *Cyber* jika diidentikan dengan dunia maya akan cukup

²⁰ Ahmad M.Ramli, *Cyber Law dan Haki*, Op., Cit, hlm. 2

menghadapi persoalan ketika terkait dengan pembuktian dan penegakan hukum.

Berkaitan dengan istilah *Cyber*, dikenal pula istilah *Cybernetic*, yang dikenalkan oleh Noebert Winner, pakar matematika yang mengenalkan istilah *Cyberspace teory*. Makna dari *Cybernetic teory* adalah teori yang ditujukan untuk pendekatan interdisipliner dalam uraian sistem kendali dan komunikasi dari manusia, hewan mesin dan organisasi yang mengutamakan umpan baik (*feedback*). Berdasarkan teori tersebut, dapat diambil maknanya yaitu dalam memahami suatu penyampaian informasi yang disampaikan dalam suatu sistem komunikasi yang baik, selayaknya harus dengan memerhatikan unpan balik (*feedback*) dari sistem tersebut.

Lingkup pengkajian Hukum Telematika dapat terbagi dua komponen. Komponen yang pertama berkaitan dengan komponen yang terkait dengan sistem, misalnya perangkat keras, perangkat lunak, prosedur, manusia dan informasi. Komponen yang kedua adalah berkaitan dengan fungsi-fungsi telekomunikasi, misalnya input, proses, output, penyimpanan, komunikasi. Kedua komponen tersebut dikenal dalam 4 komponen yaitu:²¹

1. *Content*, yaitu substansi dari data yang dapat merupakan output/input dari penyelenggaraan sistem informasi yang disampaikan kepada publik.
2. *Computing*, yaitu suatu sistem pengolah informasi yang berbasiskan sistem komputer yang merupakan jaringan komputer yang efisien, efektif dan legal.
3. *Communication*, yaitu keberadaan sistem komunikasi dari sistem *interconnection, global interpersonal, computer network*.

²¹ Edmon Makarim, Kompilasi Hukum, Op. Cit., hlm 12.

4. *Community*, yaitu masyarakat sebagai pelaku intelektual

B. Pengertian hukum telematika

Cyber law adalah rezim hukum baru yang di dalamnya memiliki berbagai aspek hukum yang sifatnya multidisiplin. Dalam modul ini *cyberlaw* juga diartikan sebagai hukum telekomunikasi multimedia dan informatika (telematika). Pengertian ini menunjukkan sifat konvergentif dari *communication*, *computing*, *content*, dan *community* sehingga cyber law membahas dari teknologi dan informasi secara konvergensi.

Definisi Hukum Telematika, atau yang dikenal dengan cyber law, adalah keseluruhan asas-asas, norma atau kaidah lembaga-lembaga, institusi-institusi dan proses yang mengatur kegiatan virtual yang dilaksanakan dengan menggunakan teknologi informasi dan komunikasi (disingkat menjadi TIK).

Perbuatan-perbuatan yang diatur seringkali bersifat tanpa batas (*borderless*) melintas batas-batas teritorial negara, berlangsung demikian cepat sehingga seringkali menembus batas ruang dan waktu. Perbuatan hukum ini meskipun memiliki karakter virtual tetapi berakibat sangat nyata. Saat ini hampir seluruh umat manusia tidak dapat melepaskan diri dari unsur *cyber law* karena penggunaan TIK telah memasuki hampir seluruh segmen kehidupan dari mulai penggunaan seluler, pemanfaatan internet, penggunaan transaksi perbankan secara elektronik dan lain-lain.

Dunia hukum sebenarnya sudah sejak lama memperluas penafsiran asas dan normanya ketika menghadapi persoalan yang bersifat tidak berwujud, misalnya dalam kasus pencurian listrik yang pada awalnya sulit dikategorikan

sebagai delik pencurian tetapi akhirnya dapat diterima sebagai perbuatan pidana. Kenyataan saat ini yang berkaitan dengan kegiatan

siber tidak lagi sesederhana itu, mengingat kegiatannya tidak lagi bisa dibatasi oleh teritori suatu negara, aksesnya dengan mudah dapat dilakukan dari belahan dunia manapun, kerugian dapat terjadi baik pada pelaku internet maupun orang lain yang tidak pernah berhubungan sekalipun, misalnya dalam pencurian dana kartu kredit melalui pembelanjaan di internet. Di samping itu masalah pembuktian merupakan faktor yang sangat penting, mengingat data elektronik bukan saja belum terakomodasi dalam sistem hukum acara Indonesia, tetapi dalam kenyataannya data dimaksud juga ternyata sangat rentan untuk diubah, disadap, dipalsukan dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik. Sehingga dampak yang diakibatkannya pun bisa demikian cepat, bahkan sangat dahsyat. Teknologi informasi telah menjadi instrumen efektif dalam perdagangan global.²²

Persoalan yang lebih luas juga terjadi untuk masalah-masalah keperdataan, karena saat ini transaksi *e-commerce* telah menjadi bagian dari perniagaan nasional dan internasional.²³ Contoh konkret adalah untuk membayar zakat atau berkurban pada saat Idul Adha, atau memesan obat-obatan yang bersifat sangat pribadi orang cukup melakukannya melalui internet. Bahkan untuk membeli majalah orang juga dapat membayar tidak dengan uang tapi cukup dengan mendebit pulsa telepon seluler melalui fasilitas SMS. Kenyataan ini menunjukkan bahwa konvergensi di bidang telematika berkembang

²² Pembahasan mengenai *e-commerce* dan dampaknya terhadap perniagaan global dapat dilihat lebih lanjut pada Abu Bakar Munir, *Cyber Law Policies and Challenges*, 1999, hlm. 205,

²³ United Nations Publication, New York, 1999, dan *UNCITRAL Model Law on Electronic Signature with Guide to Enactment 2001*, United Nations Publication, New York, 2002.

terus tanpa dapat dibendung, seiring dengan ditemukannya Hak Cipta dan paten baru di bidang teknologi informasi.²⁴

Cyber Law adalah aspek hukum yang istilahnya berasal dari Cyberspace Law, yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat mulai "*online*" dan memasuki dunia cyber atau maya. Di negara yang telah maju dan negara berkembang dalam penggunaan internet sebagai alat untuk memfasilitasi setiap aspek kehidupan mereka, perkembangan hukum dunia maya sudah sangat maju. Sebagai kiblat dari perkembangan aspek hukum ini, Amerika Serikat merupakan negara yang telah memiliki banyak perangkat hukum yang mengatur dan menentukan perkembangan Cyber Law.

Kegiatan siber meskipun bersifat *virtual* dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis untuk ruang siber sudah tidak pada tempatnya lagi untuk mengkategorikan sesuatu dengan ukuran dan kualifikasi hukum konvensional untuk dapat dijadikan objek dan perbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal-hal yang lolos dari jerat hukum. Kegiatan siber adalah kegiatan *virtual* yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian subjek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata. Dalam kegiatan *e-commerce* antara lain dikenal

²⁴ Rosener, Jonathan, *CyberLaw: The Law of The Internet*, Springer-Verlag, New York, 1996, hlm. 1-20.

adanya dokumen-dokumen elektronik yang kedudukannya disetarakan dengan dokumen-dokumen yang dibuat di atas kertas.²⁵

Perkembangan teknologi komunikasi dan informasi (*Information and Communication Technology-ICT*) yang begitu pesat dengan segala fasilitas penunjangnya dalam peradaban manusia modern saat ini, telah membawa kita memasuki era baru yang disebut sebagai era digital (*digital age*). Berbagai bidang kehidupan akhirnya dirambah oleh kemajuan ICT tersebut. Perkembangan teknologi komunikasi massa yang menekankan pada komunikasi antarindividu manusia secara langsung, seperti halnya pada penggunaan telepon, mengalami kemajuan yang sangat berarti dengan dikenal dan digunakannya telepon bergerak atau yang lebih dikenal dengan '*cellular phone*'. Dalam perkembangan teknologi informasi kemudian dikenal internet sebagai salah satu media untuk berkomunikasi.

Internet bukan merupakan objek yang kasat mata yang dapat disentuh dan dapat dirasakan. Internet merupakan lapisan kompleksitas teknologi dan jasa yang perlahan-lahan bergabung membentuk sesuatu yang dapat dinikmati oleh semua orang. Internet (merupakan) jaringan komputer terbesar di dunia yang menghubungkan jutaan manusia, tumbuh secara eksponensial. Jaringan yang terhubung ini menjadi antarjaringan (*internetwork*) karena memiliki faktor penggabung sama yang memungkinkan berbagai jaringan untuk bekerja sama.

Internet adalah milik seluruh penghuni dunia. Setiap orang atau lembaga dengan bebas dapat menyambungkan komputernya di internet. Setiap pengguna internet semakin mendapat kemudahan

²⁵ Cf. Ahmad M. Ramli, *Kekuatan Akta Elektronik Sebagai Alat Bukti Pada Transaksi E-Commerce Dalam Sistem Hukum Indonesia*, Makalah disampaikan pada Kongres Ikatan Notaris Indonesia, Bandung 23 Januari 2003, hlm. 12-19.

dalam berkomunikasi, baik itu hanya sekedar berkirim pesan, berdiskusi bahkan melakukan transaksi. Internet secara cepat dan tidak disadari telah mempertemukan dan menyatukan warga dunia. Dengan demikian batas negara di internet menjadi semakin memudar. Samarnya batas-batas negara dalam dunia internet disebabkan oleh karena internet dapat diakses oleh setiap penggunanya di seluruh dunia, dan para pengguna internet di seluruh dunia dapat saling berhubungan dalam hitungan waktu sangat tepat, pada saat mereka mengakses ke dalam jaringan (*real time*).

Seiring dengan kemajuan pola pikir manusia, penggunaan internet mulai memasuki babak selanjutnya, kemudian dikenal apa yang disebut sebagai transaksi elektronik dalam perdagangan yang dilakukan melalui media elektronik (*electronic commerce*). Terjadinya transaksi perdagangan barang maupun jasa melalui media internet kemudian menjadi trend yang berkembang dengan pesat. Dengan adanya transaksi yang menggunakan media internet, waktu dan tempat bukan merupakan penghalang bagi para pelaku ekonomi untuk melaksanakan transaksi. Para pelaku transaksi tersebut tidak perlu mengadakan pertemuan untuk melaksanakan transaksi. Sistem transaksi yang berjalan pun pada akhirnya juga berubah mengikuti perkembangan tersebut, di mana sistem transaksi berubah menjadi sistem online shopping, online dealing, dan lain-lain, di mana pembeli yang membutuhkan barang dapat mengakses internet yang dipunyainya untuk mencari dan membeli apa yang dibutuhkan tanpa harus langsung mendatangi toko yang menyediakan barang kebutuhan pembeli tersebut.

Perkembangan teknologi informasi yang sudah sedemikian pesat dengan adanya transaksi melalui media internet, pada dasarnya

merupakan pasar yang potensial, di mana konsumen dapat melakukan transaksi dengan distributor atau produsen di seluruh dunia dengan biaya yang relatif rendah.

Dalam era globalisasi, efisiensi dalam berbagai bidang kehidupan merupakan hal yang mutlak dilakukan untuk mencapai tingkat perekonomian yang lebih baik dan lebih kompetitif. Suatu negara akan tertinggal jauh apabila tidak dapat dengan cepat mengikuti dan mengaplikasikan perkembangan bidang transaksi yang memanfaatkan kemajuan di bidang teknologi informasi. Transaksi melalui media internet telah terbukti dapat meningkatkan efisiensi daya kerja dan menumbuhkan aktivitas baru yang merangsang tingkat pertumbuhan.

Sementara itu derasnya penetrasi sebuah teknologi informasi dalam kegiatan bisnis yang berbasis transaksi elektronik (seperti: layanan ATM, transaksi bisnis melalui *handphone*, *mobile banking*, *internet banking*, dan lainlain) sebagaimana digambarkan di atas ternyata belum diikuti dengan perkembangan hukum yang dapat mengikuti percepatan perkembangan implementasi teknologi. Oleh karena itu, diperlukan kehadiran hukum yang dapat meng-cover permasalahan pelanggaran-pelanggaran yang terjadi di dunia maya, karena hukum positif (*existing law*) yang ada di bidang ini belum dapat menjangkau hal-hal tersebut. Meskipun seringkali muncul pertanyaan, apakah hukum positif dapat diterapkan terhadap kasus-kasus dan pelanggaran hukum di dunia maya, sebab ada perbedaan yang sangat besar antara masyarakat virtual dengan masyarakat nyata dalam segi tindak dan perbuatan hukum, dampak yang diakibatkan, penerapan sanksi dan juga pembuktianya. Namun demikian untuk memberikan koridor hukum yang jelas dan terarah serta menyikapi pentingnya akan undang-undang yang berkaitan

dengan dunia maya (*cyberspace*), khususnya yang mencakup pengaturan transaksi elektronik.

Jenis-jenis kejahatan di internet terbagi dalam berbagai versi. Salah satu versi menyebutkan bahwa kejahatan ini merupakan kejahatan dengan motif intelektual. Biasanya jenis yang pertama ini tidak menimbulkan kerugian dan dilakukan untuk kepuasan pribadi. Jenis kedua adalah kejahatan dengan motif politik, ekonomi atau kriminal yang berpotensi menimbulkan kerugian bahkan perang informasi. Versi lain membagi cybercrime menjadi tiga bagian yaitu pelanggaran akses, pencurian data, dan penyebaran informasi untuk tujuan kejahatan.

C. Sumber-sumber hukum telematika

Sumber-sumber hukum telematika dapat dibagi menjadi sumber hukum yang sifatnya internasional yang terdiri dari:

1. konvensi-konvensi internasional publik dan perdata,
2. kebiasaan-kebiasaan internasional,
3. *policy international* di bidang *cyber law* misalnya Uniform Domain Name Resolution Dispute Policy (UDRP).

Di samping itu meskipun tidak bersifat norma terdapat pula beberapa pedoman yang menjadi rujukan secara internasional dan menjadi *guideline*. Misalnya, UNCITRAL model *law on electronic digital signature*.

Sumber hukum nasional berupa peraturan perundang-undangan di bidang *cyber law* secara khusus. Ketentuan-ketentuan tentang *cyber law* yang tersebar di dalam berbagai peraturan perundang-undangan. Misal, Undang-undang Tindak Pidana Korupsi (UU Tipikor).

D. Kedudukan hukum telematika dalam Ilmu Hukum

Akseleratif sehingga membawa *trend* baru yang ditandai oleh konvergensi perkembangan teknologi informasi dan komunikasi dirasakan semakin atau penggabungan teknologi informasi dan komunikasi yang sebelumnya terpisah-pisah. Perkembangan teknologi informasi dan komunikasi selama dekade terakhir ini tak lepas dari meningkatnya kebutuhan masyarakat dalam berkomunikasi. Meningkatnya kebutuhan untuk berkomunikasi di masyarakat menyebabkan perubahan signifikan terhadap cara-cara komunikasi konvensional yang berujung dengan upaya-upaya menghadirkan berbagai media teknologi informasi dan komunikasi yang semakin dan lebih konvergen.

Hal ini tidak saja mempengaruhi pertumbuhan bisnis dan industri telekomunikasi, namun juga bisnis dan industri lain yang terlibat dalam pemanfaatan teknologi yang mengalami konvergensi, antara lain bisnis dan industri penyiaran dan teknologi informasi.

Pesatnya perkembangan teknologi informasi dan komunikasi (*information and communication technology/ICT*) dewasa ini membuat arus globalisasi (politik, sosial, ekonomi, dan budaya) terasa semakin deras mengalir ke seluruh penjuru dunia. Indonesia sebagai masyarakat dunia tidak terlepas dari pengaruh arus globalisasi yang menghapus batas-batas ruang antarnegara, juga menghapus batas jarak dan waktu sehingga menciptakan banyak perubahan di tengah masyarakat Indonesia.

Melihat perkembangan *trend* konvergensi dan peranannya yang semakin besar pengaruhnya bagi penunjang kegiatan ekonomi dan sosial dan politik, dan untuk lebih dapat mengoptimalkan pemanfaatan konvergensi teknologi informasi dan komunikasi ini, maka bangsa dan pemerintah Indonesia harus lebih siap dan tanggap dalam merespons konvergensi teknologi informasi dan komunikasi

serta implikasi-implikasi yang dihadirkannya. Persiapan reaktif dan proaktif-antisipatif perlu dilakukan dengan melakukan perubahan-perubahan, salah satunya melalui perubahan regulasi.

E. Hubungan hukum telematika dengan hukum administrasi negara

Hukum telematika memiliki keterkaitannya dengan Hukum Administrasi Negara. Mengenai Hukum Administrasi Negara para sarjana hukum di negeri Belanda selalu berpegang pada paham Thorbecke, beliau dikenal sebagai Bapak Sistematik Hukum Tata Negara dan Hukum Administrasi Negara. Adapun salah satu muridnya adalah Oppenheim, yang juga memiliki murid Mr. C. Van Vollenhoven. Thorbecke menulis buku yang berjudul Aantekeningen op de Grondwet (Catatan atas undang-undang dasar) yang pada pokoknya isi buku ini mengkritik kebijaksanaan Raja Belanda Willem I, Thorbecke adalah orang yang pertama kali mengadakan organisasi pemerintahan atau mengadakan sistem pemerintahan di Belanda, di mana pada saat itu Raja Willem I memerintah menurut kehendaknya sendiri, pemerintahan di Den Haag, membentuk dan mengubah kementerian-kementerian menurut orang-orang dalam pemerintahan.

Oppenheim memberikan suatu definisi Hukum Administrasi Negara adalah sebagai suatu gabungan ketentuan-ketentuan yang mengikat badan-badan yang tinggi maupun yang rendah apabila badan-badan itu menggunakan wewenang yang telah diberikan kepadanya oleh Hukum Tata Negara. Hukum Administrasi Negara menurut Oppenheim adalah sebagai peraturan-peraturan tentang negara dan alat-alat perlengkapannya dilihat dalam geraknya (hukum negara dalam keadaan bergerak atau staat in beweging).

Asas-Asas Pemerintahan/administrasi yang baik ada 2 (dua) macam²⁶:

1. asas-asas yang menangani prosedur/proses pengambilan keputusan, yang bilamana dilanggar secara otomatis membuat keputusan yang bersangkutan batal karena hukum tanpa memeriksa lagi kasusnya;
2. asas-asas yang menangani kebenaran daripada fakta-faktanya yang dipakai sebagai dasar untuk pembuatan keputusan.

Hukum Administrasi Negara sangat berperan dalam melaksanakan sistem manajemen kepemerintahan dan elemen-elemen yang membantunya sebab seperti yang dikatakan Prajudi Atmasudirjo tentang Administrasi Negara memiliki 3 arti, yaitu²⁷:

1. sebagai aparatur negara, aparatur pemerintah atau sebagai institusi politik (kenegaraan);
2. administrasi negara sebagai “fungsi atau sebagai aktivitas melayani pemerintah, yakni sebagai kegiatan “pemerintahan operasional”; dan
3. administrasi negara sebagai proses teknis penyelenggaraan undang-undang

Sebagai aparatur pemerintah yang mengeluarkan pelayanan dalam bentuk kebijakan sering diklasifikasikan sebagai jasa publik yang harus dilaksanakan untuk memenuhi kebutuhan masyarakat.

²⁶ C.S.T.Kansil dan Christine S.T. Kansil, SH, *Modul Hukum Administrasi Negara*, PT Pradnya Paramita, Jakarta, 1997, hal 72

²⁷ Mustafa Bachsan, *Sistem Hukum Administrasi Negara Indonesia*, Bandung, 2001, hal 5-6

Secara teoritis menurut Ratmiko, pelayanan publik sendiri dapat diklasifikasikan atas²⁸ berikut ini.

1. Pelayanan publik atau pelayanan umum yang diselenggarakan oleh organisasi publik. Di mana pelayanan publik menyangkut kebutuhan publik dan digunakan secara publik.
2. Pelayanan publik atau pelayanan umum yang diselenggarakan oleh organisasi privat. Pelayanan publik atau pelayanan umum yang diselenggarakan oleh organisasi privat dapat dibedakan menjadi dua bagian yaitu untuk kebutuhan primer dan sekunder. Dikatakan kebutuhan primer adalah pelayanan publik yang dikelola oleh organisasi privat di mana kebutuhan yang dikelola adalah kebutuhan pokok bagi publik, contohnya listrik bagi negara yang dikelola secara privat oleh Perusahaan Listrik Negara. Selain kebutuhan primer yang dikelola oleh organisasi privat, kebutuhan sekunder juga dikelola oleh organisasi privat.

Keputusan Men-PAN RI No. 63 Tahun 2004 mengatur bahwa hakikat pelayanan publik adalah pemberian pelayanan prima kepada masyarakat yang merupakan pewujudan kewajiban aparatur pemerintah sebagai abdi masyarakat. Berkaitan dengan pengelompokan jenis-jenis pelayanan publik, Keputusan MenPAN RI No. 63 Tahun 2004 membedakan jenis-jenis pelayanan publik menjadi tiga kelompok berikut ini.

1. Kelompok pelayanan administratif yaitu pelayanan yang menghasilkan berbagai bentuk dokumen resmi yang

²⁸ Ratminto, dkk., Manajemen Pelayanan & Pengembangan Model Konseptual, Penerapan Citizen's Charter dan Standar Pelayanan Minimal, 2006, hal 9.

dibutuhkan oleh publik, misalnya status kewarganegaraan, sertifikat kompetensi, kepemilikan atau penguasaan terhadap suatu barang, dan sebagainya. Dokumen-dokumen ini antara lain Kartu Tanda Penduduk (KTP), Akta Pernikahan, Akta Kelahiran, Akta Kematian, Buku Pemilik Kendaraan Bermotor (BPKB), Surat Izin Mengemudi (SIM), Izin mendirikan Bangunan (IMB), Paspor, Sertifikat Kepemilikan / Penguasaan Tanah dan sebagainya.

2. Kelompok Pelayanan Barang yaitu pelayanan yang menghasilkan berbagai bentuk/jenis barang yang digunakan oleh publik, misalnya jaringan telepon, penyediaan tenaga listrik, air bersih, dan sebagainya.
3. Kelompok Pelayanan Jasa yaitu pelayanan yang menghasilkan berbagai bentuk jasa yang dibutuhkan oleh publik, misalnya pendidikan, pemeliharaan kesehatan, penyelenggaraan transportasi, perbankan, dan sebagainya.

Beberapa bidang yang terkait dengan telematika antara lain adalah penyelenggaraan pelayanan hukum yang menghasilkan berbagai bentuk dokumen resmi yang dibutuhkan oleh publik misalnya e-KTP, e-government, e-passport dan pengesahan badan hukum. Dalam proses pemberian pengesahan badan hukum (PT) pada saat ini dengan berkembangnya teknologi informasi pendaftaran dilakukan secara on-line oleh notaris yang berada di seluruh tanah air. Notaris cukup dengan mengakses melalui situs yang sudah disediakan.

Seiring dengan pertumbuhan dunia usaha dan investasi dan keterbukaan informasi publik, untuk mewujudkan pelayanan yang transparan dan akuntabel. Pemerintah memiliki beberapa pelayanan

hukum yang diberikan kepada masyarakat yang berhubungan dengan dunia usaha dan investasi. Pelayanan tersebut disajikan dengan sistem teknologi informasi sehingga memudahkan bagi seluruh masyarakat mendapatkan kepastian hukum.

Sistem yang diterapkan oleh pemerintah dalam memberikan suatu surat keputusan yang bersifat elektronik telah membuka pintu birokrasi yang awalnya lambat menjadi lebih cepat. Karena dalam teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi semuanya dilakukan dengan digitalisasi.

F. Hubungan hukum telematika dengan hukum pidana

Kejahatan sesungguhnya merupakan sesuatu hal yang tak lepas dari sejarah panjang umat manusia di muka bumi ini. Dan pembicaraan mengenai kriminologi dengan teori-teorinya yang telah berkembang tidak akan berhenti selama masih ada kejahatan di masyarakat. Akan tetapi, pembicaraan itu tidak bisa dijeaskan dari institusi lain karena ada keterkaitan yang sangat erat antara kriminologi dengan institusi itu, yaitu hukum terutama hukum pidana, bahkan sejak kelahirannya kriminologi dan hukum pidana mempunyai hubungan yang sangat erat.

Hukum memiliki keterikatan yang sangat luas dengan berbagai bidang ilmu. bahkan wenguasaan ilmu hukum secara tunggal tidak akan dapat memecahkan masalah yang dihadapi masyarakat, sehingga diperlukan pengetahuan lain agar pemahaman terhadap permasalahan menjadi lebih jelas tajam dan tidak simpangsiur. Dengan berbekal pengetahuan hukum dan pengetahuan sosial lain, seperti sosiologi, psikologi, antropologi, religi, ekonomi, politik dan budaya maka diagnosis mengenai kesulitan-kesulitan yang dihadapi masyarakat dapat lebih cermat dan pemecahannva pun lebih dapat

diterima oleh masyarakat. Mulyana W. Kusuma bahkan mengatakan bahwa:

"Perkembangan kriminologi dari dahulu sampai sekarang tidak bisa dilepaskan dari keberadaan hukum pidana dan sosiologi hukum itu sendiri. Kriminologi, sosiologi dan hukum pidana memiliki lahan kajian yang satu sama lain saling berkaitan, sehingga tidak mengherankan apabila dengan memberdayakan ketiga kajian itu secara integral akan diperoleh pemahaman yang lebih baik dan mendekati kebutuhan senyatanya mengenai realitas kejahatan yang ada di masyarakat".²⁹

Kriminologi, khususnya sebagai pengaruh pemikiran kritis mengarahkan studinya pada proses-proses (kriminalisasi), baik proses pembuatan maupun bekerjanya undang-undang, dapat memberikan sumbangan besar di bidang sistem peradilan pidana fokusnya berupa penelitian tentang penegakan hukum sehingga dapat digunakan untuk memperbaiki bekerja,nya aparat penegak hukum.³⁰

Perkembangan teknologi juga membawa dampak dalam perkembangan hukum pidana. Kajian yang dilakukan oleh kriminologi dapat dijadikan sebagai sarana untuk membangun hukum pidana yang didasarkan pada alasan-alasan logis hasil pemikiran kriminologis. Sampai tahap tertentu pemikiran kriminologis penting untuk perkembangan teori kriminologi dan pada tahap selanjutnya penting untuk ilmu hukum pidana terutama dalam kaitannya dengan persoalan kriminalisasi, dekriminalisasi dan depenalisasi.

²⁹ Mulyana W. Kusuma, *Realitas Sosial Kejahatan*, Prisma, LP3ES, Jakarta, 1982, hlm. 39.

³⁰ I.S. Susanto, *Kriminologi*, FI-I UNDIP Semarang, 1995, hlrn. 14.

Permasalahan kriminalisasi, dekriminalisasi dan depenalisa adalah bidang kajian hukum pidana yang erat kaitannya dengan kriminologi. Ketiganya tidak bisa dilepaskan dari kriminologi apabila ingin mendapatkan pengetahuan yang luas dan keputusan yang komprehensif mengenai suatu masalah yang hendak dikriminalkan, didekriminalisasi atau didepenalisasi. Tanpa kajian kriminologi hukum pidana sebenarnya bisa melakukan ketiga hal tersebut, tetapi hasil yang dicapai tentunya tidak akan selengkap dan sebaik apabila menggunakan bantuan kriminologi. Menurut Sudarto bahwa;

"Kriminalisasi merupakan suatu proses penetapan suatu perbuatan yang semula bukan tindak pidana menjadi tindak pidana. Untuk menetapkan suatu perbuatan yang sebelumnya tidak dikategorikan sebagai tindak pidana menjadi perbuatan yang dikategorikan sebagai tindak pidana bukanlah suatu pekerjaan yang mudah. Proses kriminalisasi berakhir dengan terbentuknya undang-undang yang menetapkan perbuatan yang itu dilarang dan diancam dengan sanksi yang berupa pidana".³¹

Tidak mudah untuk menetapkan suatu perbuatan sebagai suatu tindak pidana, artinya ada beberapa proses yang harus dilalui. Selain kajian yang mendalam mengenai perbuatan itu dari sudut kriminologi, maka harus dipertimbangkan pula beberapa hal yang perlu diperhatikan, yaitu tujuan hukum pidana itu sendiri, penetapan perbuatan yang tidak dikehendaki, perbandingan antara sarana dan hasil dan kemampuan badan penegak hukum.

Hukum pidana mempunyai sifat ultimum remedium atau alat terakhir yang berisi pengenaan penderitaan kepada pelaku kejahatan. Sifat hukum pidana ini menyebabkan hukum pidana dinilai sangat

³¹ Sudarto, Hukum dan Hukum Pidana, ... Op.cit, hlm. 32 dan hlm. 151.

kejam sehingga pengenaannya haruslah merupakan upaya terakhir apabila upaya-upaya lain tidak dapat dilakukan untuk memperbaiki pelaku kejahatan. Mengingat sifat kejamnya hukum pidana ini, maka penetapan suatu perbuatan dengan ancaman hukumannya haruslah memperhatikan berbagai aspek kemanusiaan. Proses kriminalisasi dalam hal ini tidak boleh dilakukan sembarangan karena hal ini menyangkut harkat, martabat dan hak asasi manusia untuk hidup.

Penetapan suatu perbuatan menjadi tindak pidana atau bukan haruslah didasarkan pada pertimbangan yang matang. Penetapan ini harus dijauhkan dari unsur-unsur politis sehingga mereka yang mempunyai kekuasaan tidak dapat mempengaruhi pembuat undang-undang agar perbuatan jahatnya tidak terkena jerat hukum. Meskipun ada anggapan bahwa undang-undang adalah hasil dari kompromi politis, tetapi sebisa mungkin unsur politis yang merugikan berbagai pihak (terutama mereka yang tidak mempunyai kekuasaan untuk mempengaruhi pembuat undang-undang) danat ditekan atau diminimalisir.

Penetapan suatu perbuatan menjadi tindak pidana harus pula memperhatikan perbandingan antara sarana dan hasil serta kemampuan aparat penegak hukum. Apabila sarana yang diperlukan dan kemampuan aparatnya tidak memadai, maka penetapan suatu perbuatan menjadi tindak pidana menjadi tidak berarti karena sarana untuk menegakkannya tidak ada sehingga penetapan itu hanya menjadi macan kertas saja, tidak ada implementasinya dan hanya merupakan pemborosan anggaran negara.

Dari uraian tersebut, maka dapatlah dikatakan bahwa proses kriminalisasi merupakan proses yang tidak hanya bersifat sosial, tetapi juga politis. Pandangan hidup yang ada dan dipelihara oleh

masyarakat atau pemegang kekuasaan akan mewarnai hasil kriminalisasi, Sudarto juga mengatakan bahwa:

"Dekriminalisasi adalah suatu proses penghapusan sama sekali sifat dapat dipidananya suatu perbuatan yang semula merupakan tindak pidana dan juga penghapusan sanksinya berupa pidana. Dalam proses dekriminalisasi ini tidak hanya kualifikasi pidana saja yang dihapuskan," tetapi juga sifat melawan hukum atau melanggar hukumnya, lebih dari itu adalah penghapusan sanksi negatif itu tidak diganti dengan reaksi sosial lain, baik perdata maupun administrasi"

Dalam proses dekriminalisasi ini penelitian kriminologi diperlukan untuk menentukan apakah perbuatan itu layak didekriminalisasikan dan bagaimana kemungkinannya di masa yang akan datang. Tidak menutup kemungkinan perbuatan yang telah didekriminalisasikan di masa mendatang oleh masyarakat dituntut untuk dikriminalisasikan sehingga kajian mengenai manfaat dan kerugian dekriminalisasi haruslah mendapat perhatian.

Suatu proses dekriminalisasi dapat terjadi karena beberapa sebab. seperti misalnya (contoh ini tidak bersifat limitatif):³²

1. Suatu sanksi secara sosiologis merupakan persetujuan (sanksi positif) atau penolakan terhadap pola perilaku tertentu (sanksi negatif). Ada kemungkinan bahwa nilai-nilai masyarakat mengenai sanksi negatif tertentu terhadap perilaku tertentu mengalami perubahan, sehingga perilaku yang terkena sanksi-sanksi tersebut tidak lagi ditolak.
2. Timbulnya keragu-raguan yang sangat kuat akan tujuan yang ingin dicapai dengan penetapan sanksi-sanksi negatif tertentu.

³² Soerjono Soekanto et.al., Kriminologi, Suatu Pengantar, ctk. Pertama. Ghalian Indonesia, Jakarta, 1986. hal. 47-48.

3. Adanya keyakinan yang kuat, bahwa biaya sosial untuk menerapkan sanksi-sanksi negatif tertentu sangat besar.
4. Sangat terbatasnya efektivitas dari sanksi-sanksi negatif tertentu sehingga penerapannya akan menimbulkan kepuddaran kewibawaan hukum.

Dalam kaitannya dengan kriminalisasi dan dekriminalisasi ini, Simposium Pembaharuan Hukum Pidana Nasional pada bulan Agustus 1980 dalam salah satu laporannya menyatakan:³³

"Masalah kriminalisasi dan dekriminalisasi atas suatu perbuatan haruslah sesuai dengan politik kriminil yang dianut oleh bangsa Indonesia, yaitu sejauh mana perbuatan tersebut bertentangan atau tidak bertentangan dengan nilai-nilai fundamental yang berlaku dalam masyarakat dan oleh masyarakat dianggap patut atau tidak patut dihukum dalam rangka menyelenggarakan kesejahteraan masyarakat "

Khusus mengenai kriteria kriminalisasi dan dekriminalisasi, laporan simposium itu menyatakan untuk menetapkan suatu perbuatan itu sebagai tindakan kriminil, perlu memperhatikan kriteria umum sebagai berikut:

1. Apakah perbuatan itu tidak disukai atau dibenci oleh masyarakat karena merugikan atau dapat merugikan, mendatangkan korban atau dapat mendatangkan korban;
2. Apakah biaya mengkriminalisasi seimbang dengan hasilnya yang akan dicapai, artinya cost pembuatan undang-undang, pengawasan dan penegakan hukum, serta beban yang dipikul

³³ Laporan Simposium Pembaharuan Hukum Pidana Nasional 1980 di Semarang. seperti dikutip oleh Barda Nawawi Arief, Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Hukum Pidana, BP UNDIP Semarang, 1994. hal. 36.

- korban, pelaku dan pelaku kejahatan itu sendiri harus seimbang dengan situasi tertib hukum yang akan dicapai;
3. Apakah akan makin menambah beban aparat penegak hukum yang tidak seimbang atau nyata-nyata tidak dapat diemban oleh kemampuan yang dimilikinya;
 4. Apakah perbuatan-perbuatan itu menghambat atau menghalangi cita-cita bangsa Indonesia, sehingga merupakan bahaya bagi keseluruhan masyarakat.³⁴

Depenalisa merupakan proses penghapusan ancaman pidana (sehingga ancaman pidananya itu hilang) terhadap perbuatan yang semula merupakan tindak pidana, tetapi masih dimungkinkan adanya penuntutan secara lain. Hal ini dapat dilakukan mengingat sifat hukum pidana sebagai *ultimum remedium*, di mana ancaman pidana yang ada dianggap tidak aspiratif atau terlalu berat, sehingga perlu diganti dengan ancaman pidana lain yang lebih ringan dan manusiawi.

G. Hubungan hukum telematika dengan hukum tata negara

Hukum telematika memiliki keterkaitan dengan ketatanegaraan. Bidang-bidang yang terkait dengan telematika antara lain adalah penyelenggaraan pemilihan presiden, pemilihan kepala daerah, pemilihan umum serta kegiatan-kegiatan lain seperti rapat-rapat penyusunan undang-undang yang melakukan sarana teknologi informasi. Di sisi lain kegiatan-kegiatan ketatanegaraan juga memerlukan saran teknologi informasi misalnya terkait dengan pendokumentasian dan pengalihwujudan data-data dari dokumen-

³⁴ Bandingkan dengan kriteria yang dikemukakan oleh Bassisouni dalam Barwa Nawawi Arief, *ibid*, hlm. 36-37.

dokumen yang sifatnya di atas kertas (paper based) menjadi dokumen elektronik.

Hukum Tata Negara adalah sekumpulan peraturan yang mengatur organisasi dari pada negara, hubungan antara alat perlengkapan negara dalam garis vertikal dan horizontal serta kedudukan warga negara dan hak-hak asasinya.

Unsur-unsur/ciri-ciri khas daripada suatu Negara hukum atau Rechstaat adalah:

1. adanya pengakuan dan perlindungan terhadap hak-hak asasi manusia yang mengandung persamaan dalam bidang politik, ekonomi, sosial, kultur dan pendidikan;
2. adanya peradilan yang bebas dan tidak memihak, tidak dipengaruhi oleh suatu kekuasaan atau kekuatan lain apapun;
3. adanya legalitas dalam arti hukum dalam semua bentuknya;
4. adanya undang-undang dasar yang memuat ketentuan tertulis tentang hubungan antara penguasa dengan rakyat.

Asas Pembagian Kekuasaan dan Check Belances yang berarti pembagian kekuasaan negara itu terpisah-pisah dalam beberapa bagian baik mengenai fungsinya. Montesquieu mengemukakan bahwa setiap Negara terdapat tiga jenis kekuasaan, yaitu Trias Politica: Eksekutif, Legislatif, dan Yudikatif.

Dapat kita sadari bahwa terdapat kesenjangan antara hukum dan teknologi. Hukum selalu tertinggal oleh dinamika teknologi. Perkembangan hukum cenderung memakan waktu yang lama, hal ini mungkin karena sifatnya yang kaku dan terlalu birokratis. Sementara, dinamika teknologi berkembang begitu cepat tanpa batas-batas kaku yang birokratis seperti hukum. Ketimpangan ini sering menimbulkan ruang-ruang kosong dalam hukum yang dapat menimbulkan kebingungan dalam masyarakat.

H. Hubungan hukum telematika dengan hukum perikatan

Pada era teknologi informasi orang lebih memilih bertransaksi bisnis melalui media elektronik, karena lebih efektif dan efisien. Transaksi yang dilakukan melalui media elektronik merupakan bentuk kegiatan yang berhubungan dengan telematika, yang menjadi perhatian adalah perjanjian secara elektronik atau *electronic contract*. Perjanjian di era *digital* akan menggunakan data digital sebagai pengganti kertas. Penggunaan data digital sebagai media dalam melakukan perjanjian akan memberikan efisiensi yang sangat besar terutama bagi perusahaan-perusahaan yang menjalankan bisnisnya di internet.

Menurut Mieke Komar Kantaatmadja perjanjian jual beli yang dilakukan melalui media elektronik internet tidak lain adalah merupakan perluasan dari konsep perjanjian jual beli yang ada dalam KUH Perdata. Perjanjian jual beli melalui internet ini memiliki dasar hukum perdagangan konvensional atau jual beli dalam hukum perdata. Perbedaannya adalah bahwa perjanjian melalui internet ini bersifat khusus karena terdapat unsur peranan yang sangat dominan dari media dan alat-alat elektronik.³⁵

Menurut Mieke Komar Kantaatmadja, mengenai kapan terjadinya kesepakatan terdapat beberapa teori, antara lain:³⁶

1. Teori ucapan

Suatu perjanjian tercapai pada saat orang menerima tawaran dan menyetujui tawaran tersebut.

2. Teori pengiriman

³⁵ Mieke Komar Kantaatmadja, 2001, Cyberlaw: Suatu Pengantar, cet.1, Bandung,ELIPS, Hal.15

³⁶ *Ibid* hal 29

Perjanjian tercapai pada saat dikirimkannya surat jawaban mengenai penerimaan terhadap suatu penawaran.

3. Teori pengetahuan

Menurut teori ini, bahwa perjanjian tercapai setelah orang yang menawarkan mengetahui bahwa penawarannya telah disetujui.

4. Teori penerimaan

Menyatakan perjanjian tercapai saat diterimanya surat jawaban penerimaan oleh orang yang menawarkan.

Menurut Mieke Komar Kantaatmadja mengenai kapan terjadinya kesepakatan menganut teori penerimaan di mana suatu perjanjian telah lahir ketika pihak yang melakukan penawaran menerima surat jawaban berupa penerimaan terhadap penawaran tersebut.

Hukum Perikatan adalah hubungan hukum antara dua orang atau lebih di dalam lapangan harta kekayaan di mana satu pihak mempunyai hak dan pihak yang lain mempunyai kewajiban atas suatu prestasi. Sedangkan perjanjian adalah perbuatan hukum.

Menurut ilmu pengetahuan Hukum Perdata, pengertian perikatan adalah suatu hubungan dalam lapangan harta kekayaan antara dua orang atau lebih di mana pihak yang satu berhak atas sesuatu dan pihak lain berkewajiban atas sesuatu. Beberapa sarjana juga telah memberikan pengertian mengenai perikatan. Pitlo memberikan pengertian perikatan yaitu suatu hubungan hukum yang bersifat harta kekayaan antara dua orang atau lebih, atas dasar mana pihak yang satu berhak (kreditur) dan pihak lain berkewajiban (debitur) atas suatu prestasi.

Dengan demikian, perikatan yang terjadi antara orang yang satu dengan yang lain itu disebut hubungan hukum. Jika dirumuskan,

perikatan adalah suatu hubungan hukum dalam lapangan harta kekayaan antara dua orang atau lebih di mana pihak yang satu berhak atas sesuatu dan pihak lain berkewajiban atas sesuatu. Hubungan hukum dalam harta kekayaan ini merupakan suatu akibat hukum, akibat hukum dari suatu perjanjian atau peristiwa hukum lain yang menimbulkan perikatan. Dari rumusan ini dapat diketahui bahwa perikatan itu terdapat dalam bidang hukum harta kekayaan (*law of property*), juga terdapat dalam bidang hukum keluarga (*family law*), dalam bidang hukum waris (*law of succession*) serta dalam bidang hukum pribadi (*personal law*).

I. Hubungan hukum telematika dengan hukum perlindungan konsumen

Hubungan hukum yang terjadi melalui media elektronik akan menimbulkan akibat hukum bagi pihak lain, oleh karenanya hukum telematika erat kaitannya dengan perlindungan konsumen untuk melindungi kepentingan hukum masyarakat. Perlindungan konsumen itu sendiri menurut Pasal 1 Ayat (1)

Undang-Undang Perlindungan Konsumen menyebutkan “Perlindungan konsumen adalah segala upaya yang menjamin adanya kepastian hukum untuk memberi perlindungan kepada konsumen”.

Pasal 2 Undang-Undang Perlindungan Konsumen menyebutkan “perlindungan konsumen berasaskan manfaat, keadilan, serta keseimbangan, keamanan dan keselamatan konsumen serta kepastian hukum”.

Di dalam penjelasan Pasal 2 Undang-Undang Perlindungan Konsumen menyebutkan perlindungan konsumen diselenggarakan sebagai usaha bersama berdasarkan 5 (lima) asas yang relevan dalam pembangunan nasional, yaitu sebagai berikut.

1. Asas manfaat dimaksudkan untuk mengamanatkan bahwa segala upaya dalam penyelenggaraan perlindungan konsumen harus memberi manfaat sebesar-besarnya bagi kepentingan konsumen dan pelaku usaha secara keseluruhan.
2. Asas keadilan dimaksudkan agar partisipasi seluruh rakyat dapat diwujudkan secara maksimal dan memberikan kesempatan kepada konsumen dan pelaku usaha untuk memperoleh haknya dan melaksanakan kewajibannya secara adil.
3. Asas keseimbangan dimaksudkan untuk memberikan keseimbangan antarkepentingan konsumen, pelaku usaha, dan pemerintah dalam arti materiil maupun spiritual.
4. Asas keamanan dan keselamatan konsumen dimaksudkan untuk memberikan jaminan atas keamanan dan keselamatan kepada konsumen dalam penggunaan, pemakaian, dan pemanfaatan barang dan/atau jasa yang dikonsumsi atau digunakan.
5. Asas kepastian hukum dimaksudkan agar baik pelaku usaha maupun konsumen menaati hukum dan memperoleh keadilan dalam penyelenggaraan perlindungan konsumen, serta negara menjamin kepastian hukum.

Menurut pasal 3 Undang-Undang Perlindungan Konsumen, perlindungan konsumen bertujuan:

1. meningkatkan kesadaran, kemampuan, dan kemandirian konsumen untuk melindungi diri;
2. mengangkat harkat dan martabat konsumen dengan cara menghindarkannya dari akses negatif pemakaian barang atau jasa;

3. meningkatkan pemberdayaan konsumen dalam memilih, menentukan dan menuntut hak-haknya sebagai konsumen;
4. menciptakan 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.

Menurut Johanes Gunawan, perlindungan hukum terhadap konsumen dapat dilakukan pada saat sebelum terjadinya transaksi (*no conflict/pre purchase*) dan/atau pada saat setelah terjadinya transaksi (*conflict/post purchase*).³⁷ Perlindungan hukum terhadap konsumen yang dapat dilakukan pada saat sebelum terjadinya transaksi (*no conflict/pre purchase*) dapat dilakukan dengan cara antara lain:

1. *Legislation*, yaitu perlindungan hukum terhadap konsumen yang dilakukan pada saat sebelum terjadinya transaksi dengan memberikan perlindungan kepada konsumen melalui peraturan perundang-undangan yang telah dibuat. Sehingga dengan adanya peraturan perundangan tersebut diharapkan konsumen memperoleh perlindungan sebelum terjadinya transaksi, karena telah ada batasan-batasan dan ketentuan yang mengatur transaksi antara konsumen dan pelaku usaha.

³⁷ Johanes Gunawan, 1999, Hukum Perlindungan Konsumen, Universitas Katolik Parahyangan, Bandung, hal. 3

2. *Voluntary Self Regulation*, yaitu perlindungan hukum terhadap konsumen yang dilakukan pada saat sebelum terjadinya transaksi, di mana dengan cara ini pelaku usaha diharapkan secara sukarela membuat peraturan bagi dirinya sendiri agar lebih berhati-hati dan waspada dalam menjalankan usahanya.³⁸

Dengan diundangkannya Undang-Undang Informasi dan Transaksi Elektronik sebenarnya sudah mengakomodir bagaimana tata cara bertransaksi elektronik. Urusan yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik adalah didasarkan pada urusan transaksi elektronik yang meliputi transaksi bisnis dan kontrak elektronik. Masalah yang mengemuka dan diatur dalam Undang-Undang Informasi dan Transaksi Elektronik tersebut adalah hal yang berkaitan dengan masalah kekuatan dalam sistem pembuktian dari Informasi, Dokumen, dan Tanda Tangan Elektronik. Pengaturan Informasi.

Dokumen, dan Tanda Tangan Elektronik. Juga secara umum dikatakan bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah, yang merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia. Urusan transaksi elektronik yang diatur dalam Pasal 5 s/d 22 UU ITE merupakan inti dari masalah keperdataan dan bisnis. Urusan ini menjelaskan teknisnya yang khususnya bertujuan untuk memberikan perlindungan kepada masyarakat, khususnya konsumen.

J. Konvergensi Bidang Telematika dengan Undang-Undang Informasi dan Transaksi Elektronik (ITE) di Indonesia

³⁸ Ibid

Hasil konvergensi di bidang telematika salah satunya adalah aktivitas dalam dunia siber yang telah berimplikasi luas pada seluruh aspek kehidupan. Persoalan yang muncul adalah bagaimana untuk penggunaannya tidak terjadi singgungan-singgungan yang menimbulkan persoalan hukum. Pastinya ini tidak mungkin, karena pada kenyataannya kegiatan siber tidak lagi sesederhana itu. Kegiatan siber tidak lagi bisa dibatasi oleh teritori suatu negara dan aksesnya dengan mudah dapat dilakukan dari belahan dunia manapun, karena itu kerugian dapat terjadi baik pada pelaku internet maupun orang lain yang tidak pernah berhubungan sekalipun misalnya dalam pencurian dana kartu kredit melalui pembelanjaan di internet.

Meskipun secara nyata kita merasakan semua kemudahan dan manfaat atas hasil konvergensi itu, namun bukan hal yang mustahil dalam berbagai penggunaannya terdapat berbagai permasalahan hukum. Hal itu dirasakan dengan adanya berbagai penggunaan yang menyimpang atas berbagai bentuk teknologi informasi, sehingga dapat dikatakan bahwa teknologi informasi digunakan sebagai alat untuk melakukan kejahatan, atau sebaliknya pengguna teknologi informasi dijadikan sasaran kejahatan. Sebagai contoh misalnya, dari suatu konvergensi didalamnya terdapat data yang harus diolah, padahal masalah data elektronik ternyata sangat rentan untuk diubah, disadap, dipalsukan dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik. Sehingga dampak yang diakibatkannya pun bisa demikian cepat, bahkan sangat dahsyat.³⁹

Dengan semakin pesatnya perkembangan teknologi informasi, maka pengaturan teknologi informasi tidak cukup hanya dengan

³⁹ Ahmad M Ramli, *Prinsip-prinsip Cyber Law Dan Kendala Hukum Positif Dalam Menanggulangi Cyber Crime*, Fakultas Hukum Universitas Padjajaran, 2004, hlm. 2.

peraturan perundang-undangan yang konvensional, namun dibutuhkan pengaturan khusus yang menggambarkan keadaan sebenarnya dari kondisi masyarakat, sehingga tidak ada jurang antara substansi peraturan hukum dengan realitas yang berkembang dalam masyarakat. Misalnya untuk kegiatan-kegiatan siber. Meskipun bersifat *virtual*, kegiatan siber dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis untuk ruang siber sudah tidak pada tempatnya lagi untuk mengkategorikan sesuatu dengan ukuran dan kualifikasi hukum konvensional untuk dapat dijadikan objek dan perbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal-hal yang lolos dari jerat hukum. Kegiatan siber adalah kegiatan *virtual* yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian subjek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata.

Satu langkah yang dianggap penting untuk menanggulangi masalah keamanan informasi adalah telah diwujudkannya rambu-rambu hukum yang tertuang dalam Undang-undang Transaksi dan Informasi Elektronik (UU No. 11 Tahun 2008 yang disebut sebagai UU ITE). Hal yang mendasar dari UU ITE ini sesungguhnya merupakan upaya mengakselerasikan manfaat dan fungsi hukum (peraturan) dalam kerangka kepastian hukum.⁴⁰

Dengan UU ITE diharapkan seluruh persoalan terkini berkaitan dengan aktivitas di dunia maya dapat diselesaikan dalam hal terjadi persengketaan dan pelanggaran yang menimbulkan kerugian dan bahkan korban atas aktivitas di dunia maya. Oleh karena itu UU ITE ini merupakan bentuk perlindungan kepada seluruh masyarakat

⁴⁰ Sudikno Mertokusumo, dan A. Pitlo, Bab-bab tentang Penemuan Hukum, Citra Aditya Bakti, Yogyakarta, 1993, hal 1.

dalam rangka menjamin kepastian hukum, dimana sebelumnya hal ini menjadi kerisauan semua pihak, khususnya berkenaan dengan munculnya berbagai kegiatan berbasiselektronik.

Ketentuan-ketentuan yang diatur dalam UU ITE meskipun secara umum pengaturannya tetapi cukup komprehensif dan mengakomodir semua hal terkait dunia siber.⁴¹ Materi yang diatur dalam UU ITE umumnya merupakan hal baru dalam sistem hukum Indonesia, hal tersebut meliputi : masalah pengakuan transaksi dan alat bukti elektronik, penyelesaian sengketa, perlindungan data, nama domain dan Hak Kekayaan Intelektual, serta bentuk-bentuk perbuatan yang dilarang beserta sanksi-sanksinya.

Bila dilihat dari sudut pandang keilmuan, UU ITE memiliki berbagai aspek hukum, sehingga dikatakan sebagai UU multi aspek, karena banyak memiliki aspek, dan hampir seluruh aspek hukum diatur. Aspek hukum transnasional, karena jelas-jelas UU ini mengatur lingkup yang tidak saja diIndonesia tetapi melewati batas negara. Aspek hukum pidana, mengatur *Crime* (kejahatan), Aspek Hukum Perdata yang mengatur transaksi- transaksi di bidang bisnis. Aspek Hukum Administrasi, karena menyangkutadanya pemberian izin oleh pemerintah dan aspek hukum acara baik Pidana maupun Perdata.

Banyak kritikan yang bertubi-tubi juga terjadi pada UU ITE. Beberapa persoalan tersebut menyangkut hal sebagai berikut: pertama, apakah transaksi dapat berjalan, karena banyak persoalan teknis yang harusdisiapkan khususnya menyangkut pada transaksi dan penyelenggaraan sistem elektronik; kedua, masalah berkaitan dengan hak asasi manusia dalam menyampaikan pendapat; dan

⁴¹ UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik,

ketiga, masalah ketentuan sanksi (pidana), yang dianggap terlalu berlebihan dan memberatkan. Masalah ini perlu kita perhatikan karena implementasi peraturan (hukum) setidaknya harus dapat memberikan kepastian, kemanfaatan, dan keadilan bagi masyarakat.⁴²

Di samping segala kelebihan dan manfaat dari internet, penggunaan jaringan global maya tersebut berpotensi memiliki dampak hukum yang serius dan diperlukan langkah-langkah konkret untuk mengatasi masalah yang timbul sekaligus mengantisipasi berbagai masalah hukum di masa yang akan datang. Dengan pendekatan hukum yang saat ini telah berdasar atas UU No. 11 Tahun 2008 tentang ITE, maka UU ITE merupakan bentuk upaya perlindungan kepada masyarakat. Dan, setidaknya UU ITE mengatur dua hal yang amat penting, Pertama: pengakuan transaksi elektronik dan dokumen elektronik dalam kerangka hukum perikatan dan hukum pembuktian, sehingga kepastian hukum transaksi elektronik dapat terjamin. Kedua: diklasifikasikannya tindakan-tindakan yang termasuk kualifikasi pelanggaran hukum terkait penyalahgunaan TI disertai sanksi pidananya termasuk untuk tindakan *cybersquatting*, *carding*, *hacking* dan *cracking*.

Dengan diundangkannya UU ITE, bukan berarti seluruh permasalahan yang terjadi di bidang telematika sudah selesai, masih banyak persoalan yang harus juga diantisipasi, terutama atas hasil konvergensi yang pastinya menimbulkan berbagai bentuk layanan virtual baru dan berbagai persoalan teknis yang pastinya terus

⁴² Prof. Dr. Ahmad M. Ramli, S.H., M.H., FCBArb, “*Dinamika Konvergensi Hukum Telematika dalam Sistem Hukum Nasional*”, <http://ditjenpp.kemenkumham.go.id/hukum-teknologi/668-dinamika-konvergensi-hukum-telematika-dalam-sistem-hukum-nasional.html>, diakses pada 23 Desember 2022 pukul 15.00 WIB.

berkembang. Untuk lebih memberikan pemahaman terhadap hukum, khususnya terhadap produk-produk hukum yang sifatnya teknis seperti UU ITE, disamping harus dilakukan diskusi-diskusi ilmiah, juga perlu dilakukan pembudayaan hukum melalui sosialisasi yang intens yang ditujukan terhadap seluruh lapisan masyarakat dan aparat penegak hukum

BAB III

TINDAK PIDANA CYBER CRIME DI INDONESIA

A. Pengertian Cyber Crime

Memasuki pembahasan terkait pengertian cyber crime maka akan menyinggung tentang keamanan suatu jaringan komputer atau informasi teknologi telekomunikasi. Terutama pada era globalisasi saat ini, yang membawa kemajuan teknologi sangat pesat maka hal tersebut tidak terlepas adanya resiko dari penyalahgunaan dari pemanfaatan teknologi sebagai kebutuhan informasi.

“Teknologi telekomunikasi telah membawa manusia kepada suatu peradaban baru dengan struktur sosial beserta tata nilainya. Artinya, masyarakat berkembang menuju masyarakat baru yang berstruktur global. Sistem tata nilai dalam suatu masyarakat berubah, dari yang bersifat lokalpartikular menjadi global universal. Hal ini pada akhirnya akan membawa dampak pada pergeseran nilai, norma, moral, dan kesusilaan.”⁴³

Kemajuan teknologi sangat berdampak besar bagi masyarakat yang membawa dampak positif dan dampak negatif terhadap perkembangan manusia dan peradabannya. Dampak negatif yang dimaksud adalah yang berkaitan dengan dunia kejahatan. J. E Sahetapy telah menyatakan, bahwa kejahatan erat kaitanya dan bahkan menjadi sebagian dari hasil budaya itu sendiri. Maka demikian artinya semakin tinggi tingkat budaya dan semakin modern

⁴³ Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayaantara (Cybercrime)*, Bandung, PT Refika Aditama, hlm. 23.

suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaanya.⁴⁴

Perkembangan teknologi komputer, teknologi informasi, dan teknologi komunikasi juga menyebabkan munculnya tindak pidana baru yang memiliki karakteristik yang berbeda dengan tindak pidana konvensional. Penyalahgunaan komputer sebagai salah satu dampak dari ketiga perkembangan teknologi tersebut itu tidak terlepas dari sifatnya yang memiliki ciri-ciri tersendiri sehingga membawa persoalan yang rumit dipecahkan berkenaan dengan masalah penanggulangannya mulai dari penyelidikan, penyidikan hingga dengan penuntutan.⁴⁵

Sehingga berdasarkan beberapa pendapat tersebut maka dapat dikatakan bahwa adanya kemajuan teknologi dan informasi selain dapat dipergunakan manusia sebagai komoditi informasi, juga dapat membawa dampak negatif yakni penyalahgunaan teknologi yang membawa hal tersebut pada suatu tindak pidana yang disebut dengan *cyber crime*. Adapun tindak pidana *cyber crime* ini memiliki karakteristik tersendiri karena berhubungan dengan jaringan teknologi komputer sehingga dalam penangannya tidak dapat disamakan dengan tindak pidana konvensional.

Cybercrime merupakan kejahatan yang berbeda dengan kejaharan konvensional (*street crime*). *Cyber crime* muncul bersamaan dengan lahirnya revolusi teknologi informasi. Sebagimana dikemukakan oleh Ronni R. Nitibaskara bahwa: "Interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi

⁴⁴ J. E Sahetapy dalam Abdul Wahid, 2002, *Kriminologi dan Kejahatan Kontemporer*, Lembaga Penerbitan Fakultas Hukum Unisma, Malang

⁴⁵ Edmon Makarim, 2005, *Pengantar Hukum Telematika (Suatu Kajian Kompilasi)*, Jakarta PT Raja Grafindo Persada, hlm. 426.

teknologi informasi. Penyimpangan social menyesuaikan bentuk dan karakter baru dalam kejahatan.⁴⁶

Merujuk pada pendapat tersebut maka *cyber crime* dapat dimaknai secara luas dan sempit. Dalam arti sempit, *cyber crime* dapat dimaknai sebagai perbuatan yang melanggar hukum dengan memanfaatkan teknologi komputer. Sedangkan dalam arti luas, *cyber crime* merupakan keseluruhan bentuk kejahatan yang ditujukan pada komputer baik dari jaringan maupun penggunanya serta kejahatan konvensional yang menggunakan teknologi komputer.

Cyber crime atau kejahatan dunia maya dalam peraturan Perundang-undangan di Indonesia juga sering disebut dengan kejahatan tindak pidana yang berkaitan dengan teknologi informasi, hal ini sejalan dengan pengertian yang diberikan oleh Donn B. Parker yang memberikan definisi sebagai berikut.

“Computer abuse is broadly defined to be any incident associated with computer technology in which a victim suffered or could suffer loss and a perpetrator by intention made or could have gain”, yang kemudian diterjemahkan oleh Andi Hamzah sebagai penyalahgunaan komputer didefinisikan secara luas sebagai suatu kejadian yang berhubungan dengan teknologi komputer yang seorang korban menderita atau akan telah menderita kerugian dan seorang pelaku dengan sengaja memperoleh keuntungan atau akan telah memperoleh keuntungan”^{.47}

Sehingga tindak pidana *cyber crime* adalah suatu tindak pidana yang dilakukan dengan menggunakan jaringan teknologi informasi

⁴⁶ Ronni R Nitibaskara dalam Didik M. Arief Mansur dan Elisatris Gultom, 2005, *Cyber Law Aspek Hukum Teknologi Informasi*, Bandung, PT Refika Aditama, hlm. 25.

⁴⁷ Andi Hamzah, 1993, *Hukum Pidana yang berkaitan dengan komputer*, Jakarta : Sinar Grafika Offset, hal. 18

komputer untuk mendapatkan data secara ilegal serta dipergunakan untuk mengambil keuntungan yang tidak sah dan menyebabkan kerugian pada masyarakat.

B. Dasar Hukum Cyber Crime

Sebelum membahas definisi dari tindak pidana cyber crime, terlebih dahulu akan dijabarkan terkait dengan dasar hukum dari cyber crime itu sendiri. Adapun dasar hukum yang mengatur tentang tindak pidana cyber crime adalah sebagai berikut.

1. Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi mengatur beberapa pasal yang memuat tentang perbuatan yang dilarang termasuk tindak pidana cyber crime. Undang-Undang Nomor 36 Thn 1999 tentang Telekomunikasi diberlakukan untuk mengakomodir pemidanaan dari tindak pidana cyber crime, sebelum lahirnya Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun Undang- undang Nomor 36 Tahun 1999 tentang Telekomunikasi ini hanya mengatur beberapa tindak pidana yang termasuk tindak pidana cybercrime yang masih bersifat umum dan luas, dan hanya berkaitan dengan telekomunikasi, sehingga belum dapat mengakomodir tindak-tindak pidana yang berkaitan dengan komputer. Adapun beberapa pasal tersebut yakni sebagai berikut:

Tabel 1 Pengaturan Cyber crime dalam Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Pasal	Materi
Pasal 22	dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi : Akses ke jaringan telekomunikasi; dan atau Akses ke jasa telekomunikasi; dan atau Akses ke jaringan telekomunikasi khusus
Pasal 38	dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan Telekomunikasi
Pasal 40	dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun

Sumber: Undang-Undang Nomor 36 Thn 1999 tentang
Telekomunikasi

Selain dari pasal-pasal tersebut, bentuk-bentuk tindak pidana cyber crime yang disebutkan dalam Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi adalah akses illegal. Akses ilegal yakni tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi, menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi dan penyadapan informasi melalui jaringan telekomunikasi.

2. Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik diundangkan pada tanggal 23 April 2008. Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik memuat dan mengakomodir tentang pengelolaan informasi dan transaksi elektronik untuk pembangunan, dan juga sebagai antisipasi atau payung hukum dari resiko buruk jika terdapat penyalahgunaan kemajuan teknologi informasi dan transaksi elektronik yang dapat merugikan kepentingan hukum baik bagi orang pribadi, masyarakat ataupun negara yang menggunakan alat teknologi atau dengan kata lain yang dapat disebut dengan tindak pidana cyber crime.

Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik telah menetapkan perbuatan-perbuatan mana yang termasuk tindak pidana di bidang cyber crime dan telah ditentukan unsur-unsur tindak pidana dan penyerangan terhadap berbagai kepentingan hukum dalam bentuk rumusan-rumusan tindak pidana tertentu. Adapun pasal-pasal yang mengatur tindak pidana cyber crime adalah sebagai berikut.

Tabel 2 Pengaturan Cyber crime dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Pasal	Materi
Pasal 27 ayat (1)	Dengan sengaja atau tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang

	memiliki muatan yang melanggar kesusilaan
Pasal 27 ayat (2)	Dengan sengaja tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian
Pasal 27 ayat (3)	tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik
Pasal 27 ayat (4)	tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman
Pasal 28 ayat (1)	tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik
Pasal 28 ayat (2)	tanpa hak menyebarkan yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA).
Pasal 29	tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi
Pasal 30 ayat (1)	tanpa hak atau melawan hukum mengakses Komputer dan/atau

	Sistem Elektronik milik Orang lain dengan cara apa pun
Pasal 30 ayat (2)	tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik
Pasal 30 ayat (3)	tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan
Pasal 31 ayat (1)	tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain
Pasal 31 ayat (2)	tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.
Pasal 31 ayat (3)	Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum

	lainnya yang ditetapkan berdasarkan undang - undang
Pasal 32 ayat (1)	tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik public
Pasal 32 ayat (2)	tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak
Pasal 32 ayat (3)	Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya
Pasal 33	tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.
Pasal 34 ayat (1)	tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki: a) perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33

	b) 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
Pasal 34 ayat (2)	Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum
Pasal 35	tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik
Pasal 36	tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.
Pasal 37	dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia

Sumber: Undang-undang Nomor 11 Tahun 2008 Tentang
Informasi Dan Transaksi Elektronik

Berdasarkan penjelasan tersebut, maka pasal yang mengatur secara jelas terkait penyadapan adalah pasal 31 ayat (1) tentang penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, lalu dilanjutkan dengan pasal 31 ayat (2) yakni penyadapan baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan. Lebih lanjut lagi dalam pasal 31 ayat (3) penyadapan diperbolehkan jika dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.

3. Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik merupakan bentuk dari perubahan Undang- undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Namun terkait dengan bentuk-bentuk dari tindak pidana cyber crime yang diatur tidak ada perubahan, sehingga segala bentuk tindak pidana cyber crime masih sama halnya dengan yang diatur dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

C. Bentuk-Bentuk Tindak Pidana Cyber Crime

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur bentuk- bentuk tindak pidana cyber crime yang tercantum dalam psl 27 sampai dengan psl 35 UU No11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, diantaranya yakni.

1. Cybercrime yang menggunakan komputer sebagai alat kejahatan, yakni Pornografi Online (*Cyber- Porno*), Perjudian Online, Pencemaran nama baik melalui media sosial, penipuan melalui komputer, pemalsuan melalui komputer, pemerasan dan pengancaman melalui komputer, penyebaran berita bohong melalui komputer, pelanggaran terhadap hak cipta, cyber terrorism
2. Cybercrime yang berkaitan dengan komputer, jaringan sebagai sasaran untuk melakukan kejahatan, yakni akses tidak sah (*illegal acces*), mengganggu sistem komputer dan data komputer, penyadapan atau intersepsi tidak sah, pencurian data, dan menyalahgunakan peralatan komputer.

Dari penjelasan tersebut dapat ditarik bahwa tindak pidana cybercrime berdasarkan bentuknya dapat dibedakan secara dua garis besar. Pertama, cybercrime yang menggunakan komputer sebagai sarana atau alat dalam melakukan pidana seperti pencemaran nama baik melalui media sosial, penyeberan berita hoax di media masa, dan lain-lain. Sedangkan yang kedua adalah cybercrime dengan komputer sebagai sasaran kejahatan yakni hacking, penyadapan, pencurian data komputer secara ilegal dan lain-lain.

D. Tindak Pidana Carding

1. Pengertian Carding

Tindak pidana *Carding* merupakan bagian dari tindak pidana *cyber crime*, yakni tindak pidana yang menggunakan kartu kredit milik orang lain yang diperoleh secara illegal dan digunakan untuk mengambil keuntungan pribadi.

Tindak pidana *carding* dapat dilakukan dengan beberapa modus kejahatan. Mulai dari pelaku membuat identitas palsu untuk aplikasi kartu kredit samoai dengan membuat kartu kredit palsu yang menggunakan teknologi canggih dalam menerbitkan kartu kredit.⁴⁸Pelaksanaan modus operandi tersebut juga didukung berbagai instrumen seperti skimmer atau software untuk generate nomor kartu kredit dan kesempatan yang relatif terbuka untuk mencuri data dari kartu kredit seperti di hotel, restaurant, card centre dll. sehingga identitas kartu kredit dapat diperoleh dengan mudah.⁴⁹

Penipuan kartu kredit adalah masalah yang sedang menjadi trend di dunia maya modern ini. Jumlah total penipuan kartu kredit pada tahun 1982, termasuk yang melibatkan kartu bank, kartu toko ritel, dan kartu gas, kira-kira satu miliar dolar, dan kerugian tahunan segera bisa mencapai dua miliar dolar.⁵⁰ Tentunya, kerugian ini ditanggung oleh konsumen atau pemegang kartu kredit.

Tindak pidana *carding* merupakan kejahatan yang membawa resiko sangat besar bagi masyarakat, sehingga untuk menyikapi hal tersebut maka penegak hukum diberikan pelatihan untuk menangani kasu-kasus dari teknik

⁴⁸ Sigid Suseno dan Syarif A. Barmawi. *Kebijakan Pegaturan Carding dalam Hkm Pidana di Indonesia*. Jurnal Sosiohumaniora, Vol. 6, No. 3. Hal 253.

⁴⁹ VISA International, 2002. *Credit Card Fraud Trend & Legislation*, Bandung, Hal.13.

⁵⁰ *Journal of Criminal Law and Criminology*, Volume 76, Isuue 3, Article 7, hal. 3

penyelidikan, penyidikan dan pengamanan untuk menangani kejahatan dalam bidang elektronik akan tetapi kemampuan hukum untuk menanggulangi kejahatan mengalami penurunan, hal ini dikarenakan struktur hukum dengan fungsi hukum tidak berkembang secara paralel sehingga penegakan hukum cenderung terus melemah.⁵¹

Adapun beberapa modus yang dapat dilakukan oleh pelaku adalah sebagai berikut.⁵²

- a. *Fraud application;* Menggunakan kartu kredit asli yang diperoleh dengan aplikasi palsu. Pelaku memalsu data pendukung dalam proses aplikasi seperti : KTP, Pasport, rekening koran, Surat Keterangan Pengahsilan dll.
- b. *Non received card;* Menggunakan kartu kredit asli yang tidak diterima oleh pemegang kartu kredit yang sah (berhak) kemudian pelaku membubuhkan tanda tangan di kolom tanda tangan. Kartu kredit diperoleh melalui kurir atau membobol kantos pos bila dikirim melalui Pos.
- c. *Lost/stolen card;* Menggunakan kartu kredit asli hasil curian atau hilang. Pada waktu melakukan transaksi pelaku menandatangani sales draft dan meniru tanda tangan pada kartu kredit atau tanda tangan pemegang kartu yang sah. Transaksi dilakukan di bawah floor limit agar tidak perlu dilakukan otorisasi.
- d. *Altered card;* Menggunakan kartu kredit asli yang sudah diubah datanya. Pelaku menggunakan kartu hasil curian (*lost/stolen, non received, expired card*) dan kartu reliefnya

⁵¹ Mahfud M.D, 2000, *Poitik Hukum Nasional*, Bandung: Alumni . Hal. 35

⁵² Sigid Suseno dan Syarif A. Barmawi. Op.cit. Hal 254

dipanasi dan diratakan kemudian direembossed dengan data baru. Sedangkan *magnetic stripe* diisi data baru dengan *reencoded* yang diperoleh dari *point of compromise* (POC).

- e. *Totally counterfeited*; Menggunakan kartu kredit yang seluruhnya palsu. Pelaku mencetak kartu tiruan dengan menggunakan data nomor dan pemegang kartu yang masih berlaku dengan melakukan *reembossed* dan *reencoded*.
- f. *White plastic card*; Menggunakan kartu plastik polos yang berisi data asli. Pelaku mencetak data dari pemegang kartu kredit yang sah pada plastik polos, tanpa meniru hologram dan logo penerbit. Magnetic stripe diisi dengan data pemegang kartu dengan cara *encoding*.
- g. *Record of charge (Roc) pumping*; Penggandaan sales draft oleh *merchant* (pedagang). Sales draft yang satu tidak ditandatangi oleh pemegang kartu yang sah dan diserahkan kepada merchant lain untuk diisi dengan data transaksi fiktif.
- h. *Altered amount*; Mengubah nilai transaksi pada sales draft oleh *merchant* (pedagang).
- i. *Telephone/mail ordered*; Memesan barang melalui telepon atau surat dengan menggunakan kartu kredit orang lain yang sudah diketahui nama dan nomornya.
- j. Mengubah program *Electronic Data/Draft Capture* (EDC); Mengubah dan merusak program pada alat otorisasi (*electronic data/draft capture/EDC*) milik pengelola oleh *merchant* (pedagang).
- k. *Fictius merchant*. Pelaku berpura-pura menjadi pedagang dengan mengajukan aplikasi disertai dengan data-data palsu.

Sehingga berdasarkan pada beberapa modus yang dapat dilakukan untuk melakukan kejahatan *carding* mulai dari menggunakan aplikasi *hacking* untuk mencuri beberapa data milik pengguna kredit untuk verifikasi, menggunakan kartu kredit curian, bahkan pelaku dapat menggandakan file yang berisikan data transaksi fiktif.

2. Dasar Hukum Carding

Pengaturan tentang tindak pidana *carding* diatur dalam ketentuan perundang-undangan sebagai berikut.

- 1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Carding dapat ditangani dengan beberapa pasal yang ada dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Elektronik. Dalam melakukan tindak pidana *carding*, pelaku dapat melakukan *hacking* untuk mendapatkan beberapa data dan informasi yang akan digunakan pelaku untuk mengambil keuntungan.

Sehingga hal tersebut dapat diberat dengan pasal 31 ayat (1) Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Elektronik yang menyatakan "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronika dan atau dokumen elektronik dalam suatu komputer dan atau sistem elektronik secara tertentu milik orang lain".

Dan pasal 31 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Elektronik yang menyatakan Setiap orang dengan sengaja atau tanpa hak

atau melawan hukum melakukan intersepsi atau transmisi elektronik dan atau dokumen elektronik yang tidak bersifat publik dari, ke dan di dalam suatu komputer dan atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan, penghilangan dan atau penghentian informasi elektronik dan atau dokumen elektronik yang ditransmisikan.

3. Penindakan Hukum Pidana terhadap Carding

Tindak pidana *carding* dapat dikaitkan dengan pasal pencurian, tindak pidana pemalsuan dan pidana penipuan yang terdapat dalam Kitab Undang- Undang Hukum Pidana yakni dalam pasal sebagai berikut.⁵³

- a. Pasal 362 KUHP yang menyatakan "Barang siapa mengambil suatu benda yang seluruhnya atau sebagian milik orang lain, dengan maksud untuk dimiliki secara melawan hukum".
- b. Pasal 378 KUHP "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain dengan melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat ataupun dengan rangkaian kebohongan menggerakkan orang lain untuk menyerahkan sesuatu benda kepadanya, atau supaya memberi hutang maupun menghapuska piutang."

Sehingga sebelum lahirnya Undang- undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, para penegak hukum menggunakan pasal 362 dan pasal 378 KUHP

⁵³ Kurniawan. 2006. Penegakan Hukum Tindak Pidana Kartu Kredit. Skripsi. Unair di akses 01 april 2019 pukul 20.00 WIB

untuk menjerat pelaku, namun tentunya karakteristik dari tindak pidana carding yang menggunakan teknologi berbeda dengan tindak pidana konvensional.

BAB IV

MEKANISME SANKSI DAN PENYELESAIAN SENGKETA TRANSAKSI ELEKTRONIK

A. Bentuk - bentuk sengketa dalam transaksi elektronik

Dengan maraknya perkembangan *e-commerce* di Indonesia saat ini selain memberikan kemudahan, terdapat aspek negatif dari pengembangannya, yaitu berkaitan dengan persoalan keamanan dalam bertransaksi dengan menggunakan media *e-commerce*. Saat ini telah banyak muncul bentuk penyelewengan yang cenderung merugikan konsumen dan menimbulkan berbagai permasalahan

hukum dalam melakukan transaksi *e-commerce*.⁵⁴

Di dalam jual beli melalui internet, seringkali terjadi kecurangan. Kecurangan tersebut dapat menyangkut keberadaan pelaku usaha, barang yang dibeli, harga barang, dan cara pembayaran oleh konsumen seperti kecurangan yang menyangkut barang yang dikirimkan oleh pelaku usaha, misalnya barang tersebut tidak dikirimkan kepada konsumen atau terjadi keterlambatan pengiriman yang berkepanjangan, terjadi kerusakan atas barang yang dikirimkan atau barang yang dikirimkan cacat, dan lain sebagainya. Yayasan Lembaga Konsumen Indonesia (YLKI) mencatat pada 2017 terdapat 23.229 pengaduan konsumen. Dari total 642 pengaduan umum, persentase tertinggi terdapat pada belanja online sebesar 16%. Staff bidang Pengaduan Konsumen dan Hukum YLKI Abdul Baasith juga memaparkan tren pengaduan belanja onlinemengalami kenaikan

⁵⁴ Tetanoe Bernada, "Upaya Perlindungan Hukum Pada Konsumen Dalam Transaksi E-commerce Untuk Mendukung Pertumbuhan Ekonomi Digital Di Indonesia", Jurnal Hukum Dan Peradilan, Uph, Banten Vol. 6 No.1 (Maret 2017), h., 4.

signifikan selama lima tahun terakhir, bahkan naik 100 persen dari tahun 2016 yang hanya menyumbang 8% angka pengaduan. Abdul Baasith juga menyebutkan dari 101 pengaduan, toko online yang paling banyak dikeluhkan konsumen adalah Lazada sebesar yaitu adanya 18 aduan, Akulaku sebanyak 14 aduan, Tokopedia sebnayka 11 aduan, Bukalapak sebanyak 9 aduan, Shopee sebanyak tujuh aduan, Blibli sebanyak lima aduan, JD.ID sebanyak empat aduan, Elevania sebanyak tiga aduan, dan sisanya dari media sosial serta blog pribadi. 36 persen konsumen mengeluhkan barang tidak sampai. Konsumen juga banyak yang mengeluhkan lambatnya respons komplain dari pelaku usaha dan ada yang melaporkan karena dugaan penipuan. Banyaknya keluhan konsumen *e-commerce* karena sikap dari beberapa pelaku usaha di situs belanja *online* kurang kooperatif dalam merespons pengaduan, bahkan akunnya seperti diblokir sehingga akses untuk mengajukan keluhan seperti live chat tidak bisa digunakan.⁵⁵

Adapun YLKI adalah lembaga yang berwenang menerima pengaduan konsumen yang dirugikan, khusus untuk penyelesaian sengketa konsumen, wewenang dapat diselesaikan melalui pengadilan (*litigasi*) dan diluar pengadilan (*non-litigasi*) yaitu melalui BPSK sesuai dengan amanat UUPK Pasal 49:

“Pemerintah membentuk badan penyelesaian sengketa konsumen di Daerah Tingkat II untuk penyelesaian sengketa konsumen di luar pengadilan.”

Pada dasarnya aturan yang mengatur *e-commerce* adalah Undang-Undang Informasi dan Transaksi Elektronik, karena pada

⁵⁵ <https://economy.okezone.com/read/2018/01/19/320/1847340/pengaduan-ytki-2017-paling-banyak-belanja-online?page=1> Diakses tanggal 24 Desember 2022 pukul 11.22 WIB

pelaksanaannya *e-commerce* adalah hubungan perikatan konsumen dengan pelaku usaha melalui media media elektronik atau internet, sehingga kesepakatan ataupun kontrak yang tercipta adalah melalui media online/elektronik. Hampir sama dengan jual- beli konvensional yang dilakukan oleh masyarakat, jual-beli yang dilakukan masyarakat pada umumnya (*konvensional*) yaitu terdiri dari penawaran dan penerimaan sebab suatu kesepakatan selalu diawali dengan adanya penawaran oleh salah satu pihak dan penerimaan oleh pihak lainnya. Namun terdapat banyaknya kerugian yang dialami dan tidak pastinya Undang-Undang yang mengatur terkait penyelesaian sengketa transaksi *e-commerce* secara khusus membuat konsumen tidak mengetahui bagaimana cara berikut prosedur penyelesaiannya.

Bagaimanapun juga pembeli dalam transaksi *e-commerce* juga merupakan konsumen, maka hak-hak nya terdapat pada Undang-Undang Perlindungan Konsumen termasuk bagaimana konsumen *e-commerce* dapat menyelesaikan sengketa atas kerugian yang dialami. Tahun 2015 terdapat 130 kasus sengketa yang sudah terselesaikan di BPSK, Pada tahun 2016 terdapat 90 kasus yang telah selesai dari 216 pengaduan, tahun 2017 terdapat 139 pengaduan sebanyak 54 pengaduan bisa diselesaikan, pada tahun 2018 terdapat 121 total aduan dan 51 yang telah diselesaikan.⁵⁶

B. Perbuatan yang dilarang dalam UU ITE

UU No. 19 Tahun 2016 tentang Perubahan UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menjelaskan secara rinci apa saja perbuatan yang dilarang. Bagi mereka yang melanggar UU

⁵⁶ *Ibid*

ITE berpotensi mendapat hukuman berupa denda hingga kurungan penjara. Berikut beberapa perbuatan yang dilarang UU ITE:

1. Menyebarluaskan Video Asusila

Perbuatan pertama yang dilarang dalam UU ITE adalah orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan. Ini diatur dalam pasal 27 ayat (1) UU ITE. Setiap orang yang melanggar kesusilaan sebagaimana dimaksud dalam pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

2. Judi Online

Selanjutnya, pasal 27 ayat (2) UU ITE memuat larangan perbuatan yang bermuatan perjudian. Hukuman untuk mereka yang melanggar adalah dipidana dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

3. Pencemaran Nama Baik

Pasal 27 ayat (3) UU ITE juga mengatur tentang pencemaran nama baik. Pelaku yang dijerat dengan pasal ini bakal dipidana dengan pidana penjara paling lama 4 tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah). Selanjutnya pada revisi UU No. 19 Tahun 2016, dijelaskan bahwa ketentuan pada pasal 27 ayat (3) merupakan delik aduan.

4. Pemerasan dan Pengancaman

Orang yang melakukan pemerasan dan pengancaman juga berpeluang dijerat pasal 27 ayat (4) UU ITE. Hukumannya

adalah dipidana dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

5. Berita Bohong

Berita bohong juga dilarang dalam pasal 28 ayat (1) UU ITE yang berbunyi bahwa setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik. Bagi para pelaku penyebar berita bohong bakal dipidana dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

6. Ujaran Kebencian

Orang yang menyebarkan informasi dengan tujuan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA) juga merupakan perbuatan yang dilarang dalam pasal 28 ayat (2) UU ITE. Hukuman pelaku ujaran kebencian sebagaimana dijelaskan pada pasal 28 ayat (2) adalah dipidana dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

7. Teror Online

Pada pasal 29 UU ITE mengatur perbuatan teror online yang dilarang. Pasal ini bakal menjerat setiap orang dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi. Hukuman bagi pelaku teror online yang bersifat menakut-nakuti orang lain

dengan adalah pidana penjara paling lama 4 tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).

Perbuatan Lain yang Dilarang UU ITE

1. Mengakses, mengambil, dan meretas sistem elektronik milik orang lain dengan cara apapun (pasal 30)
2. Melakukan intersepsi atau penyadapan terhadap sistem elektronik milik orang lain dari publik ke privat dan sebaliknya (pasal 31)
3. Mengubah, merusak, memindahkan ke tempat yang tidak berhak, menyembunyikan informasi atau dokumen elektronik, serta membuka dokumen atau informasi rahasia (pasal 32)
4. Mengganggu sistem elektronik (pasal 33)
5. Menyediakan perangkat keras atau perangkat lunak, termasuk sandi komputer dan kode akses untuk pelanggar larangan yang telah disebutkan (pasal 34)
6. Pemalsuan dokumen elektronik dengan cara manipulasi, penciptaan, perubahan, penghilangan, dan pengrusakan (pasal 35).

C. Alternatif Penyelesaian Sengketa (Alternative Dispute Resolution (ADR))

Transaksi e- di dunia maya dimungkinkan terjadi sengketa seperti halnya sengketa yang terjadi dalam suatu hubungan hukum yang dilakukan secara konvensional. Semakin banyak dan luas kegiatan perdagangan, maka frekuensi terjadinya sengketa semakin tinggi, hal ini berarti akan banyak sengketa yang harus diselesaikan.

Sengketa ini dapat terjadi karena adanya wanprestasi maupun perbuatan melawan hukum.⁵⁷

Sengketa-sengketa tersebut dapat diselesaikan melalui proses litigasi maupun non litigasi. Namun demikian, sebagaimana telah disebutkan sebelumnya, bahwa *e-commerce* dilahirkan dengan maksud untuk meniadakan hambatan dalam model transaksi bisnis yang konvensional berupa pertemuan langsung, sehingga dibatasi oleh waktu dan tempat, serta diperlukan nya kertas-kertas sebagai suatu dokumen. Model *e-commerce* dalam transaksi bisnis secara dapat dilakukan secara non face dan non sign. Oleh karena itu, model penyelesaian sengketa yang terlalu banyak memakan waktu, biaya dan terlalu banyak formalitas-formalitas pada hakikatnya merupakan suatu model penyelesaian sengketa yang tidak diharapkan dalam *e-commerce*. Sebaliknya *e-commerce* justru mengharapkan penyelesaian sengketa yang lebih cepat, murah dan tidak terlalu banyak formalitas-formalitas.

Penyelesaian sengketa sendiri pada dasarnya dapat dikualifikasikan menjadi penyelesaian sengketa secara damai dan penyelesaian sengketa secara adversarial. Penyelesaian sengketa secara damai lebih dikenal dengan penyelesaian secara musyawarah mufakat. Sementara penyelesaian sengketa secara adversial lebih dikenal dengan penyelesaian sengketa oleh pihak ketiga yang tidak terlibat dalam sengketa. Dalam penyelesaian sengketa secara damai tidak ada pihak yang mengambil keputusan bagi penyelesaian sengketa. Keterlibatan pihak ketiga dalam penyelesaian sengketa secara damai adalah dalam rangka mengusahakan agar para pihak yang bersengketa dapat sepakat untuk menyelesaian sengketa

⁵⁷ Rahadi Wasi Bintoro, "Tuntutan Hak Dalam Persidangan Perkara Perdata", Jurnal Dinamika Hukum, Vol. 10 No. 2, mei 2010, Purwokerto: FH Unsoed, hlm. 156.

mereka. Bentuk dari penyelesaian sengketa secara damai adalah negosiasi, mediasi dan konsiliasi. Negosiasi adalah penyelesaian sengketa secara damai dimana para pihak ber-hadapan langsung tanpa ada keikutsertaan dari pihak ketiga. Sementara mediasi dan konsiliasi adalah penyelesaian sengketa secara damai dimana ada turut campur pihak ketiga. Perbedaan antara konsiliasi dan mediasi terletak pada aktif tidaknya pihak ketiga dalam mengusahakan para pihak untuk menyelesaikan sengketa. Penyelesaian sengketa secara damai, apabila dilihat dari sifatnya, maka penyelesaian ini merupakan hal yang ideal mengingat keadilan muncul dari para pihak.

Mediasi menjadi salah satu bentuk penyelesaian yang dipilih oleh para pihak yang bersengketa dalam sengketa e-commerce. Melalui mediasi pihak ketiga yang netral akan duduk bersama-sama dengan para pihak yang bersengketa dan secara aktif akan membantu para pihak dalam upaya menemukan kesepakatan yang adil dan memuaskan bagi keduanya. Dalam proses mediasi, seorang mediator hanya berperan sebagai fasilitator saja. Mediator tidak mempunyai kewenangan untuk membuat suatu keputusan yang mengikat para pihak. Seorang mediator akan membantu para pihak yang bersengketa untuk mengidentifikasi persoalan-persoalan yang menjadi pokok sengketa, memfasilitas komunikasi di antara kedua belah pihak.

Bentuk Alternatif Penyelesaian Sengketa (APS) lainnya adalah negosiasi yang pada dasarnya dilakukan pada saat proses persidangan. Hal ini dikarenakan, dalam proses persidangan berlaku prinsip hakim bersifat pasif, dimana terkandung arti bahwa para pihak dapat mengakhiri sengketa kapan pun dan hakim tidak boleh menghalang-halangnya. Negosiasi sendiri suatu proses di mana

para pihak berupaya untuk menyelesaikan sengketa yang timbul secara informal, dengan atau tanpa pihak lain mewakilinya.⁵⁸

Sengketa *e-commerce* yang cenderung terjadi berkaitan dengan masalah harga, kualitas barang dan jangka waktu pengiriman. Produk yang menjadi obyek sengketa, apabila jumlahnya (harga maupun kuantitas) relatif kecil, maka para pihak cenderung tidak memerlukan bantuan pihak ketiga untuk penyelesaiannya. Hal ini wajar, mengingat biaya yang harus di-keluarkan untuk membayar jasa pihak ketiga akan lebih besar daripada obyek sengketa. Dalam hal sengketa yang nilainya relatif kecil (dari segi harga maupun kuantitas), proses negosiasi dilakukan secara langsung antara penjual dan pembeli, baik melalui pertemuan secara fisik (*face to face*), apabila domisili keduanya salingberdekatan maupun melalui surat-menyurat (*e-mail*), jika kedua pihak berjauhan.

Mekanisme Penyelesaian sengketa melalui konsiliasi (*conciliation*) juga merupakan suatu proses penyelesaian sengketa yang melibatkanpihak ketiga yang netral dan tidak memihak. Seperti juga pada tugas seorang mediator, tugas dari konsiliator hanyalah sebagai fasilitator untuk melakukan komunikasi di antara para pihak sehingga pada akhirnya solusi akan dihasilkan oleh para pihak itu sendiri. Dalam proses konsiliasi, pihak ketiga yang akan membantu, telah membawa usulan penyelesaian, sehingga berperan lebih aktif dalam mengarahkan para pihak untuk sampai pada kesimpulan penyelesaiansengketa yang dapat disepakati para pihak. Dalam melakukan proses konsiliasi, seorang konsiliator harus mampu mengetahui situasi dan kondisi kasus tersebut, mengetahui apa yang

⁵⁸ Lihat juga M Husni, "Arbitrase Sebagai Alternatif Penyelesaian Sengketa Bisnis di Luar Pengadilan", Jurnal E-quality, Vol. 13 No. 1, Februari 2008, Medan: Fakultas Hukum USU, hlm. 11-12.

menjadi keinginan para pihak yang bersengketa serta mengetahui kebutuhan para pihak agar sengketa dapat diselesaikan secara cepat.

Perlu ditegaskan disini, bahwa penyelesaian sengketa secara damai menuntut adanya kesukarelaan dari pihak-pihak yang bersengketa. Tanpa adanya kesukarelaan diantara para pihak, tidak mungkin penyelesaian sengketa secara damai berjalan.

D. Online Dispute Resolution (ODR)

Untuk mempermudah penyelesaian sengketa dalam *e-commerce*, dalam perkembangannya muncul alternatif penyelesaian sengketa secara online (*online dispute resolution/ODR*).⁵⁹

Dalam hal ini ODR merupakan alternatif penyelesaian sengketa bisnis di luar pengadilan yang menggunakan internet sebagai media untuk menyelesaikan sengketa yang terjadi antara para pihak. Pada dasarnya mekanisme yang ditempuh dalam penyelesaian sengketa melalui ODR pada prinsipnya sama dengan arbitrase secara konvensional, yang membedakan hanyalah tempat dan media penyelesaian sengketa yang digunakan. Dalam keadaan tertentu pun, demi kelancaran jalannya penyelesaian sengketa, ODR dapat mempertemukan para pihak yang bersengketa. Sebagai contoh ODR adalah *The Virtual magistre* yang dilahirkan oleh para akademisi hukum dunia maya yang bekerja untuk

National Center for Automated Information Research (NCAIR) dan *Cyberspace Institute* yang didirikan oleh asosiasi arbitrase Amerika. Arbitrase online bekerja seperti persida-ngan, di mana arbitrator bertindak seperti hakim yang didahului dengan

⁵⁹ Bambang Sutiyoso, "Penyelesaian Sengketa Bisnis Melalui online Dispute Resolution dan Pemberlakunya di Indonesia", Mimbar Hukum, Vol. 20 No. 2, Juni 2008, Yogyakarta: FH UGM, hlm. 232-234.

mendengarkan keterangan kedua belah pihak dan kemudian menjatuhkan putusan. Namun demikian, putusan yang dihasilkan dari ODR yang ada menekankan bahwa putusan yang dijatuhkan dapat bersifat mengikat ataupun tidak mengikat tergantung pada kesepakatan kedua belah pihak.⁶⁰ Teknis penyelesaian sengketanya dilakukan secara *online* dengan menggunakan media *e-mail*, *video conferencing*, *radio button elektronic fund transfer*, *web conference*, maupun *online chat*.⁶¹

Penyelesaian sengketa melalui ODR terdapat kelemahan, di mana arbitrator tidak dapat melihat sengketa yang sebenarnya karena hanya mendasarkan pada teks di *e-mail* atau media internet lainnya.

⁶⁰ Ibid., hlm. 238

⁶¹ Fakih Fahmi Mubarok, 2006, Tinjauan Hukum Penyelesaian Sengketa Perkara Melalui Arbitrase Online Berdasarkan Undang-undang No. 30 Tahun 1999, makalah, Yogyakarta: Fakultas Hukum UII, hlm. 4.

BAB V

CYBER CRIME SEBAGAI KEJAHATAN TRANSNASIONAL SERTA PEMBERANTASAN DAN PENANGANAN CYBERCRIME MELALUI PERLUASAN ALAT BUKTI

A. Pengertian Kejahatan Transnasional

Cyber crime merupakan suatu kejahatan yang dapat dikatakan sebagai kerjahatan baru, karena kejahatan siber memiliki karakteristik yang sangat khusus jika dibandingkan 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*".⁶²

Dengan memperhatikan jenis-jenis *cyber crime* yang dibahas pada bab sebelumnya dapat digambarkan bahwa *cyber crime* memiliki ciri-ciri khusus, yaitu (1) tanpa kekerasan, (2) sedikit melibatkan kontak fisik, (3) menggunakan peralatan, (4) memanfaatkan jaringan telematika (telekomunikasi, media, dan informatika) global. Melihat cirri ke 3 dan 4, terlihat jelas *cyber crime*

⁶² Dikdik, Elisatris, Op., Cit., hlm.25.

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 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. Sifanya 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 yurisdiksi, 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.

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

1. Prinsip Teritorial, Dapat menerapkan yurisdiksi 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 dilaksanakan 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 suatu 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

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 bertentangan dengan kepentingan masyarakat secara luas.

Secara garis besar, yurisdiksi dapat dibedakan menjadi dua yaitu pertama adalah yurisdiksi perdata dimana kewenangan hukum suatu negara terdapat obyek perkara dalam yang di dalamnya dalam lingkup hukum privat yang memiliki 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 berkewajiban untuk berkolaborasi dengan negara lain untuk dapat menuntut 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 yurisdiksi di dunia mayantara (*cyberspace*); hal ini muncul karena sulitnya untuk menetapkan diwilayah mana dunia mayantara (*cyberspace*) dapat dikenai yurisdiksi. Menghadapi masalah yurisdiksi di dunia mayantara ini serta mem perhatikan 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, Domestically and Regionally di Portland, Oregon, Amerika Serikat, tanggal 19-23 Maret 1994.*⁶³

C. Yurisdiksi Hukum Pidana Indonesia dalam Cybercrime

Tindak pidana siber merupakan salah satu kejahatan tarsnasional 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 payung hukum terkait 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

⁶³ Ibid, halaman 26

wilayah hukum 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 dilakukan 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 nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan 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 tersebut 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 kedaulatan 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. Penegakan Hukum Tindak Pidana *Cybercrime*

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.⁶⁴ Aparat penegak

⁶⁴ Satjipto Rahardjo, *Penegakan Hukum Suatu Tinjauan Sosiologis*, Genta Publishing, Cetakan 1, Yogyakarta, 2009, hlm. 24.

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 tantangan yang dihadapi oleh aparat penegak hukum bukan tidak mungkin sangatlah banyak Penegak hukum tidak hanya dituntut untuk professional dan tepat dalam menerapkan normannya akan tetapi juga dituntut dapat membuktikan kebenaran atas dakwaan kejahatan yang terkadang

dipengaruhi oleh rangsangan dari prilaku masyarakat 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:⁶⁵

1. Faktor hukumnya sendiri, yaitu peraturan perundang-undangan yang berlaku di Indonesia.
2. Faktor penegak 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 penegakan 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 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

⁶⁵ Soerjono Soekanto, *Faktor-faktor yang Mempengaruhi Penegak Hukum*, Rajawali Pers, Cetakan 13, Jakarta, 2014, hlm. 8.

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.⁶⁶

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 kejahtaan yang sering sekali sulit untuk dibuktikan sehingga hal tersebut menjadi tantangan tersendiri dalam penegakan hukum tindak pidana *cybercrime*.

Setiap penegak hukum diberi kewenangan berdasarkan Peraturan Perundang-undangan yang berlaku untuk menjelaskan

⁶⁶ 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.

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-undang Nomor 11 tahun 2008. Dalam Pasal 42 UU Undang-undan Nomor 11 tahun 2008 disebutkan : Penyidikan terhadap tindak pidana sebagaimana 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 generalis, 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. Ketentuan 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 lainnya, 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-patrolling* 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 pidana 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 diberikan 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 jasadan penyelenggara sistem elektronik mengenai data-data yang berhubungan dengan tindak pidana, dengan tetap terikat terhadap privasi, kerahasiaan, 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.

E. 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 sahmenurut 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 dihadapan pengadilan, keterangan satu orang saksi tidak cukup menjadikan keterangan tersebut sebagai bukti, karena satu orang saksi tidak bisa dianggap sebagai bukti sehingga harus disertai dengan 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 168KUHAP yang pada pokoknya 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, iaraskan, 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 diIndonesia 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 diperlukan 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, iaberwenang 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 perundangan undangan atau surat yang dibuat oleh pejabat mengenai hal yang termasuk dalam tata laksana 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 petunjuk 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 memilih 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 sebagaimana dari perbuatan atau keadaan.

F. 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 rationnee* 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 negatif *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 bertumpu 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,

jugamenggunakan 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 (*doublen 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. Sehingga pembuktian tidak hanya ditujukan untuk menjatuhkan pidana saja berdasarkan syarat minimal dua alat bukti yang harus dipenuhi dalam hal pembuktian untuk menjatuhkan pidana.

G. Alat Bukti Elektronik dalam Cyber Crime

Berbicara mengenai pembuktian secara elektronik, tidak terlepas dari alat-alat elektronik 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 di pertanggung jawabkan 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, menjadi tidak tertulis dan bersifat on-line. Alat bukti surat dalam sistem komputer ada dua kategori :

- a. Bila sebuah sistem komputer yang telah disertifikasi oleh badan yang berwenang maka hasil print 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 apa 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 ke arah 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 dapat dialihkan atau ditransformasikan) 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 :

- a. Dokumen perusahaan dapat dialihkan ke dalam *microfilm* atau media lainnya.
- b. 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.
- c. Dalam mengalihkan dokumen perusahaan sebagaimana 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.
- d. 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 pendukung 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 International 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 Karsipan yang menyatakan bahwa suatu informasi elektronik tetap diakui, karena definisi karsipan 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.

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

KAJIAN UMUM TENTANG DATA PRIBADI DAN PERLINDUNGAN HUKUMNYA

A. Pengertian Data Pribadi

Menurut Kamus Besar Bahasa Indonesia pengertian data adalah keterangan yang benar dan nyata yang dapat dijadikan dasar kajian.⁶⁷ Sedangkan Pribadi sendiri memiliki arti manusia sebagai perseorangan (diri manusia atau diri sendiri),⁶⁸ sehingga dapat disimpulkan bahwa data pribadi merupakan keterangan yang benar dan nyata yang dimiliki oleh manusia sebagai perseorangan.

UU ITE tidak memberikan definisi hukum yang jelas tentang data pribadi. Akan tetapi, dilihat dari prespektif penafsiran resmi tentang hak pribadi (*privacy right*) dalam Pasal 26 ayat (1), maka data pribadi meliputi urusan kehidupan pribadi termasuk (riwayat) komunikasi seseorang dan data tentang seseorang.⁶⁹

Dalam PP No. 82 Tahun 2012 tentang Penyelenggara Sistem dan Transaksi Elektronik, mendefinisikan data pribadi yaitu “*data perseorangan tertentu yang disimpan, dirawat, dijaga kebenaran serta dilindungi kerahasiaannya*” (Pasal 1 ayat 27).

Menurut penjelasan Pasal 1 ayat 1 Data Protection Act Inggris tahun 1998 menentukan bahwa:

⁶⁷ KBBI. “Pengertian Data”. <https://kbbi.web.id/data> diakses pada 03 Desember 2019 Pukul 16.00

⁶⁸ KBBI. “Pengertian kata Pribadi”. <https://kbbi.web.id/pribadi> pada 03 Desember 2019 Pukul 21.30 WIB

⁶⁹ Diani Supriyadi. 2017. “Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya”. <https://www.hukumonline.com/berita/baca/lt59cb4b3feba88/data-pribadi-dan-dua-dasar-legalitas-pemanfaatannya-oleh--daniar-supriyadi/>. Diakses pada 16 Maret 2020. Pukul 18.04 WIB.

“Data adalah setiap informasi yang diproses melalui peralatan yang berfungsi secara otomatis menanggapi instruksi-instruksi yang diberikan bagi tujuannya dan disimpan dengan maksud untuk dapat diproses. Data juga termasuk informasi yang merupakan bagian tertentu dari catatancatatan kesehatan, kerja sosial, pendidikan atau yang disimpan sebagai bagian dari suatu sistem penyimpanan yang relevan.”

Diterangkan juga dalam Data Protection Act Inggris tahun 1998 bahwa data pribadi adalah data yang berhubungan dengan seseorang individu yang hidup yang dapat diidentifikasi dari data atau dari data-data atau informasi yang dimiliki atau akan dimiliki oleh data controller. Selain itu data pribadi juga dapat dikaitkan dengan ciri responden contohnya jenis kelamin, umur, nama dan lain-lain.

Menurut peraturan menteri Data Pribadi adalah Data Perseorangan Tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Secara umum data pribadi terdiri atas fakta-fakta yang berkaitan dengan individu yang merupakan informasi sangat pribadi sehingga orang yang bersangkutan ingin menyimpan untuk dirinya sendiri dan/atau membatasi orang lain untuk menyeirkannya kepada pihak lain maupun menyalahgunakannya. Secara khusus, data pribadi menggambarkan suatu informasi yang erat kaitannya dengan seseorang yang akan membedakan karakteristik masing-masing individu.⁷⁰ Menurut Pasal 1 Ayat (1) RUU Perlindungan data pribadi memberikan definisi tentang data pribadi yaitu :

“Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau

⁷⁰ Jerry Kang, 1998, Information Privacy in Cyberspace Transaction, Stanford Law Review Vol. Issue 4, Standford, h. 5.

dikombinasikan dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik”⁷¹

Adapun jenis data dalam RUU Perlindungan data pribadi terdapat dua pengelompokan yaitu data prinadi yang bersifat umum dan yang bersifat spesifik hal ini tertera dalam pasal 3 ayat (1-3) RUU Perlindungan data pribadi. Data bersifat umum meliputi: nama lengkap, jenis kelamin, kewarganegaraan, agama, dan/atau Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang. Sedangkan yang bersifat spesifik meliputi :⁷²

1. data dan informasi kesehatan;
2. data biometrik;
3. data genetika;
4. kehidupan/orientasi seksual;
5. pandangan politik;
6. catatan kejahatan;
7. data anak;
8. data keuangan pribadi; dan/atau
9. data lainnya sesuai dengan ketentuan peraturan perundang-undangan.

B. Dasar Hukum Perlindungan Data Pribadi

1. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi
2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah kedalam

⁷¹ Pasal 1 Ayat (1) RUU Perlindungan Data Pribadi

⁷² Pasal 3 Ayat (1-3) RUU Perlindungan Data pribadi

Undang-Undang Nomor 19 Tahun 2016 Informasi dan Transaksi Elektronik

3. Undang-Undang Nomor 7 Tahun 1971 tentang Ketentuan Pokok Karsipan
4. Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan
5. Undang-Undang nomor 36 Tahun 1999 tentang Telekomunikasi
6. Undang-Undang nomor 23 Tahun 2006 tentang Administrasi Kependudukan

Apabila membahas soal dasar hukum perlindungan data pribadi bahwasannya secara umum perlindungan data pribadi sudah terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang kemudian diubah menjadi Undang-Undang Nomor 19 Tahun 2016. Selain itu terdapat juga dalam Rancangan Undang-Undang Perlindungan Data Pribadi yang sampaui saat ini masih dalam proses pembentukan. Perlindungan hukum itu sendiri adalah segala upaya pemenuhan hak dan pemberian bantuan untuk memberikan rasa aman kepada saksi dan/atau korban, perlindungan hukum korban kejahanan sebagai bagian dari perlindungan masyarakat, dapat diwujudkan dalam berbagai bentuk, seperti melalui pemberian restitusi, kompensasi, pelayanan medis, dan bantuan hukum.⁷³

Perlindungan hukum yang diberikan kepada subyek hukum ke dalam bentuk perangkat baik yang bersifat preventif maupun yang bersifat represif, baik yang lisan maupun yang tertulis. Dengan kata lain dapat dikatakan bahwa perlindungan hukum sebagai suatu gambaran tersendiri dari fungsi hukum itu sendiri, yang memiliki

⁷³ Soerjono Soekanto, Pengantar Penelitian Hukum, Ui Press. Jakarta, 1984, hlm 133.

konsep bahwa hukum memberikan suatu keadilan, ketertiban, kepastian, kemanfaatan dan kedamaian.

Menurut Philipus M. Hadjon Perlindungan Hukum adalah Sebagai kumpulan peraturan atau kaidah yang akan dapat melindungi suatu hal dari hal lainnya. Berkaitan dengan konsumen, berarti hukum memberikan perlindungan terhadap hak-hak pelanggan dari sesuatu yang mengakibatkan tidak terpenuhinya hak-hak tersebut.⁷⁴

Dalam beberapa pasal UU ITE sudah memberikan perlindungan hukum terkait data pribadi pasal 26 contohnya. Dalam pasal tersebut telah ditegaskan bahwa penggunaan informasi elektronik apapun di media harus dengan persetujuan pemilik data tersebut.

Apabila dikaitkan kepada perbuatan yang dilarang maka UU ITE sudah melarang perbuatan memperoleh informasi dengan cara apapun sebagaimana yang tertera dalam pasal 30 khususnya pada ayat (2). Ketika pelanggaran itu dilakukan maka dapat dikenakan sanksi pidana berupa pidana penjara maksimal 7 tahun dan denda maksimal Rp 700.000.000,- (Tujuh ratus juta rupiah). Hal ini berdasarkan pasal 46 ayat (2) UU ITE yang telah tertulis sehingga dengan adanya peraturan ini data pribadi seseorang sudah memiliki payung hukum dan dilindungi oleh hukum.

Sebagaimana kewajiban sebagai penyelenggara layanan aplikasi yaitu menjaga kerahasiaan serta keamanan dari informasi elektronik yang dikelolanya. Hal ini sesuai dengan pasal 15 ayat (1) karena apabila penyelenggara aplikasi tidak dapat menjaga data yang dikelolanya dapat dikenakan sanksi administratif sesuai Pasal 84 ayat

⁷⁴ Philipus M. Hadjon, Perlindungan Bagi Rakyat diIndonesia, PT.Bina Ilmu, Surabaya,1987,h. 1-2.

(1) dan (2) PP No 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Penyelenggara layanan aplikasi juga harus mematuhi UU ITE dan Juga seluruh perundang-undangan terkait yang berlaku di Indonesia hal ini juga dipertegas oleh Surat Edaran dari KOMINFO Nomor 3 Tahun 2016 terkait Penyediaan Layanan Aplikasi dan/atau Konten Melalui Internet.

Dalam RUU Perlindungan Data Pribadi Juga khususnya di Pasal 20 ayat (1) menjelaskan bahwa pengelola data atau penyelenggara aplikasi wajib mencegah data pribadi yang diakses secara tidak sah. Larangan hal tersebut juga tertera dalam pasal 51 ayat (1) yang berbunyi :

“Setiap Orang dilarang memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian Pemilik Data Pribadi.”⁷⁵

Sehingga dari sinilah terdapat dasar hukum perlindungan data pribadi yang tersebar di beberapa peraturan perundang-undangan.

C. Prinsip Perlindungan Data Pribadi

Dikutip dari skripsi milik Rizkia Nurdinisari,³⁶ dijelaskan bahwa terdapat *Basic Principles Of National Application* (Implementasi Nasional atas Prinsip-prinsip Dasar), yang dimana beberapa prinsipnya adalah :

1. *Use Limitation Principle* (Prinsip Pembatasan Penggunaan Data)
Prinsip ini menjelaskan tentang data pribadi yang tidak boleh

⁷⁵ Pasal 50 Ayat (1) RUU Perlindungan Data Pribadi

diungkapkan, disediakan atau digunakan untuk tujuan selain yang ditentukan kecuali dengan persetujuan dari pemilik data atau oleh otoritas hukum.

2. *Security Safeguards Principle* (Prinsip Perlindungan Keamanan Data) Prinsip ini menjelaskan tentang keharusan dalam melindungi data pribadi dengan penjagaan keamanan yang wajar terhadap risiko seperti kehilangan atau akses, perusakan, penggunaan, modifikasi atau pengungkapan data yang tidak sah.

Selain itu kewajiban penyelenggara Aplikasi untuk menjaga keamanan data juga tercantum dalam Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Prinsip Tanggung Jawab Mutlak atau disebut Prinsip Tanggung Jawab Absolute (*Absolute Liability*), dan *Strict Liability* juga harus dipahami dengan seksama. Namun beberapa ahli menilai bahwa dua istilah tersebut merupakan istilah yang berbeda.⁷⁶

Ada yang beranggapan bahwa Strict Liability merupakan prinsip tanggung jawab yang tidak melihat kesalahan sebagai faktor utama namun, ada pengecualian sebagaimana *force majeur*. Selain itu ada juga yang beranggapan bahwa Absolute liability merupakan prinsip tanggung jawab tanpa pengecualian sehingga apapun alasannya memang pelaku usaha harus bertanggung jawab atas apa yang sudah diproduksi atau disebarluaskan apabila menimbulkan dampak kerugian.

⁷⁶ Celina Tri Siwi Kristiyanti. 2009. "Hukum Perlindungan Konsumen". Sinar Grafika, Jakarta. Hal 96.

Dikutip dari buku milik Celina Tri Siwi Kristiyanti,⁷⁷ Menurut R.C. Horber *et.al.*, berpendapat biasanya tanggung jawab mutlak ini diterapkan karena:

1. Konsumen tidak dalam kondisi menguntungkan untuk membuktikan adanya kesalahan dalam suatu proses produksi dan distribusi yang kompleks;
2. Diasumsikan produsen lebih dapat mengantisipasi jika sewaktu-waktu ada gugatan atas kesalahannya, misalnya dengan asuransi atau menambah komponen buaya tertentu pada harga produknya;
3. Asas ini dapat memaksa produsen lebih hati-hati

D. Penindakan terhadap Pelanggaran Data Pribadi

Undang-Undang Perlindungan Data Pribadi mengatur mengenai sanksi pidana dan sanksi administratif apabila ada penyalahgunaan data pribadi secara ilegal. Menteri Komunikasi dan Informatika (Menkominfo) Johnny G Plate mengatakan, sanksi tersebut bervariasi berdasarkan tingkat kesalahan yang dilakukan apabila ada korporasi maupun perorangan yang menggunakan data pribadi secara ilegal, maka sanksinya jauh lebih berat. Berupa perampasan seluruh kegiatannya yang terkait dengan manfaat ekonomi atas data pribadi dimaksud kalau ilegal.

Sebab itu, Kominfo mendorong semua pihak menggunakan seluruh kepercayaan publik ruang usaha di bidang digital dengan baik. Khususnya bidang data secara legal. Berdasarkan draf UU Perlindungan Data Pribadi, pengenaan sanksi administratif diatur pada pasal 57 Sanksi administratif sebagaimana dimaksud berupa:

⁷⁷ Ibid, Hal 97.

1. peringatan tertulis;
2. penghentian sementara kegiatan pemrosesan Data Pribadi;
3. penghapusan atau pemusnahan Data Pribadi; dan/atau denda administratif. Sanksi administratif berupa denda administratif sebagaimana dimaksud paling tinggi 2% dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.

Penjatuhan sanksi administratif sebagaimana dimaksud diberikan oleh lembaga penyelenggara perlindungan data pribadi. Ketentuan lebih lanjut mengenai tata cara pengenaan sanksi administratif sebagaimana dimaksud diatur dalam Peraturan Pemerintah. Sementara itu, ketentuan pidana diatur pada pasal 67 sampai pasal 73. Diantaranya sebagai berikut :

Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi dipidana dengan pidana penjara paling lama 5 tahun dan/atau pidana denda paling banyak Rp 5 miliar. Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya dipidana dengan pidana penjara paling lama 4 tahun dan/atau pidana denda paling banyak Rp 4 miliar. Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya dipidana dengan pidana penjara paling lama 5 tahun dan/atau pidana denda paling banyak Rp 5 miliar. Setiap Orang yang dengan sengaja membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain

dipidana dengan pidana penjara paling lama 6 tahun dan/atau pidana denda paling banyak Rp 6 miliar.

Selain dijatuhi pidana juga dapat dijatuhi pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian. Dalam hal tindak pidana dilakukan oleh Korporasi, pidana dapat dijatuhan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/atau Korporasi. Pidana yang dapat dijatuhan terhadap Korporasi hanya pidana denda. Pidana denda yang dijatuhan kepada Korporasi paling banyak 10 kali dari maksimal pidana denda yang diancamkan. Selain dijatuhi pidana denda, Korporasi dapat dijatuhi pidana tambahan berupa:

1. perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana;
2. pembekuan seluruh atau sebagian usaha Korporasi;
3. pelarangan permanen melakukan perbuatan tertentu;
4. penutupan seluruh atau sebagian tempat usaha dan/atau kegiatan Korporasi;
5. melaksanakan kewajiban yang telah dilalaikan;
6. pembayaran ganti kerugian;
7. pencabutan izin; dan/atau
8. pembubaran Korporasi

BAB VII

SISTEM TEKNOLOGI INFORMASI DALAM TRANSAKSI E-COMMERCE

A. Syarat sahnya jual beli dalam KUHPerdata

Dalam kegiatan bisnis, jual dan beli barang/jasa menjadi salah satu aktivitas rutin yang terjadi setiap harinya. Misalnya, ketika Anda menjual makanan dan konsumen membelinya, berarti telah terjadi kesepakatan antara Anda dan konsumen untuk melakukan kegiatan jual beli. Atau ketika Anda menjual baju melalui *online marketplace* dan ada pembeli yang menghubungi Anda untuk membeli baju tersebut, ketika Anda dan pembeli telah sepakat dengan harga dan Anda berjanji akan mengirimkan baju tersebut, maka jual beli sudah terjadi meskipun belum ada barang yang diserahkan dan belum ada pembayaran yang dilakukan. Apakah jual beli tetap sah meskipun tidak ada surat perjanjian secara tertulis? Pasal 1320 KUHPerdata yang mengatur tentang syarat sah perjanjian tidak memberikan syarat bahwa perjanjian harus dibuat secara tertulis.

Namun, lain halnya ketika produk yang Anda jual atau beli bernilai tinggi dan pembayaran dilakukan secara bertahap. Misalnya Anda menjual barang dalam jumlah yang banyak dengan nilai transaksi yang besar. Ketika kondisi ini terjadi, membuat perjanjian jual beli sangat dianjurkan untuk memberikan kejelasan mengenai transaksi tersebut dan melindungi Anda dari kemungkinan pembeli gagal melakukan pembayaran yang seharusnya. Di bawah ini Libera akan menjelaskan beberapa hal penting yang perlu ada dalam surat perjanjian jual beli.

1. Adanya Para Pihak yakni Pembeli dan Penjual

Hal pertama yang harus ada dalam perjanjian jual beli adalah adanya para pihak yang melakukan kesepakatan yang melibatkan dua pihak, yaitu penjual dan pembeli. Di mana, kedua belah pihak yang membuat perjanjian jual beli memiliki hak dan kewajiban untuk melaksanakan isi perjanjian yang dibuat. Perlu diperhatikan bahwa para pihak harus memiliki kecakapan untuk melakukan transaksi jual beli. Artinya, baik penjual maupun pembeli telah dianggap dewasa menurut hukum yang berlaku dan tidak sedang berada di bawah pengampuan. Dalam membuat perjanjian, para pihak diberikan kebebasan untuk menentukan bentuk dan isi perjanjian yang mereka buat. Namun, kebebasan ini tetap harus sesuai dengan dan tidak boleh melanggar hukum yang berlaku di Indonesia. Jika isi perjanjian tersebut melanggar hukum yang berlaku, maka perjanjian tersebut tidak memenuhi syarat sah perjanjian yang diatur di Pasal 1320 KUHPerdata dan berakibat batal demi hukum.

2. Obyek yang Diperjualbelikan

Pasal 1457 KUHPerdata menyebutkan bahwa jual beli adalah suatu persetujuan, di mana pihak penjual mengikatkan dirinya untuk menyerahkan suatu benda, dan pihak pembeli membayar harga yang telah disepakati. Perjanjian jual beli dalam KUHPerdata juga menentukan bahwa obyek perjanjian harus tertentu, atau setidaknya dapat ditentukan wujud dan jumlahnya pada saat akan diserahkan hak milik atas barang tersebut kepada pembeli. Sementara itu, KUHPerdata mengenal tiga macam barang yaitu barang bergerak, barang tidak bergerak

(barang tetap), dan barang tidak berwujud seperti piutang atau saham

3. Hak dan Kewajiban Para Pihak

Seperti yang sudah Anda ketahui, surat perjanjian jual beli dilakukan untuk mengatur hak dan kewajiban para pihak. Di mana, penjual memiliki dua kewajiban utama yaitu menyerahkan hak milik atas barang yang telah dibeli dan menanggung kerugian atas kondisi cacat tersembunyi pada barang yang dijual. Sedangkan pembeli berkewajiban membayar harga barang dan pembeli berhak untuk menuntut kepada penjual atas penyerahan barang yang telah dibelinya. Pembayaran ini dilakukan pada waktu dan tempat yang telah ditetapkan dalam perjanjian. Selain itu, pembeli juga memiliki hak untuk membatalkan transaksi jual beli apabila barang yang telah disepakati ternyata memiliki kerusakan atau cacat tersembunyi yang sebelumnya tidak diberitahukan kepada pembeli.

4. Penyerahan dan Pengiriman Barang

Ketika barang sudah dibeli, ada kemungkinan barang tersebut tidak bisa langsung diambil oleh pembeli di tempat, melainkan akan dikirimkan dari tempat penjual ke tempat pembeli. Tata cara penyerahan dan pengiriman barang ini merupakan kesepakatan antara penjual dan pembeli, terutama mengenai biaya pengiriman. Dalam surat perjanjian jual beli, menuliskan dengan jelas tentang siapa yang akan menanggung biaya pengiriman dan kapan pengiriman dilakukan merupakan hal yang jangan sampai terlupakan.

Selain itu, penting juga ditentukan mengenai pengalihan hak milik atas barang. Pasal 612 KUHPerdata menyebutkan

bahwa pengalihan hak milik atas barang bergerak dilakukan dengan penyerahan yang nyata atas barang tersebut. Untuk beberapa kasus, bisa diatur antara penjual dan pembeli mengenai kapan hak milik dan tanggung jawab atas barang beralih, apakah pada saat barang sudah dikeluarkan dan diantarkan dari penjual, atau ketika barang tersebut sampai di tempat pembeli.

5. Syarat Pembayaran

Ketika penjualan dilakukan secara kredit, hal ini penting untuk dipikirkan dan ditulis sejelas mungkin di dalam perjanjian jual beli. Misalnya ketika Anda melakukan penjualan 100.000 tas terhadap *reseller* dengan harga Rp300.000.000. Maka Anda harus menuliskan dengan jelas syarat pembayaran di atas perjanjian tersebut. Misalnya, melakukan DP minimal 10%, dan harus melunasi seluruhnya pada saat 30 hari sebelum barang tersebut Anda kirimkan. Anda juga bisa memberikan denda keterlambatan, misalnya denda 5% ketika melewati jangka waktu tersebut. Hal ini dilakukan untuk mengantisipasi kerugian jika pembeli terlambat melakukan pembayaran.

6. Pengembalian Barang Rusak

Retur barang yang rusak menjadi hal yang sah dilakukan dalam kegiatan jual beli. Namun, pengembalian barang juga harus sesuai dengan syarat yang telah disepakati bersama. Karena itulah hal ini penting untuk ditentukan di awal dan sebelum perjanjian jual beli dibuat atau ditandatangani. Anda dapat memberikan beberapa syarat pengembalian barang di dalam perjanjian, misalnya ketika Anda menjual handphone atau ponsel. Anda bisa memberikan garansi selama 30 hari untuk mesin yang rusak, atau pengembalian barang ketika

ponsel tersebut cacat seperti layar yang tergores, dan lain sebagainya. Namun, jika Anda sebagai penjual, Anda juga perlu membatasi mengenai jenis kerusakan yang dapat diganti. Apabila terdapat kerusakan pada barang namun hal tersebut sudah disampaikan kepada pembeli dan pembeli menerima kerusakan tersebut, maka di kemudian hari pembeli tidak dapat mengembalikan barang atau meminta ganti rugi atas kerusakan tersebut.

7. Ketentuan Berakhirnya Perjanjian

Selain itu, Anda juga harus menuliskan ketentuan berakhirnya perjanjian yang telah Anda buat. Biasanya perjanjian akan berakhir otomatis ketika hak dan kewajiban telah terpenuhi oleh masing-masing pihak. Menurut Pasal 1381 KUHPerdata terdapat beberapa hal yang mengakibatkan berakhirnya suatu perjanjian yaitu:

- a. Karena pembayaran;
- b. Karena penawaran;
- c. Karena pembayaran tunai, diikuti dengan penyimpangan atau penitipan;
- d. Karena perjumpaan utang atau kompensasi;
- e. Karena percampuran utang;
- f. Karena pembebasan utang;
- g. Karena musnahnya barang yang terutang;
- h. Karena kebatalan dan pembatalan;
- i. Karena berlakunya syarat batal;
- j. Karena lewat waktu (kedaluwarsa).

8. Langkah Penyelesaian Perselisihan

Dalam proses jual beli, ada kemungkinan perselisihan yang terjadi antara penjual dan pembeli, baik mengenai salah satu

pihak yang tidak melaksanakan kewajibannya sesuai dengan perjanjian, pengiriman yang terlambat, barang yang tidak sesuai dengan kesepakatan di awal, dan permasalahan lainnya yang dapat menimbulkan perselisihan. Hal ini tentu dapat menghambat pelaksanaan perjanjian dan akan menimbulkan kerugian bagi masing-masing pihak jika dibiarkan berlarut-larut. Karena itulah, Anda harus menuliskan dengan jelas langkah apa saja yang mungkin dilakukan ketika hal ini terjadi, mulai dari melakukan negosiasi hingga membawa masalah ini ke pengadilan.

9. Memenuhi Syarat Perjanjian

Hal terakhir yang harus Anda perhatikan ketika membuat surat perjanjian jual beli adalah memenuhi syarat sahnya perjanjian sesuai Pasal 1320 KUHPerdata yaitu adanya kesepakatan para pihak, kecakapan para pihak dalam membuat perjanjian, adanya hal tertentu, dan terdapat suatu sebab yang diperkenankan. Dengan memenuhi 4 syarat di atas berarti surat perjanjian tersebut sah dan mengikat para pihak. Sehingga perjanjian tersebut harus dilaksanakan oleh para pihak dan dapat digunakan sebagai alat bukti di kemudian hari ketika terjadi sengketa atau perselisihan antara para pihak.

10. Jual Beli yang Harus Menggunakan Akta Otentik

Jual beli pada umumnya cukup dilakukan secara lisan maupun perjanjian tertulis yang dibuat oleh penjual dan pembeli. Bahkan, Pasal 1458 KUHPerdata menyebutkan bahwa jual beli sudah dianggap terjadi ketika penjual dan pembeli sudah mencapai kesepakatan mengenai barang dan harganya, meskipun barang belum diserahkan dan harganya belum dibayar. Namun, khusus untuk barang tidak bergerak seperti

tanah, pengalihan kepemilikan atas barang tersebut harus dilakukan dengan akta otentik sebagaimana diatur dalam Pasal 616 dan 620 KUHPerdata. Saat ini, hal ini sudah secara khusus diatur dalam Pasal 19 ayat (2) Undang-Undang No. 5/1960 tentang Peraturan Dasar Pokok-Pokok Agraria jo. **Pasal 37 ayat (1) Peraturan Pemerintah No. 24/1997 tentang Pendaftaran Tanah** di mana peralihan hak atas tanah yang terjadi karena jual beli perlu didaftarkan dengan menggunakan akta yang dibuat di hadapan Pejabat Pembuat Akta Tanah (PPAT). Akta jual beli merupakan bukti sah bahwa hak atas tanah sudah beralih kepada pihak lain.

B. Keabsahan Kontrak Transaksi Elektronik

Sebagaimana diketahui bahwa secara konvensional sebelum ditetapkan berlakunya UU ITE pada tanggal 21 April 2008 setiap orang yang melakukan berbagai kegiatan transaksi perdagangan, jual beli, sewa menyewa atau mengadakan kontrak dengan orang lain terhadap pihak lain selalu dibuat dalam suatu surat atau dokumen yang tertulis, dihadiri oleh para pihak secara langsung, dan ditandatangani secara langsung pula oleh para pihak yang terkait dengan transaksi atau kontrak dan perikatan atau perjanjian tersebut sebagai suatu bukti yang sah secara hukum sebagaimana ditentukan dalam hukum keperdataan.

“Perikatan” (*verbintenis*) dalam hukum perdata dalam pandangan Subekti mempunyai arti yang lebih luas dari perkataan “perjanjian”. ... Perikatan merupakan suatu pengertian abstrak, sedangkan suatu perjanjian adalah suatu peristiwa hukum yang

konkrit⁷⁸. Suatu perikatan menurut ketentuan hukum perdata dalam hal ini KUHPerdt dapat dikatakan sah bila telah memenuhi syarat-syarat tertentu. Ketentuan mengenai hal ini diatur dalam Pasal 1320, yang secara tegas ditentukan: Untuk sahnya suatu perjanjian diperlukan empat syarat:

1. Sepakat mereka yang mengikatkan dirinya;
2. Kecakapan untuk membuat suatu perikatan;
3. Suatu hal tertentu;
4. Suatu sebab yang halal⁷⁹.

Atas dasar ketentuan di atas, dapat dikemukakan bahwa suatu perikatan sah setelah memenuhi syarat-syarat tersebut, yaitu: 1) Adanya kesepakatan para pihak yang terlibat dalam perjanjian atau perikatan, transaksi atau kontrak tersebut; 2) Adanya suatu kemampuan atau kecakapan untuk membuat suatu perikatan atau perjanjian, kontrak atau transaksi tersebut; 3) Adanya suatu objek yang ditentukan dalam perikatan atau perjanjian, kontrak atau transaksi tersebut; 4) Adanya suatu sebab yang wajar, layak, patut, pantas, dan halal. Selain itu, secara teknis-praktis para pihak harus saling berhadapan secara langsung atau fisik dan dilakukan secara manual. Lalu, dengan disahkan dan berlakunya UU ITE tersebut mulai pada tanggal ditetapkannya seperti yang disebutkan di atas, maka pandangan yang bersifat konvensional tadi tentunya menjadi berubah. Demikian pula yang berkenaan dengan kekawatiran atau kecemasan dan keragu-raguan mengenai keabsahan dari perbuatan hukum yang dilakukan melalaui media teknologi informasi di mana para pihak tidak perlu ketemu secara langsung.

⁷⁸ Subekti, *Pokok-Pokok Hukum Perdata*, Jakarta, 1984, hlm. 123.

⁷⁹ Terpetik dalam, *Kitab Undang-undang Hukum Perdata*, Pradnya Paramita, Jakarta, 2005, hlm. 339.

Lalu bagaimana dengan kekuatan dan akibat hukum dari informasi dan dokumen serta tandatangan dan capnya yang dibuat melalui teknologi informasi tersebut seperti halnya melalui internet terhadap hak dan kewajiban para pihak.

Sehubungan dengan pengaturan persoalan tersebut, maka secara materil pengaturan mengenai informasi elektronik, dokumen dan tanda tangan elektronik tersebut telah diatur dalam UU ITE, yang mana dalam Pasal 5 ditentukan bahwa:

1. Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
2. Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.
3. Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-undang ini.
4. Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:
 - a. Surat yang menurut Undang-undang harus dibuat dalam bentuk tertulis; dan;
 - b. Surat beserta dokumennya yang menurut Undang-undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

Selanjutnya, dalam Penjelasan Pasal 5 ayat (4) a dijelaskan bahwa surat yang menurut undang-undang harus dibuat tertulis meliputi tetapi tidak terbatas pada surat berharga, surat yang

berharga, dan surat yang digunakan dalam proses penegakan hukum acara perdata, pidana, dan administrasi negara.

Selanjutnya dalam Pasal 6 juga ditentukan bahwa dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Selain itu, dalam penjelasan Pasal 6 dijelaskan bahwa selama ini bentuk tertulis identik dengan informasi dan/atau dokumen yang tertuang di atas kertas semata, padahal pada hakikatnya informasi dan/atau dokumen dapat dituangkan ke dalam media apa saja, termasuk media elektronik. Dalam lingkup sistem elektronik, informasi yang asli dengan salinannya tidak relevan lagi untuk dibedakan sebab sistem elektronik pada dasarnya beroperasi dengan cara penggandaan yang mengakibatkan informasi yang asli tidak dapat dibedakan lagi dari salinannya.

Menyadari hal itu, pembentuk UU ITE telah mempertimbangkan secara mendalam sebagaimana yang dinyatakan dalam bagian Penjelasan Umum alinea kesebelas yang menyatakan bahwa⁸⁰ Secara yuridis kegiatan pada ruang siber tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional saja sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan yang lolos dari pemberlakuan hukum. Kegiatan dalam ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian, subjek pelaku harus

⁸⁰ Terpetik dalam, *Penjelasan umum Undang-undang Nomor 11 tahun 2008* Op. cit., hlm. 33.

dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata. Dalam kegiatan *E-Commerce* antara lain dikenal adanya dokumen elektronik yang kedudukannya disetarakan dengan dokumen yang dibuat di atas kertas.

Demikian pula dalam Pasal 7 ditentukan: Setiap orang yang menyatakan hak, memperkuat hak yang telah ada, atau menolak hak Orang lain berdasarkan adanya Informasi Elektronik dan/atau Dokumen Elektronik harus memastikan bahwa Informasi Elektronik dan/atau Dokumen Elektronik yang ada padanya berasal dari Sistem Elektronik yang memenuhi syarat berdasarkan peraturan perundang-undangan. Lalu dalam penjelasannya dijelaskan bahwa: Ketentuan ini dimaksudkan bahwa suatu Informasi Elektronik dan/atau Dokumen Elektronik dapat digunakan sebagai alasan timbulnya suatu hak.

Berkenaan dengan pengaturan waktu pengirimannya, UU ITE telah mengaturnya secara limitatif, yang mana dalam Pasal 8 ditentukan:

1. Kecuali diperjanjikan lain, waktu pengiriman suatu Informasi Elektronik dan/atau Dokumen Elektronik ditentukan pada saat Informasi Elektronik dan/atau Dokumen Elektronik telah dikirim dengan alamat yang benar oleh Pengirim ke suatu Sistem Elektronik yang ditunjuk atau dipergunakan Penerima dan telah memasuki Sistem Elektronik yang berada di luar kendali Pengirim.
2. Kecuali diperjanjikan lain, waktu penerimaan suatu Informasi Elektronik dan/atau Dokumen Elektronik ditentukan pada saat Informasi Elektronik dan/atau Dokumen Elektronik memasuki Sistem Elektronik di bawah kendali Penerima yang berhak.
3. Dalam hal Penerima telah menunjuk suatu Sistem Elektronik tertentu untuk menerima Informasi Elektronik, penerimaan

terjadi pada saat Informasi Elektronik dan/atau Dokumen Elektronik memasuki Sistem Elektronik yang ditunjuk.

4. Dalam hal terdapat dua atau lebih sistem informasi yang digunakan dalam pengiriman atau penerimaan Informasi Elektronik dan/atau Dokumen Elektronik, maka Pasal 8 ayat (4) UUITE:
 - a. Waktu pengiriman adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki sistem informasi pertama yang berada di luar kendali Pengirim;
 - b. Waktu penerimaan adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki sistem informasi terakhir yang berada di bawah kendali Penerima.

Selain itu, UU ITE juga mengatur hal-hal yang berkenaan dengan hak dan kewajiban pelaku usaha, yang dalam Pasal 9 ditentukan: Pelaku usaha yang menawarkan produk melalui Sistem Elektronik harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen dan produk yang ditawarkan. Lalu, dalam Penjelasannya menjelaskan bahwa: Yang dimaksud dengan "informasi yang lengkap dan benar" meliputi:

- a. Informasi yang memuat identitas serta status subjek hukum dan kompetensinya, baik sebagai produsen, pemasok, penyelenggara maupun perantara;
- b. Informasi lain yang menjelaskan hal tertentu yang menjadi syarat sahnya perjanjian serta menjelaskan barang dan/atau jasa yang ditawarkan, seperti nama, alamat, dan deskripsi barang/jasa.

Lebih jauh dalam Pasal 10 ditentukan bahwa:

1. Setiap pelaku usaha yang menyelenggarakan Transaksi Elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan.
2. Ketentuan mengenai pembentukan Lembaga Sertifikasi Keandalan tersebut akan diatur dengan Peraturan Pemerintah.

Selanjutnya dalam Pejelasannya dijelaskan bahwa: Sertifikasi Keandalan dimaksudkan sebagai bukti bahwa pelaku usaha yang melakukan perdagangan secara elektronik layak berusaha setelah melalui penilaian dan audit dari badan yang berwenang. Bukti telah dilakukan Sertifikasi Keandalan ditunjukkan dengan adanya logo sertifikasi berupa *trust mark* pada laman (*home page*) pelaku usaha tersebut.

Dalam konteks Tanda Tangan Elektronik yang dibuat oleh para pihak, maka UUITE telah mengaturnya secara tegas, yang mana dalam Pasal 11 ditentukan:

1. Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:
 - a. Data pembuatan Tanda Tangan Elektronik terkait hanya kepada Penanda Tangan;
 - b. Data pembuatan Tanda Tangan Elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penanda Tangan;
 - c. Segala perubahan terhadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;
 - d. Segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui;

- e. Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa Penandatangannya; dan
 - f. Terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait.
2. Ketentuan lebih lanjut tentang Tanda Tangan Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan pemerintah.

Lalu, dalam Penjelasannya dijelaskan bahwa : Undang-undang ini memberikan pengakuan secara tegas bahwa meskipun hanya merupakan suatu kode, Tanda Tangan Elektronik memiliki kedudukan yang sama dengan tanda tangan manual pada umumnya yang memiliki kekuatan hukum dan akibat hukum. Persyaratan sebagaimana dimaksud dalam pasal ini merupakan persyaratan minimum yang harus dipenuhi dalam setiap Tanda Tangan Elektronik. Ketentuan ini membuka kesempatan seluas-luasnya kepada siapa pun untuk mengembangkan metode, teknik, atau proses pembuatan Tanda Tangan Elektronik. Ketentuan lebih lanjut tentang Tanda Tangan Elektronik tersebut diatur dengan Peraturan Pemerintah yang di dalamnya mengatur antara lain, tentang teknik, metode, sarana, dan proses pembuatan Tanda Tangan Elektronik. Selain itu, dalam Pasal 12 ditentukan:

- a. Setiap Orang yang melakukan pelanggaran ketentuan yang terkait dengan Tanda Tangan Elektronik, bertanggung jawab atas segala kerugian dan konsekuensi hukum yang timbul.
- b. Pengamanan Tanda Tangan Elektronik sebagaimana dimaksud pada ayat (1) sekurang-kurangnya:

- 1) Sistem tidak dapat diakses oleh orang lain yang tidak berhak.
- 2) Penanda Tanganan harus menerapkan prinsip kehati-hatian untuk menghindari penggunaan secara tidak sah terhadap data terkait pembuatan Tanda Tangan Elektronik.
- 3) Penanda Tanganan harus tanpa menunda nunda, menggunakan cara yang dianjurkan oleh Penyelenggara Tanda Tangan Elektronik atau pun cara lain yang layak dsn sepantasnya harus segera memberitahukan kepada seseorang yang Penanda Tangan elektronik dianggap memercayai Tanda Tangan Elektronik atau kepada pihak pendukung layanan anda Tangan Elektronik jika: Penanda tangan mengetahui bahwa data pembuat Tanda Tangan Elektronik telah dibobol, atau Keadaan yang diketahui oleh Penanda Tangan dapat menimbulkan resiko yang berarti, kemungkinan akibat bobolnya data pembuatan Tanda Tangan Elektronik; dan
- 4) Dalam hal Sertifikat Elektronik digunakan untuk mendukung Tanda Tangan Elektronik, Penanda Tangan harus memastikan kebenaran dan keutuhan semua informasi yang terkait dengan Sertifikat Eletronik tersebut.
- 5) Setiap orang yang melakukan pelanggaran ketentuan sebagaimana dimaksud pada ayat (1), bertanggungjawab atas segala kerugian dan konsekuensi hukum yang timbul.

Bertitik tolak dari ketentuan dan pandangan yang dikemukakan di atas mengenai persoalan keabsahan dalam pembuktian yuridis dari Informasi elektronik, dokumen elektronik dan tanda tangan elektronik tidak perlu diragukan lagi kepastian hukum dan akhibat hukum dari dokumen elektronik tersebut semenjak diberlakukannya UU ITE ini. Dalam pada itu tepat apa yang dikemukakan Ahmad M Ramli berpendapat ;

Kegiatan siber meskipun bersifat virtual dapat dikategorikan sebagai tidakan dan perbuatan hukum yang nyata. Secara yuridis dalam hal ruang siber sudah tidak pada tempatnya lagi untuk mengkategorikan sesuatu dengan ukuran dan kualifikasi hukum konvesional untuk dapat dijadikan objek dan perbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal-hal yang lolos dari jeratan hukum. Kegiatan siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian subjek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata.

Menyimak pandangan tersebut, tentunya juga berlaku hal yang sama dan yang terjadi dalam kegiatan perdagangan atau bisnis di berbagai belahan dunia termasuk di Indonesia yang saat ini lagi *trend* di dunia internasional. Dalam pada itu Ahmad M. Ramli, lebih jauh berpendapat⁸¹: Dalam kegiatan *e-commerce* antara lain dikenal adanya dokumen-dokumen elektronik yang kedudukannya disetarakan dengan dokumen-dokumen yang dibuat di atas kertas.

⁸¹ *Ibid.*

C. Kontrak Jual Beli Transaksi Elektronik

Pada prinsipnya, transaksi perdagangan dengan menggunakan teknologi *e-commerce* sesungguhnya merupakan suatu model kontrak yang sama dengan kontrak jual beli konvensional yang dilakukan dalam masyarakat Indonesia.

Jual beli secara konvensional yang dilakukan oleh masyarakat Indonesia hingga saat ini dilakukan baik itu berdasarkan sistem KUH Perdata maupun menurut sistem hukum adat. Menurut hukum adat Indonesia, yang dinamakan jual beli, bukanlah persetujuan belaka yang berada di antara kedua belah pihak, tetapi adalah suatu penyerahan barang oleh si penjual kepada si pembeli dengan maksud memindahkan hak milik atas barang itu dengan syarat pembayaran harga tertentu, berupa uang oleh pembeli kepada penjual. Dengan demikian, dalam hukum adat, setiap hubungan jual beli tidak mengikat kepada asas atau sistem obligator atau sistem/asas yang lainnya.

Wirjono Prodjodikoro mengemukakan bahwa dalam hukum adat ada juga persetujuan antara kedua belah pihak yang berupa mufakat tentang maksud untuk memindahkan hak milik dari tangan penjual ke tangan pembeli dan pembayaran harga pembeli oleh pembeli kepada penjual, tetapi persetujuan itu hanya bersifat pendahuluan untuk suatu perbuatan hukum tertentu yaitu berupa penyerahan tadi. Selama penyerahan barang belum terjadi, maka belum ada jual beli.⁸²

Tentang perjanjian jual beli, dianggap sudah berlangsung antara pihak penjual dan pembeli, apabila mereka telah menyetujui dan

⁸² Wirjono Prodjodikoro, *Op. cit*, hal. 26.

bersepakat tentang keadaan benda dan harga barang tersebut, sekalipun barangnya belum diserahkan dan harganya belum dibayarkan (Pasal 1458 KUH Perdata). Jual beli tiada lain dari persesuaian kehendak (*wis overeensteeming*) antara penjual dan pembeli mengenai barang dan harga. Barang dan hargalah yang menjadi essensial perjanjian jual beli.

Tanpa ada barang yang hendak dijual, tidak mungkin terjadi jual beli. Sebaliknya jika barang objek jual beli tidak dibayar dengan sesuatu harga, jual beli dianggap tidak ada. Cara dan terbentuknya perjanjian jual beli, bisa terjadi secara *openbaar*/ terbuka, seperti yang terjadi pada penjualan atas dasar eksekutorial atau yang disebut *excitoriale verkoop*. Penjualan eksekutorial mesti dilakukan melalui lelang di muka umum oleh pejabat lelang, akan tetapi cara dan bentuk penjualan eksekutorial yang bersifat umum ini, jarang sekali terjadi. Penjualan demikian harus memerlukan keputusan pengadilan.

Dari pembahasan di atas dapat dipahami bahwa jual beli secara konvensional yang terjadi dalam lalu lintas kehidupan masyarakat sehari-hari adalah jual beli antara tangan ke tangan, yakni jual beli yang dilakukan antara penjual dan pembeli tanpa campur tangan pihak resmi dan tidak perlu di muka umum. Bentuk jual belinya pun, terutama jika objeknya barang-barang bergerak cukup dilakukan dengan lisan, kecuali mengenai benda-benda tertentu, terutama mengenai objek benda-benda tidak bergerak pada umumnya, selalu memerlukan bentuk akta jual beli. Tujuan akta ini hanya sekedar mempelajari jual beli itu dengan keperluan penyerahan yang kadang-kadang memerlukan penyerahan yuridis di samping penyerahan nyata.

Memperhatikan uraian di atas mengenai persamaan antara transaksi perdagangan *e-commerce* dengan jual beli secara

konvensional, maka dapat dilihat bahwa letak perbedaan utamanya adalah hanya pada media yang digunakan. Pada transaksi *e-commerce*, media yang digunakan adalah media elektronik atau internet. Sehingga kesepakatan ataupun kontrak yang tercipta adalah melalui *online*. Kemudian, hampir sama pula dengan kontrak jual beli konvensional, kontrak jual beli *e-commerce* tersebut juga terdiri dari penawaran dan penerimaan. Sebab suatu kesepakatan selalu diawali dengan adanya penawaran oleh salah satu pihak dan penerimaan oleh pihak yang lainnya.⁸³

Berikut adalah contoh-contoh transaksi *e-commerce*:

⁸³ Atip Latifulhayat, 2002, "Perlindungan Data Pribadi dalam Perdagangan Secara Elektronik (*E-Commerce*), Artikel dalam *Jurnal Hukum Bisnis*, Volume 18 Maret, hal. 28.

TRANSAKSI ZALORA



TRANSAKSI SHOPEE



TRANSAKSI LAZADA



Secara umum, baik yang dilakukan dalam skala nasional maupun yang bersifat internasional, transaksi *e-commerce* menimbulkan berbagai pertanyaan yuridis. Dalam proses dan mekanisme terjadinya transaksi dapat dikemukakan beberapa permasalahan keabsahan hukum sehubungan dengan masalah hukum kontrak, antara lain:⁸⁴

Pertama, masalah saat kapan terjadi atau lahirnya kesepakatan dalam transaksi *e-commerce*. Permasalahan ini erat kaitannya dengan saat bertemu penawaran dan penerimaan melalui media maya tersebut. penawaran dilakukan melalui internet dan penerimaan juga demikian. Kapan saat pesanan dan jawaban itu terjadi? Pada saat di-klik melalui simbol-simbol di dalam internet tersebut atau ada saat lain yang dapat dikualifikasikan secara yuridis sebagai saat lahirnya kontrak. Tidakkah perlu adanya konfirmasi dari pihak pemesan atau pembeli? Sementara isi pesan yang disampaikan melalui internet itu dapat diubah atau diganti oleh orang lain. Secara konvensional, kontrak lahir dan bahkan berlaku segera setelah terjadi kesepakatan antara para pihak.

Kedua, masalah yang lain masih berkaitan dengan keabsahan transaksi. Bagaimana melacaknya jika transaksi itu dibuat oleh orang yang di bawah umur atau orang yang mempunyai maksud jahat? Persoalan hukum tentang ukuran atau kriteria di bawah umur pun berbeda-beda antara satu negara dengan negara lain.

⁸⁴ Nindyo Pramono, “Revolusi Dunia Bisnis Indonesia Melalui E-Commerce dan E-Business: Bagaimana Solusi Hukumnya”, *makalah disampaikan dalam Seminar Nasional Peluang E-Bisnis serta Kesiapan Hukumnya di Indonesia*, UKDW Yogyakarta di Hotel Ambarukmo, Yogyakarta, 14 April 2001, hlm. 16.

Jenis kontrak *e-commerce* dalam bisnis ke konsumen ada pula kontrak dalam bentuk *shirnkwrap contract* dan *click wrap contract* yang merupakan perjanjian yang menawarkan kepada konsumennya penggunaan produk dengan syarat-syarat yang menyertai produk tersebut, umumnya terjadi dalam kontrak penggunaan perangkat lunak komputer.⁸⁵

Setiap kontrak pada dasarnya merupakan bagian penting dari suatu proses bisnis yang sarat dengan pertukaran kepentingan di antara para pelakunya. Merancang suatu kontrak pada hakikatnya dapat diibaratkan menuangkan proses bisnis ke dalam format hukum. Mengandaikan hubungan yang sinergis-korelatif antara aspek bisnis dengan hukum (kontrak), ibarat lokomotif dan gerbongnya sebagai personifikasi aspek bisnis sedang bantalan rel di mana lokomotif dan gerbong itu berkalan menuju tujuannya sebagai personifikasi aspek hukumnya (kontrak). Oleh karena itu, keberhasilan bisnis antara lain juga akan ditentukan oleh struktur atau bangunan kontrak yang dirancang dan disusun oleh para pihak.⁸⁶

Di dalam setiap kontrak jual beli maupun bentuk kontrak lainnya akan melalui 3 (tiga) rangkaian tahapan hingga pelaksanaan dari kontrak yaitu diawali dengan tahap *pra contractual*, yaitu adanya penawaran dan penerimaan, tahap *contractual*, yaitu adanya persesuaian pernyataan kehendak antara para pihak, dan tahap *post contractual*, yaitu pelaksanaan perjanjian.⁸⁷ Hal yang paling penting sebelum menuju kepada

⁸⁵ *Ibid.*, hlm 21-22.

⁸⁶ Agus Yudha Hernoko, *Op. cit*, hal. 147.

⁸⁷ H. Salim HS, 2010, *Perkembangan Teori Dalam Ilmu Hukum*, Jakarta: PT RajaGrafindo Persada, hal. 164.

kesepakatan dalam setiap kontrak adalah tahapan pra kontrak, yaitu adanya penawaran dan penerimaan di antara para pihak.

Sama halnya dengan pra kontrak pada umumnya, pra kontrak dalam transaksi jual beli yang menggunakan *e-commerce* biasanya akan didahului oleh penawaran jual, penerimaan beli. Sebelum itu, dapat saja terjadi penawaran secara *online*, misalnya melalui *website*, situs internet atau melalui posting di *mailing list* dan *news group* atau melalui undangan para *customer* melalui model *business to business*. Untuk menyediakan keberadaan sebuah *website*, maka harus tersedia unsur-unsur penunjangnya adalah sebagai berikut:

1. domain (Domain name/*Uniform Resource Locator*).

Pengertian Nama domain atau biasa disebut dengan Domain Name atau URL adalah alamat unik di dunia internet yang digunakan untuk mengidentifikasi sebuah *website*, atau dengan kata lain domain name adalah alamat yang digunakan untuk menemukan sebuah *website* pada dunia internet. Contoh: <http://www.palasarionline.com>, <http://www.toko bagus.com>, dan lain-lain. Nama domain diperjualbelikan secara bebas di internet dengan status sewa tahunan. Nama domain sendiri mempunyai identifikasi ekstensi/akhiran sesuai dengan kepentingan dan lokasi keberadaan *website* tersebut. Contoh nama domain ber-ekstensi internasional adalah com, net, org, info, biz, name, ws. Contoh nama domain ber-ekstensi lokasi Negara Indonesia adalah co.id (untuk nama domain *website* perusahaan), ac.id (nama domain *website* pendidikan), go.id

(nama domain *website* instansi pemerintah), or.id (nama domain *website* organisasi).

2. Rumah tempat *website* (*web hosting*). Pengertian *Web Hosting* dapat diartikan sebagai ruangan yang terdapat dalam *harddisk* tempat menyimpan berbagai data, file-file, gambar dan lain sebagainya yang akan ditampilkan di *website*. Besarnya data yang bisa dimasukkan tergantung dari besarnya *web hosting* yang disewa/dipunyai, semakin besar *web hosting*, semakin besar pula data yang dapat dimasukkan dan ditampilkan dalam *website*. *Web Hosting* juga diperoleh dengan menyewa. Besarnya *hosting* ditentukan ruangan *harddisk* dengan ukuran MB (Mega Byte) atau GB (Giga Byte). Lama penyewaan *web hosting* rata-rata dihitung per tahun. Penyewaan *hosting* dilakukan dari perusahaan-perusahaan penyewa *web hosting* yang banyak dijumpai, baik di Indonesia maupun luar negeri.
3. Bahasa Program (*scripts program*). Bahasa Program adalah bahasa yang digunakan untuk menerjemahkan setiap perintah dalam *website* yang pada saat diakses. Jenis bahasa program sangat menentukan statis, dinamis atau interaktifnya sebuah *website*. Semakin banyak ragam bahasa program yang digunakan maka akan terlihat *website* semakin dinamis, dan interaktif serta terlihat bagus. Beragam bahasa program saat ini telah hadir untuk mendukung kualitas *website*. Jenis jenis bahasa program yang banyak dipakai para desainer *website* antara lain HTML, ASP, PHP, JSP, Java Scripts, Java applets dsb. Bahasa dasar yang dipakai setiap situs adalah HTML sedangkan PHP, ASP, JSP dan lainnya merupakan bahasa pendukung yang bertindak sebagai

pengatur dinamis, dan interaktifnya situs. Bahasa program ASP, PHP, JSP atau lainnya bisa dibuat sendiri. Bahasa program ini biasanya digunakan untuk membangun portal berita, artikel, forum diskusi, buku tamu, anggota organisasi, email, mailing list dan lain sebagainya yang memerlukan update setiap saat.

4. Desain *website*. Setelah melakukan penyewaan *domain name* dan *web hosting* serta penguasaan bahasa program (*scripts program*), unsur *website* yang penting dan utama adalah desain. Desain *website* menentukan kualitas dan keindahan sebuah *website*. Desain sangat berpengaruh kepada penilaian pengunjung akan bagus tidaknya sebuah *website*. Untuk membuat *website* biasanya dapat dilakukan sendiri atau menyewa jasa *website designer*. Saat ini sangat banyak jasa web designer, terutama di kota-kota besar. Perlu diketahui bahwa kualitas situs sangat ditentukan oleh kualitas designer. Semakin banyak penguasaan web designer tentang beragam program/software pendukung pembuatan situs maka akan dihasilkan situs yang semakin berkualitas, demikian pula sebaliknya. Jasa web designer ini yang umumnya memerlukan biaya yang tertinggi dari seluruh biaya pembangunan situs dan semuanya itu tergantung kualitas designer.

Keberadaan situs tidak ada gunanya dibangun tanpa dikunjungi atau dikenal oleh masyarakat atau pengunjung internet. Karena efektif tidaknya situs sangat tergantung dari besarnya pengunjung dan komentar yang masuk. Untuk mengenalkan situs kepada masyarakat memerlukan apa yang disebut publikasi atau promosi. Publikasi situs di masyarakat

dapat dilakukan dengan berbagai cara seperti dengan pamlet-pamlet, selebaran, baliho dan lain sebagainya tapi cara ini bisa dikatakan masih kurang efektif dan sangat terbatas. Cara yang biasanya dilakukan dan paling efektif dengan tak terbatas ruang atau waktu adalah publikasi langsung di internet melalui *search engine* (mesin pencari, spt: Yahoo, Google, Search Indonesia, dsb). Cara publikasi di *search engine* ada yang gratis dan ada pula yang membayar. Situs yang gratis biasanya terbatas dan cukup lama untuk bisa masuk dan dikenali di *search engine* terkenal seperti Yahoo atau Google. Cara efektif publikasi adalah dengan membayar, walaupun harus sedikit mengeluarkan akan tetapi situs cepat masuk ke *search engine* dan dikenal oleh pengunjung.

Penawaran dalam hukum positif Indonesia merupakan suatu "*invitation to enter into a binding agreement*". Tawaran merupakan suatu tawaran jika pihak lain menganggap atau memandangnya sebagai suatu tawaran, suatu perbuatan seseorang beralasan bahwa perbuatan itu sendiri sebagai ajakan untuk masuk kedalam suatu ikatan kontrak, maka hal ini dapat dianggap sebagai suatu tawaran. Dalam transaksi jual beli yang menggunakan *ecommerce*, khususnya jenis *business to customer* yang melakukan penawaran adalah *merchant* atau produsen/penjual.

Para *merchant* atau penjual tersebut memanfaatkan *website* untuk menjajakan produk dan jasa pelayanan. Para penjual ini menyediakan semacam *storefront* yang berisikan katalog produk dan pelayanan yang diberikan dan para pembeli seperti berjalan-jalan di depan toko-toko dan melihat-lihat barang-barang di dalam etalase. Keuntungannya melakukan belanja di toko *online* ini adalah kita dapat melihat dan berbelanja kapan saja dan di mana

saja tanpa dibatasi oleh jarak lintas suatu daerah, kota, bahkan negara dan jam buka serta tutup toko, dan kita juga tidak akan risih dengan penjaga toko yang mengawasi kegiatan kita.

Dalam *website* tersebut biasanya ditampilkan barang-barang yang ditawarkan, harganya, nilai *rating* atau *poll* otomatis tentang barang itu yang diisi oleh pembeli sebelumnya, spesifikasi tentang barang tersebut dan menu produk lain yang berhubungan, dan penawaran tersebut terbuka bagi semua orang sehingga semua orang yang tertarik dapat melakukan *window shopping* di toko-toko *online* ini. Tawaran ini adalah pernyataan mengenai syarat-syarat yang dikehendaki oleh penawar supaya mengikat, jika suatu tawaran diterima sebagaimana adanya berarti persetujuan itu tercapai. Dalam transaksi bisnis yang menggunakan *e-commerce* ini, suatu tawaran boleh dilakukan terhadap seseorang tertentu dan hanya terbuka baginya untuk menerimanya. Selain itu tawaran juga boleh diberikan dan hanya terbuka kepada kelompok dan dalam hal ini hanya orang-orang yang tergabung dalam kelompok itu saja yang diperbolehkan untuk menerima tawaran tersebut.

Dalam proses penawaran, penjual juga mesti beritikad baik di dalam memberikan informasi mengenai barang yang diperdagangkan melalui *ecommerce* tersebut. Hal itu juga ditegaskan dalam Pasal 17 ayat (2) Undang- undang Informasi dan Transaksi Elektronik yang menentukan: “Para pihak yang melakukan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) wajib beritikad baik dalam melakukan interaksi dan/atau pertukaran Informasi Elektronik dan/atau Dokumen Elektronik selama transaksi berlangsung.”

Dalam kedudukannya juga sebagai pelaku usaha, maka penjual transaksi jual beli *e-commerce* ini tidak hanya tunduk pada sistematika Undang-undang Informasi dan Transaksi Elektronik, akan tetapi juga tunduk pada sistematika Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (selanjutnya disebut Undang-undang Perlindungan Konsumen) dalam rangka hubungan hukumnya dengan konsumen selaku pembeli. Sebagai pelaku usaha oleh Undang-undang Perlindungan Konsumen menegaskan bahwa setiap pelaku usaha memiliki kewajiban untuk memberikan informasi yang benar dan tidak menyesatkan atas produk barang dan/jasa yang ditawarkan kepada konsumen. Hal tersebut secara tegas diatur dalam Pasal 7 huruf b Undang-undang Perlindungan Konsumen yang menentukan bahwa pelaku usaha wajib: "memberikan informasi yang benar, jelas dan jujur mengenai kondisi dan jaminan barang dan/atau jasa serta memberi penjelasan penggunaan, perbaikan dan pemeliharaan."

Akan tetapi, yang harus menjadi perhatian terkait dengan penawaran dalam transaksi jual beli *e-commerce* ini bahwa tidak semua tawaran termasuk dalam tawaran yang membawa konsekuensi hukum. Berikut ini beberapa kriteria tawaran yang tidak termasuk dalam arti hukum, yaitu:⁸⁸

Ajakan untuk melayani semata-mata, dalam hal ini ada suatu indikasi bahwa seseorang berkehendak untuk melakukan perundingan, akan tetapi tidak berkehendak untuk terikat dengan syarat-syarat yang disebutkan, daftar barang dagangan atau media dalam mengiklankan barang-barang untuk dijual. Indikasi yang

⁸⁸ SB. Marsh dan J. Soulsby, 2006, *Business Law (Hukum Perjanjian)*, alih bahasa Abdulkadir Muhammad, Bandung: PT Alumni, hal. 110.

sama berlaku juga apabila usaha yang besar mengundang para penawar untuk menyediakan barang-barang atau jasa-jasa, misalnya suatu iklan perusahaan di *website* yang mengundang para penanam modal untuk membeli saham-saham perusahaannya juga merupakan ajakan, bukan suatu tawaran, sebab perusahaan itu masih dapat menolak membagikan saham-sahamnya itu kepada mereka yang mengajukan permohonan untuk memperolehnya.

Isapan jempol atau bualan semata-mata, dalam hal ini tidak seorang pun yang akan memperhatikan secara serius, seperti merek yang tertera dalam paket misalnya bahwa: "Merek X paling tangguh" atau "Merek Y membersihkan paling bersih" tidak akan dianggap sebagai tawaran tetap, akan tetapi dapat ditarik garis batas yang sempit antara bualan semata-mata dan janji-janji yang akan diterima serius oleh orang awam. Contohnya dalam kasus *Carlil* melawan *Carbolic Smoke Ball Co* (1893), para tergugat mengiklankan bahwa mereka akan membayar €100, kepada setiap orang yang terkena influenza setelah memakai bola-bola asap mereka, dan bahwa sebagai bukti kejujuran, mereka telah menyediakan uang €100 pada sebuah bank ternama. Ny. *Carlil* mengikuti petunjuk-petunjuk mereka, akan tetapi masih terkena influenza, dan akibatnya Ny. *Carlil* menuntut ganti rugi €100. Salah satu dari banyak pembelaan yang diajukan tergugat adalah bahwa iklan itu bukan tawaran. Diputuskan pengadilan bahwa dalam keadaan ini, iklan tersebut adalah tawaran, orang biasa akan tertarik dan menerima janji itu secara serius dan menganggap bahwa pemasang iklan itu bermaksud untuk terikat dengan syarat-syarat yang dinyatakan itu.

Pernyataan kehendak, ini sama juga halnya dengan tidak bermaksud untuk membentuk dasar perjanjian dan bukan suatu tawaran. Misalnya iklan pelelangan umum, dalam kasus *Harris* melawan *Nickerson* (1873), suatu pelelangan diiklankan dan kemudian dibatalkan, dan penggugat yang telah berpergian ke tempat pelelangan tersebut menuntut ongkos perjalannya sebagai ganti rugi, dan gugatannya tidak dikabulkan oleh pengadilan, karena iklan itu bukanlah suatu tawaran yang dapat diterima dengan melakukan perjalanan tersebut.

Semata-mata memberikan informasi, pada prinsipnya dalam *website* atau situs banyak berisi informasi-informasi menyangkut suatu barang bahkan sampai harga dari barang tersebut. Hal ini tidak dapat dikatakan sebagai suatu tawaran.

Transaksi pra kontrak secara *online* dalam *e-commerce* ini menurut *Research Paper on Contract Law* memiliki banyak variasi, yakni: transaksi melalui *chatting* dan *video conference*, transaksi melalui *e-mail*, dan Transaksi melalui *Web* atau Situs.⁸⁹ Transaksi melalui *chatting* atau *video conference* adalah seseorang dalam melakukan penawaran sesuatu barang dengan menggunakan model dialog interaktif melalui internet, seperti melalui telepon, *chatting* dilakukan melalui tulisan, sedangkan *video conference* dilakukan melalui media elektronik, di mana seseorang dapat melihat langsung gambar dan mendengar suara pihak lain yang melakukan penawaran dengan menggunakan alat ini.⁹⁰

⁸⁹ Haris Faulidi Asnawi, 2004, *Transaksi Bisnis E-Commerce: Perspektif Islam*, Yogyakarta: Magistra Insania Press, hal. 5.

⁹⁰ *Ibid.*

Transaksi dengan menggunakan *e-mail* dapat dilakukan dengan cara mudah di mana dalam hal ini kedua belah pihak harus memenuhi syarat, yaitu memiliki *e-mail address*. Selanjutnya sebelum melakukan transaksi, konsumen sudah mengetahui *e-mail* yang akan dituju dan jenis barang serta jumlah yang akan dibeli, kemudian konsumen menulis nama produk dan jumlah produk, alamat pengiriman, dan metode pembayaran yang digunakan. Konsumen selanjutnya akan menerima konfirmasi dari *merchant* mengenai *order* barang yang telah dipesan tersebut. Model transaksi melalui *web* atau situs yaitu dengan cara di mana *merchant* menyediakan daftar atau katalog barang yang dijual disertai dengan deskripsi produk yang dijual dalam *web* atau situs yang telah dibuat oleh penjual. Pada model transaksi ini dikenal istilah *order form* dan *shopping cart*.¹⁰

Belanja dengan menggunakan *order form* merupakan salah satu cara belanja yang sering digunakan dalam bisnis *e-commerce*, dengan cara *merchant* menyediakan daftar atau katalog barang (*product table*) yang dijual. Saat tahap *order* dilaksanakan, biasanya produk yang dijual tidak divisualisasikan dalam bentuk gambar, akan tetapi dalam deskripsi produk. Dalam sebuah halaman *order form*, sesi penawaran produk terbagi dalam empat bagian, yaitu: *Check box*, yang dibuat untuk memberi kesempatan kepada konsumen untuk memiliki produk yang ditawarkan dengan mengklik kotak tersebut sehingga bertanda *check*, penjelasan produk yang ditawarkan, kuantitas barang yang dipesan, dan harga untuk tiap-tiap produk.

Selain tabel produk ditawarkan juga jenis pembayaran. Jenis-jenis pembayaran yang ditawarkan berbeda-beda sesuai dengan

layanan yang disediakan oleh *merchant*, seperti dengan *credit card*, transfer lewat bank, check, dan lain-lain. Pada saat pengisian formulir, konsumen juga diminta untuk mengisi formulir yang bersifat informasi kontak untuk konsumen (sering disebut dengan *Contact Information Table*). Bila pembayaran menggunakan *credit card*, maka formulir akan diisi dengan mengisi jenis atau tipe *credit card*, nomor *credit card*, tanggal kadaluarsa (*expiry date*) serta informasi pemegang kartu (*card holder*).

Setelah pengisian *order form* dilakukan, selanjutnya akan disediakan tombol untuk konfirmasi order, biasanya digunakan tombol *Submit* dan tombol *Reset*, jika di klik *Reset*, proses akan mereset semua pilihan dan informasi yang telah dimasukkan oleh customer dan dapat diulang dari awal. Jika yang di klik adalah tombol *Submit*, maka proses akan dilanjutkan ke tahap pengesahan dan pengecekan order. Pada bagian ini dipasang sistem keamanan, misalnya SSL (*Secure Sockets Layer*) untuk melindungi dari tindakan penipuan. Selanjutnya jika informasi yang dikirimkan oleh konsumen telah memenuhi persyaratan atau dinyatakan valid, maka *merchant* akan mengirimkan berita konfirmasi kepada konsumen dalam bentuk *e-mail*.

Sebagai analogi jika seseorang berbelanja di salah satu pasar swalayan tentunya memerlukan dan membutuhkan kereta belanja untuk mempermudah meletakkan barang-barang yang akan dibeli. Selama belum dilakukan pembayaran di kasir, maka orang tersebut dapat membatalkan pembelian barang dan menukarkannya dengan yang lain. Demikian juga halnya dengan berbelanja melalui *e-commerce*. Dalam *e-commerce*, untuk memilih barang yang akan dibeli, ada semacam formulir yang harus diisi

dalam *web* tempat ia akan melakukan transaksi. Formulir pengisian barang yang akan dibeli dinamakan *shopping cart* yang berfungsi seperti kereta belanja. *Shopping cart* merupakan sebuah *software* di dalam *web* yang mengijinkan seorang konsumen untuk melihat toko yang dibuka dan kemudian memilih *item-item* untuk diletakkan dalam “kereta belanja” yang kemudian membelinya saat melakukan *check out*.

Software ini akan melakukan penjumlahan terhadap biaya transportasi pengiriman barang (jika ada), kuantitas barang dan harga total barang yang dibeli. Biaya transportasi pengiriman dengan menggunakan jasa kurir pengiriman biasanya telah ditentukan terlebih dahulu tergantung kota yang dituju, misalnya barang yang dituju ke kota Banjarmasin akan berbeda biaya pengirimannya ke kota Palangkaraya, dan begitu juga kota lainnya. Seseorang bisa memilih barang yang dibutuhkan untuk dimasukkan ke dalam *shopping cart* dan masih bisa membatalkan sebelum mengadakan transaksi. Setelah semua barang yang akan dibeli dimasukkan ke dalam *shopping cart*, kemudian melakukan *check out*, selanjutnya adalah mengisi formulir transaksi yang berupa data identitas pembeli dan jenis pembayaran yang digunakan. Setelah semua ketentuan terpenuhi, *merchant* segera mengirim barang yang dipesan kepada konsumen.

Berdasarkan uraian di atas, dapat dipahami bahwa penawaran juga merupakan proses yang penting di dalam transaksi jual beli *e-commerce* dan menjadi suatu tahapan pra kontrak seperti jual beli pada umumnya. Melalui penawaran dapat mempertemukan perbedaan atau ketidaksamaan kepentingan di antara para pihak. Dengan penawaran, konsumen selaku pembeli

dapat mengetahui setiap produk yang ditawarkan oleh penjual secara *online*. Tentunya dalam menyampaikan informasi mengenai produk barang dan diperdagangkan tersebut, penjual selaku pelaku usaha harus beritikad baik di dalam menjalankan kegiatan usahanya tersebut yaitu memberikan informasi penawaran yang benar, jelas, dan jujur.

Sebagaimana transaksi bisnis biasa, dalam transaksi jual beli yang menggunakan *e-commerce* ini, antara penawaran dan penerimaan, selalu ada selang jangka waktu tertentu yang bisa singkat saja dan bisa juga memakan waktu yang cukup lama. Dalam transaksi bisnis biasa sebelum penawaran diakseptir oleh pihak lain, penawaran tersebut dapat ditarik kembali, akan tetapi jika penawaran tersebut telah diakseptir, maka penawaran tersebut tidak dapat ditarik kembali, sedangkan dalam transaksi jual beli yang menggunakan *e-commerce*, penawaran dapat saja ditarik walaupun sudah ada akseptir oleh pihak lain.

Hal ini akan menimbulkan masalah, yaitu berkaitan dengan apakah dalam hal sesudah ada penerimaan tersebut tetapi sebelum jawaban tersebut sampai kepada pihak yang menawarkan, orang yang menawarkan mengirimkan berita yang menyatakan menarik kembali penawarannya dapat dikatakan telah terjadinya kontrak/perjanjian atau tidak. Persoalan ini tentu saja akan bergantung pada jawaban kapan sebenarnya kita dapat menganggap telah terjadi/lahir suatu perjanjian. Menjawab hal tersebut tentunya memerlukan suatu teori di mana melalui teori tersebut akan memberikan ruang bagi penjelasan suatu objek yang konkret. Terkait dengan hal tersebut, dalam teori-teori hukum

perdata, terdapat beberapa teori mengenai momentum terjadinya kontrak antara lain:⁹¹

1. Teori Pernyataan (*Uitingstheorie*)

Menurut teori ini, kesepakatan terjadi pada saat pihak yang menerima penawaran itu menyatakan bahwa ia menerima pernyataan itu. Dengan perkataan lain, perjanjian itu ada, pada saat pihak lain menyatakan penerimaan (penerimaan yang dinyatakan dalam bentuk/wujud suatu tulisan). Pada saat tersebut pernyataan kehendak dari orang yang menawarkan dan akseptor saling bertemu. Dalam transaksi jual beli *e-commerce* berpijak pada teori pernyataan teori ini, maka dapat dikatakan bahwa perjanjian/kontrak itu sudah ada sejak pihak penerima tawaran menulis *e-mail* (apabila transaksi menggunakan sarana *e-mail*) atau dalam transaksi yang menggunakan *website*/situs, pada saat akseptor mengetik untuk mengisi form khusus yang telah disediakan oleh pihak penawar. Adapun keberatan terhadap teori ini adalah bahwa orang tidak dapat menerapkan secara pasti kapan perjanjian telah terjadi/lahir, karena sangat sulit bagi kita untuk mengetahui dengan pasti dan membuktikan kapan saat penulisan jawaban penerimaan tersebut, apalagi menyangkut transaksi jual beli yang menggunakan *e-commerce*. Di samping itu, perjanjian sudah terjadi pada saat akseptor masih mempunyai kekuasaan penuh atas surat jawaban tersebut. Ia dapat mengulur atau bahkan membatalkan akseptasinya, sedangkan orang yang menawarkan sudah terikat.

⁹¹ H. Salim HS, *Op. cit*, hal. 166-167.

2. Teori Pengiriman (*Verzendtheorie*)

Menurut teori ini ditetapkan bahwa saat pengiriman jawaban akseptasi adalah saat lahirnya perjanjian, maka orang mempunyai pegangan yang relatif sedikit pasti mengenai saat terjadinya kontrak. Untuk transaksi bisnis biasa relatif lebih mudah, karena misalnya tanggal cap pos dapat dijadikan sebagai salah satu patokan utama. Sejak saat surat itu dikirimkan, akseptor tidak lagi mempunyai kekuasaan atas surat tersebut dan sejak saat itu pulalah kontrak telah terjadi. Teori ini pada prinsipnya masih memiliki kekurangan dan kelemahan, yaitu bahwa perjanjian tersebut telah lahir dan mengikat pihak yang menawarkan pada saat yang menawarkan tersebut belum mengetahui tentang hal itu. Konsekuensi dari teori ini adalah bahwa dalam hal orang yang menawarkan telah mengirim berita penarikan kembali penawarannya lebih dahulu dari pada tanggal pengiriman berita penerimaan pihak akspetor, maka tidaklah lahir perjanjian antara mereka. Teori pengiriman ini sulit untuk diterima berdasarkan asas kepatutan (*billijkheid*), ada sesuatu yang dirasakan tidak adil, ditinjau dari sudut orang yang menawarkan selalu masih ada kemungkinan untuk menarik kembali penawarannya, asal penarikan itu sampai pada orang yang ditawari sebelum ia mengirimkan jawaban penerimanya, tetapi sebaliknya si penerima tidak mempunyai kesempatan seperti itu, sebab perjanjian sudah lahir dan karenanya sudah mengikat dengan dikirimkannya jawaban persetujuan, sekalipun belum sampai pada orang yang menawarkan.

3. Teori Pengetahuan (*Vernemingstheorie*)

Menurut teori ini pada saat terjadinya kontrak kemudian digeser sampai pada jawaban akseptasinya diketahui oleh orang yang menawarkan. Berdasarkan teori ini, dapat dikatakan, bahwa dalam transaksi bisnis yang menggunakan *e-commerce*, kontrak terjadi pada saat *e-mail* atau pada saat form konfirmasi jawaban atas penawaran dibuka dan dibaca pihak yang memberikan penawaran. Teori pengetahuan ini sebenarnya sudah nampak baik dan adil, akan tetapi dapat menimbulkan masalah, yakni dalam hal penerima surat membiarkan dan tidak membuka suratnya, atau kepastian kapan surat itu benar-benar telah dibuka dan dibaca, karena yang tahu pasti hanya si penerima saja, maka ia bebas untuk mengundurkan saat lahirnya perjanjian.

4. Teori Penerimaan (*Ontvangstheorie*)

Sebagai jawaban atas kekurangan teori pengetahuan, maka muncullah teori lain, yaitu teori penerimaan. Dalam teori ini, saat diterimanya jawaban, terlepas dari apakah surat itu telah dibuka atau dibiarkan tidak dibuka, menentukan saat lahir/terjadinya perjanjian/ kontrak. Intinya adalah saat surat tersebut sampai pada alamat si penerima, maka saat itulah kontrak terjadi. Penerimaan ini harus terjadi selama penawaran masih terbuka. Penerimaan harus bersifat absolut dan tanpa syarat atas tawaran tersebut, sebagaimana adanya syarat yang melekat padanya atau sebagaimana telah diketahui syarat-syarat lain yang berlaku sebagai penolakan. Jika kita berpegang pada teori penerimaan ini, dalam menentukan saat terjadinya kontrak dalam transaksi jual beli *e-commerce*, maka dapat dikatakan bahwa sejak *email* jawaban atas penerimaan tawaran yang dikirimkan oleh pembeli

diterima oleh penjual, sejak saat itulah, terjadinya kontrak dalam transaksi bisnis yang menggunakan *e-commerce* ini.

Memperhatikan teori momentum terjadinya kontrak di atas, maka dapat disimpulkan bahwa momentum terjadinya transaksi jual beli *e-commerce* adalah bergantung pada dari sisi mana penjual dan konsumen pembeli menganggap kontrak tersebut telah terjadi. Akan tetapi dalam praktiknya momentum terjadinya transaksi jual beli *e-commerce* ini lebih dekat pada teori penerimaan. Hal tersebut karena bergantung pada proses atau mekanisme yang disediakan oleh pihak penjual dalam transaksi jual beli *e-commerce*. Untuk memperkuat argumentasi, penulis mengangkat contoh misalnya momentum terjadinya transaksi jual beli buku di situs palasarionline.com.

Ketika konsumen pembeli di situs palasarionline.com tertarik untuk menerima penawaran sejumlah buku, maka konsumen dapat meletakkannya di dalam *shopping cart*. Apabila konsumen pembeli telah selesai memilih buku yang sesuai keinginannya, maka konsumen pembeli dapat melakukan penyelesaian pemesanan dengan masuk ke dalam pilihan *shopping cart*. Dalam *shopping cart* apabila konsumen ingin membatalkan beberapa item buku, telah disediakan pilihan untuk membatalkan item yang dikehendaki. Jika telah yakin, maka konsumen diwajibkan untuk mengisi *form* berupa data identitas pembeli dan jenis pembayaran yang akan digunakan lalu kemudia *check out* sambil menunggu konfirmasi dari penjual melalui sms. Pada saat sms dari pihak penjual diterima, maka konsumen akan menerima *invoice* pemesanan berikut nomor *invoice*-nya.

Ketika *invoice* pemesanan ini telah diterima, pembeli dapat saja melanjutkan transaksi dengan melakukan pembayaran sesuai jumlah dalam *invoice* atau mengabaikan *invoice* tersebut (dengan kata lain tidak jadi membeli). Ketika konsumen melakukan pembayaran, konsumen perlu selanjutnya untuk melakukan konfirmasi pembayaran dengan *check in* pada palasarionline.com dengan mengisi *form* yang disediakan dengan benar. Pada saat konfirmasi pembayaran ini diterima, maka barulah kontrak jual beli telah terjadi. Penjual akan melaksanakan kewajibannya dengan mengirimkan buku yang dipesan kepada konsumen pembeli melalui kurir pengiriman barang.

Dari contoh yang telah penulis kemukakan di atas, walaupun momentum terjadinya kontrak atau transaksi jual beli *e-commerce* terjadi ketika penjual menerima konfirmasi pembayaran dari konsumen pembeli, akan tetapi proses jual beli *e-commerce* secara keseluruhan tidak bisa dilepaskan dalam kerangka tahapan kontrak jual beli pada umumnya. Tahapan transaksi jual beli *e-commerce* selalu dimulai dari penawaran dari penjual dan kemudian adanya penerimaan dari konsumen pembeli, kemudian ketika konsumen yakin akan barang pilihannya maka akan melakukan proses pembayaran, dan kemudian tahapan yang terakhir adalah pengiriman barang oleh penjual kepada konsumen pembeli.

Para pihak yang melakukan Transaksi Elektronik harus menggunakan Sistem Elektronik yang “disepakati”. Yang dimaksud dengan “disepakati” dalam pasal ini juga mencakup disepakatinya prosedur yang terdapat dalam

Sistem Elektronik yang bersangkutan. Kecuali ditentukan lain oleh para pihak, Transaksi Elektronik terjadi pada saat penawaran transaksi yang dikirim Pengirim telah diterima dan disetujui Penerima. Transaksi Elektronik terjadi pada saat kesepakatan antara para pihak yang dapat berupa, antara lain pengecekan data, identitas, nomor identifikasi pribadi (*personal identification number/PIN*) atau Sandi lewat (*password*). Persetujuan atas penawaran Transaksi Elektronik terjadi pada saat penawaran transaksi yang dikirim Pengirim telah diterima dan disetujui Penerima harus dilakukan dengan pernyataan penerimaan secara elektronik.

Dalam Pasal 5 Undang-undang Informasi dan Transaksi Elektronik tersebut Informasi dan Transaksi Elektronik ditentukan bahwa dokumen elektronis dan tandatangan digital (*digital signature*) tidak berlaku untuk pembuatan dan pelaksanaan surat wasiat, surat-surat berharga selain saham yang diperdagangkan di bursa efek, perjanjian yang berkaitan dengan barang tidak bergerak, dokumen-dokumen lain yang menurut peraturan perundang- undangan yang berlaku mengharuskan adanya pengesahan notaris atau pejabat yang berwenang. Ketentuan ini mengandung arti bahwa ada akta-akta otentik tertentu yang tidak dapat dibuat dalam bentuk elektronis.

D. Pengaturan UU ITE Terhadap Kontrak Jual Beli e-Commerce

Undang-undang Informasi dan Transaksi Elektronik mengatur secara khusus mengenai transaksi elektronik dalam Bab V undang-undang tersebut, yakni pada Pasal 17 s.d. Pasal 22 Undang-undang Informasi dan Transaksi Elektronik. Dalam Pasal 17 ayat (2), para pihak yang melakukan transaksi elektronik sebagaimana dimaksud

pada ayat (1) wajib beritikad baik dalam melakukan interaksi dan/ atau pertukaran informasi elektronik dan/ atau dokumen elektronik selama transaksi berlangsung. Pasal 18 ayat (1) Undang- undang Informasi dan Transaksi Elektronik mengatur bahwa Transaksi Elektronik yang dituangkan ke dalam Kontrak Elektronik mengikat para pihak. Selanjutnya, dalam Pasal 18 UU ITE ditentukan pula bahwa:

1. Transaksi Elektronik yang dituangkan ke dalam Kontrak Elektronik mengikat para pihak.
2. Para pihak memiliki kewenangan untuk memilih hukum yang berlaku bagi Transaksi Elektronik internasional yang dibuatnya.
3. Jika para pihak tidak melakukan pilihan hukum dalam Transaksi Elektronik internasional, hukum yang berlaku didasarkan pada asas Hukum Perdata Internasional.
4. Para pihak memiliki kewenangan untuk menetapkan forum pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternative lainnya yang berwenang manangani sengketa yang mungkin timbul dari Transaksi elektronik internasional yang dibuatnya.
5. Jika para pihak tidak melakukan pilihan forum tersebut, penetapan kewenangan pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari transaksi tersebut, didasarkan pada asas Hukum Perdata Internasional.

Beranjak dari isi ketentuan Pasal 18 tersebut dapat dikemukakan bahwa setiap transaksi elektronik harus dibuatkan dalam bentuk kontrak elektronik yang mengikat para pihak. Selain itu, para pihak diberi kewenangan untuk melakukan pilihan hukum (*choice of law*)

dan pilhan forum (*choice of forum*) dalam menyelesaikan segala sengketa yang berkenaan masalah dalam transaksi elektronik. Sebaliknya dalam UUITE sebagaimana yang dijelaskan dalam Pasal 18 tersebut dijelaskan bahwa: Dalam hal para pihak tidak melakukan pilhan forum, kewenangan forum berlaku berdasarkan prinsip atau asas hukum perdata internasional. Asas tersebut dikenal dengan asas tempat tinggal tergugat (*the basis of presence*) dan efektivitas yang menekankan pada tempat harta benda tergugat berada (*principle of effectiveness*).

Lalu, dalam Pasal 19 juga ditentukan: Para pihak yang melakukan Transaksi Elektronik harus menggunakan Sistem Elektronik yang disepakati. Lalu, dalam Penjelasannya dijelaskan bahwa; Yang dimaksud dengan "disepakati" dalam pasal ini juga mencakup disepakatinya prosedur yang terdapat dalam Sistem Elektronik yang bersangkutan. Lebih lanjut dalam Pasal 20 ditentukan:

1. Kecuali ditentukan lain oleh para pihak, Transaksi Elektronik terjadi pada saat penawaran transaksi yang dikirim Pengirim telah diterima dan disetujui Penerima.
2. Persetujuan atas penawaran Transaksi Elektronik tersebut harus dilakukan dengan pernyataan penerimaan secara elektronik.

Dalam Penjelasannya Pasal 20 ayat dijelaskan bahwa: Transaksi Elektronik terjadi pada saat kesepakatan antara para pihak yang dapat berupa, antara lain pengecekan data, identitas, nomor identifikasi pribadi (*personal identification number/PIN*) atau sandi lewat (*password*). Selain itu, dalam Pasal 21 ditentukan: Pengirim atau Penerima dapat melakukan Transaksi Elektronik sendiri, melalui pihak yang dikuasakan olehnya, atau melalui Agen Elektronik.

1. Pihak yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) diatur sebagai berikut:
 - a. Jika dilakukan sendiri, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab para pihak yang bertransaksi;
 - b. Jika dilakukan melalui pemberian kuasa, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab pemberi kuasa; atau
 - c. Jika dilakukan melalui Agen Elektronik, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab penyelenggara Agen Elektronik.
2. Jika kerugian Transaksi Elektronik disebabkan gagal beroperasinya Agen Elektronik akibat tindakan pihak ketiga secara langsung terhadap Sistem Elektronik, segala akibat hukum menjadi tanggung jawab penyelenggara Agen Elektronik.
3. Jika kerugian Transaksi Elektronik disebabkan gagal beroperasinya Agen Elektronik akibat kelalaian pihak pengguna jasa layanan, segala akibat hukum menjadi tanggung jawab pengguna jasa layanan.

Ketentuan sebagaimana dimaksud pada Pasal 21 ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/ atau kelalaian pihak pengguna Sistem Elektronik. Selanjutnya, dalam Pasal 22 UU ITTE juga ditentukan:

1. Penyelenggara Agen elektronik tertentu harus menyediakan fitur pada Agen elektronik yang dioperasikannya yang

memungkinkan penggunaannya melakukan perubahan informasi yang masih dalam proses transaksi.

2. Ketentuan lebih lanjut mengenai penyelenggara Agen elektronik tertentu sebagaimana yang dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah (PP).

Lalu, dalam Penjelasan Pasal 23 dijelaskan bahwa: Yang dimaksud dengan “fitur” adalah fasilitas yang memberikan kesempatan kepada pengguna Agen Elektronik untuk melakukan perubahan atas informasi yang disampaikannya, misalnya fasilitas pembatalan (*cancel*), edit, dan konfirmasi ulang.

E. Aspek Pengaturan Penyelenggaraan Sertifikasi Elektronik dan Tanda tangan Elektronik

Secara konseptual perlu diketahui makna yuridis dari Penyelenggaraan sistem elektronik, Penyelenggaraan sertifikasi elektronik, Penyelenggara sertifikasi elektronik dan sistem elektronik serta sistem sertifikasi elektronik.

Sehubungan dengan itu, dalam UU ITE telah memberikan batasan mengenai Penyelenggaraan sistem elektronik, yang mana dalam Pasal 1 butir 6 ditentukan: Penyelenggaraan sistem elektronik adalah pemanfaatan sistem elektronik oleh penyelenggara Negara, orang, badan usaha, dan/ atau masyarakat. Sedangkan batasan mengenai sistem elektronik diatur dalam Pasal 1 butir 5, yang secara tegas ditentukan: Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirim, dan/atau menyebarluaskan informasi elektronik.

Selanjutnya, dalam UU ITE Pasal 1 butir 10, ditentukan: Penyelenggara sertifikasi elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit sertifikat elektronik. Sementara itu, batasan mengenai sertifikasi elektronik telah diatur dalam Pasal 1 butir 9 yang secara tegas ditentukan: Sertifikasi elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik. Namun dalam UU ITE tidak memberikan suatu batasan mengenai pengertian penyelenggaraan sertifikasi elektronik.

Dalam kaitannya dengan pengertian penyelenggaraan sertifikasi dapat dikemukakan bahwa Penyelenggaraan Sertifikasi elektronik adalah suatu sistem dan prosedur yang dipakai atau digunakan serta ditetapkan oleh penyelenggara sertifikasi elektronik dalam upaya mencapai tujuannya berdasarkan ketentuan undang-undang ini dan peraturan pelaksanaan yang lainnya.

Dalam kaitannya dengan pengaturan mengenai penyelenggaraan sertifikasi, Sertifikasi elektronik dan Sistem elektronik tersebut telah diatur dalam UU ITE, yang mana dalam Pasal 13 ditentukan:

1. Setiap Orang berhak menggunakan jasa Penyelenggara Sertifikasi Elektronik untuk pembuatan Tanda Tangan Elektronik.
2. Penyelenggara Sertifikasi Elektronik harus memastikan keterkaitan suatu Tanda Tangan Elektronik dengan pemiliknya.
3. Penyelenggara Sertifikasi Elektronik terdiri atas:
 - a. Penyelenggara Sertifikasi Elektronik Indonesia; dan
 - b. Penyelenggara elektronik asing.

4. Penyelenggara Sertifikasi Elektronik Indonesia berbadan hukum Indonesia dan berdomisili di Indonesia.
5. Penyelenggara Sertifikasi Elektronik asing yang beroperasi di Indonesia harus terdaftar di Indonesia.
6. Ketentuan lebih lanjut mengenai Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Demikian pula dalam Pasal 14 ditentukan: Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud dalam Pasal 13 ayat (1) sampai dengan ayat (5) harus menyediakan informasi yang akurat, jelas, dan pasti kepada setiap pengguna jasa, yang meliputi:

1. Metode yang digunakan untuk mengidentifikasi Penanda Tangan;
2. Hal yang dapat digunakan untuk mengetahui data diri pembuat Tanda Tangan Elektronik; dan
3. Hal yang dapat digunakan untuk menunjukkan keberlakuan dan keamanan Tanda Tangan Elektronik.

Selanjutnya dalam Penjelasannya dijelaskan; Informasi sebagaimana dimaksud dalam hal ini adalah informasi yang minimum harus dipenuhi oleh setiap penyelenggara Tanda Tangan Elektronik. Tanda tangan elektronik adalah sebagaimana yang diatur dalam Pasal 1 butir 12 ditentukan: Tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.

Selain itu, dalam penyelenggaraan sistem elektronik, tentunya ada semacam pengaturan yang berkenaan dengan tanggung jawab atau hak dan kewajiban para penyelenggara sistem sertifikasi

elektronik. Dalam pada itu, bila memperhatikan isi ketentuan UU ITE dapat dikemukakan bahwa pengaturan mengenai hal tersebut telah diatur secara jelas pada Pasal 15, yang mana ditentukan:

1. Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.
2. Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.
3. Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Lebih lanjut, dalam Penjelasan Pasal 15 ayat (1) dijelaskan: "Andal" artinya Sistem Elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunaannya. "Aman" artinya Sistem Elektronik terlindungi secara fisik dan nonfisik. "Beroperasi sebagaimana mestinya" artinya Sistem Elektronik memiliki kemampuan sesuai dengan spesifikasinya. Demikian pula dalam Pasal 15 ayat (2) dijelaskan: Bertanggung jawab" artinya ada subjek hukum yang bertanggung jawab secara hukum terhadap Penyelenggaraan Sistem Elektronik tersebut. Selanjutnya dalam Pasal 16, ditentukan bahwa:

1. Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut:

- a. Dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;
 - b. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;
 - c. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;
 - d. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut;
 - e. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.
2. Ketentuan lebih lanjut tentang Penyelenggaraan Sistem Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Merujuk pada ketentuan yang dikemukakan di atas dapat dikemukakan bahwa dalam suatu penyelenggaraan sistem elektronik yang konsisten dan menjamin perlindungan hukum, kepastian hukum, dan keadilan hukum bagi semua pihak sesuai dengan kepentingan dan kebutuhannya masing-masing, maka dalam penyelenggaraan informasi para penyelenggara harus melaksanakan setiap unsur yang disyaratkan dan diembankan dalam undang-undang ini. Selain itu, tentunya berpulang kembali pada sistem penegakkan hukumnya dan kesadaran,

kepatuhan serta budaya hukum masyarakat atau pengguna dan penyelenggara itu sendiri dalam penyelenggaraan informasi dan transaksi elektronik itu sendiri.

Masalah data *message* erat kaitannya dengan *confidentiality*, *integrity* dan *authenticity* dari para pihak yang bertransaksi. Bagaimanakah memastikan bahwa data pesan yang sangat erat kaitannya dengan *privacy* pemesan, *confidentiality* para pihak dan pesanan, *integrity* dan *authenticity*, benar- benar data asli yang disepakati dan diakui oleh pihak pemesan? Hukum pembuktian di Indonesia sampai saat ini belum menjangkau pembuktian dengan menggunakan data *message* sebagai alat bukti di pengadilan.

Dalam suatu kontrak adanya tanda tangan diperlukan untuk menyatakan persetujuan dari para pihak yang menandatangani terhadap suatu kontrak. Tanda tangan juga dapat menjadi bukti bahwa para pihak telah mengetahui dan menyatakan keaslian dari suatu kontrak. Penandatanganan suatu dokumen secara umum mempunyai tujuan sebagai berikut:⁹²

- a. Bukti (*evidence*): suatu tanda tangan akan mengotentifikasi penandatanganan dengan dokumen yang ditandatanganinya. Pada saat penandatanganan membubuhkan tanda tangan dalam suatu bentuk yang khusus, tulisan tersebut akan mempunyai hubungan (*attribute*) dengan penandatangan;

⁹² Abdul Halim Barkatullah & Teguh Prasetyo, *Bisnis E-Commerce: Studi Sistem Keamanan dan Hukum di Indonesia* (Yogyakarta: Pustaka Pelajar, 2005), hlm 117

- b. *Ceremony*: penandatanganan suatu dokumen akan berakibat penandatangan tahu bahwa ia telah melakukan suatu perbuatan hukum, sehingga akan mengeliminasi kemungkinan adanya *inconsiderate engagement*.
- c. Persetujuan (*approval*): dalam penggunaannya dalam berbagai konteks baik oleh hukum atau oleh kebiasaan, tanda tangan melambangkan adanya persetujuan atau otorisasi terhadap suatu tulisan, atau penandatangan telah secara sadar mengetahui bahwa tanda tangan tersebut mempunyai konsekuensi hukum.

Ada yang berpendapat bahwa transaksi elektronik tanpa tanda tangan elektronik, kekuatannya sama dengan ucapan lisan. Artinya, selama pihak yang tersangkut dengan transaksi elektronik tersebut merasa bahwa tidak ada permasalahan, maka kontrak dalam transaksi elektronik itu mengikat. Namun akan terjadi masalah besar dalam pembuktian jika terjadi perselisihan mengenai transaksi elektronik tersebut.⁹³

Dalam Pasal 164 HIR (284 RBG) dan 1866 KUHPerdata ada lima alat bukti yang dapat diajukan dalam proses persidangan. Alat bukti itu adalah:

- a. Bukti tulisan;
- b. Bukti dengan saksi;
- c. Persangkaan-persangkaan;
- d. Pengakuan;
- e. Sumpah.

⁹³ *Ibid* hlm 85

Apabila melihat pada ketentuan ini, maka *digital signature* tidak dapat digunakan sebagai alat bukti atau akan ditolak baik oleh hakim maupun pihak lawan. Hal ini karena pembuktian yang dikehendaki berdasarkan pada ketentuan yang mensyaratkan bahwa alat bukti itu berupa tulisan, sementara *digital signature* sifatnya tanpa kertas bahkan merupakan *scriptless transaction*. Dokumen Elektronik yang merupakan setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya, dapat dijadikan sebagai alat bukti yang sah menurut Undang-undang tentang Teknologi Informasi dan Transaksi Elektronik, walaupun sulit untuk diklasifikasikan termasuk alat bukti yang sah yang mana sebagaimana dimaksud Pasal 184 ayat (1) Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana.⁹⁴

Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik⁹⁵ sesuai

⁹⁴ Pasal 184 ayat (1) Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana berbunyi: alat bukti yang sah ialah: a. keterangan saksi; b. keterangan ahli; c. surat; d. petunjuk; e. keterangan terdakwa.

⁹⁵ Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarluaskan Informasi Elektronik.

dengan ketentuan yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik, yaitu antara lain:

- a. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), Surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
- b. Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik yang merupakan alat bukti hukum yang sah, tidak berlaku untuk:

- a. Surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis, antara lain meliputi tetapi tidak terbatas pada surat berharga, surat yang berharga, dan surat yang digunakan dalam proses penegakan hukum acara perdata, pidana, dan administrasi negara.

- b. Surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaris atau akta yang dibuat oleh pejabat pembuat akta.

Dalam hal terdapat ketentuan lain selain yang diatur tentang ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik yang merupakan alat bukti hukum yang sah, tidak berlaku untuk surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis, antara lain meliputi tetapi tidak terbatas pada surat berharga, surat yang berharga, dan surat yang digunakan dalam proses penegakan hukum acara perdata, pidana, dan administrasi negara dan Surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaris atau akta yang dibuat oleh pejabat pembuat akta, yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Selama ini bentuk tertulis identik dengan informasi dan/atau dokumen yang tertuang di atas kertas semata, padahal pada hakikatnya informasi dan/atau dokumen dapat dituangkan ke dalam media apa saja, termasuk media elektronik. Dalam lingkup Sistem Elektronik, informasi yang asli dengan salinannya tidak relevan lagi untuk dibedakan sebab Sistem Elektronik pada dasarnya beroperasi dengan cara penggandaan yang mengakibatkan informasi yang asli tidak dapat dibedakan lagi dari salinannya.

Setiap orang yang menyatakan hak, memperkuat hak yang telah ada, atau menolak hak orang lain berdasarkan adanya Informasi Elektronik dan/atau Dokumen Elektronik harus memastikan bahwa Informasi Elektronik dan/atau Dokumen Elektronik yang ada padanya berasal dari Sistem Elektronik yang memenuhi syarat berdasarkan Peraturan Perundang-undangan. Ketentuan ini dimaksudkan bahwa suatu Informasi Elektronik dan/atau Dokumen Elektronik dapat digunakan sebagai alasan timbulnya suatu hak.

Kecuali diperjanjikan lain, waktu pengiriman suatu Informasi Elektronik dan/atau Dokumen Elektronik ditentukan pada saat Informasi Elektronik dan/atau Dokumen Elektronik telah dikirim dengan alamat yang benar oleh Pengirim ke suatu Sistem Elektronik yang ditunjuk atau dipergunakan Penerima dan telah memasuki Sistem Elektronik yang berada di luar kendali Pengirim dan waktu penerimaan suatu Informasi Elektronik dan/ atau Dokumen Elektronik ditentukan pada saat Informasi Elektronik dan/ atau Dokumen Elektronik memasuki Sistem Elektronik di bawah kendali Penerima yang berhak.

Dalam hal Penerima telah menunjuk suatu Sistem Elektronik tertentu untuk menerima Informasi Elektronik, penerimaan terjadi pada saat Informasi Elektronik dan/atau Dokumen Elektronik memasuki Sistem Elektronik yang ditunjuk. Dalam hal terdapat dua atau lebih sistem informasi yang digunakan dalam pengiriman atau penerimaan Informasi Elektronik dan/atau Dokumen Elektronik, maka:

Waktu pengiriman adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki sistem informasi pertama yang berada di luar kendali Pengirim.

- a. Waktu penerimaan adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki sistem informasi terakhir yang berada di bawah kendali Penerima.
- b. Pelaku usaha yang menawarkan produk melalui Sistem Elektronik harus menyediakan “informasi yang lengkap dan benar” berkaitan dengan syarat kontrak, produsen, dan produk yang ditawarkan.

Yang dimaksud dengan “informasi yang lengkap dan benar” meliputi:

- a. Informasi yang memuat identitas serta status subjek hukum dan kompetensinya, baik sebagai produsen, pemasok, penyelenggara maupun perantara.
- b. Informasi lain yang menjelaskan hal tertentu yang menjadi syarat sahnya perjanjian serta menjelaskan barang dan/atau jasa yang ditawarkan, seperti nama, alamat, dan deskripsi barang/jasa.

Setiap pelaku usaha yang menyelenggarakan Transaksi Elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan. Sertifikasi Keandalan dimaksudkan sebagai bukti bahwa pelaku usaha yang melakukan perdagangan secara elektronik layak berusaha setelah melalui penilaian dan audit dari badan yang berwenang. Bukti telah dilakukan Sertifikasi Keandalan ditunjukkan dengan adanya logo Sertifikasi berupa *trust mark* pada halaman (*home page*) pelaku usaha tersebut. Ketentuan mengenai pembentukan Lembaga Sertifikasi Keandalan diatur dengan Peraturan Pemerintah.

Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:

1. Data pembuatan Tanda Tangan Elektronik terkait hanya kepada Penanda Tangan.
2. Data pembuatan Tanda Tangan Elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penanda Tangan.
3. Segala perubahan terhadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui.
4. Segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui.
5. Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa Penandatangannya, dan
6. Terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait.

Undang-Undang Informasi dan Transaksi Elektronik memberikan pengakuan secara tegas bahwa meskipun hanya merupakan suatu kode, Tanda Tangan Elektronik memiliki kedudukan yang sama dengan tanda tangan manual pada umumnya yang memiliki kekuatan hukum dan akibat hukum.

Persyaratan-persyaratan yang tersebut huruf a sampai dengan f merupakan persyaratan minimum yang harus dipenuhi dalam Setiap Tanda Tangan Elektronik. Ketentuan ini membuka kesempatan seluas-luasnya kepada siapa pun untuk

mengembangkan metode, teknik, atau proses pembuatan Tanda Tangan Elektronik.

Ketentuan lebih lanjut tentang Tanda Tangan Elektronik diatur dengan Peraturan Pemerintah. Peraturan Pemerintah dimaksud, antara lain, mengatur tentang teknik, metode, sarana, dan proses pembuatan Tanda Tangan Elektronik. Setiap orang yang terlibat dalam Tanda Tangan Elektronik berkewajiban memberikan pengamanan atas Tanda Tangan Elektronik yang digunakannya. Pengamanan Tanda Tangan Elektronik tersebut sekurang-kurangnya meliputi:

1. Sistem tidak dapat diakses oleh orang lain yang tidak berhak;
2. Penanda Tangan harus menerapkan prinsip kehati-hatian untuk menghindari penggunaan secara tidak sah terhadap data terkait pembuatan Tanda Tangan Elektronik.
3. Penanda Tangan harus tanpa menunda-nunda, menggunakan cara yang dianjurkan oleh penyelenggara Tanda Tangan Elektronik ataupun cara lain yang layak dan sepatutnya harus segera memberitahukan kepada seseorang yang oleh Penanda Tangan dianggap memercayai Tanda Tangan Elektronik atau kepada pihak pendukung layanan Tanda Tangan Elektronik jika:
 - a. Penanda Tangan mengetahui bahwa data pembuatan Tanda Tangan Elektronik telah dibobol; atau
 - b. Keadaan yang diketahui oleh Penanda Tangan dapat menimbulkan risiko yang berarti, kemungkinan akibat bobolnya data pembuatan Tanda Tangan Elektronik; dan

4. Dalam hal Sertifikat Elektronik digunakan untuk mendukung Tanda Tangan Elektronik, Penanda Tangan harus memastikan kebenaran dan keutuhan semua informasi yang terkait dengan Sertifikat Elektronik tersebut. Setiap orang yang melakukan pelanggaran ketentuan mengenai Tanda Tangan Elektronik yang berkewajiban memberikan pengamanan atas Tanda Tangan Elektronik yang digunakannya, bertanggung jawab atas segala kerugian dan konsekuensi hukum yang timbul.

F. Sistem Pembayaran Transaksi Elektronik

Internet mengalami perkembangan yang sangat cepat baik dilihat dari segi jumlah pengguna maupun nilai bisnis didalamnya. Kalangan bisnis berusaha untuk memanfaatkan fenomena ini sebagai strategi *marketing* yang baru dan juga media penjualan yang baru. Berbagai barang dan jasa tersedia disini mulai dari barang (*informasi digital*) seperti software dan lagu sampai dengan jasa seperti layanan perbankan. Berbagai jenis barang dan jasa ini membutuhkan adanya teknologi pembayaran yang mendukung transaksi di dunia maya ini.

Sistem pembayaran yang ada pada saat ini dapat dikategorikan menjadi 5 sebagai berikut:

1. COD (*cash on delivery*)

COD (*cash on delivery*) atau pembayaran di tempat. Metode pembayaran ini hanya untuk wilayah terdekat, atau daerah lain yang dia memiliki jaringan di daerah itu, dan pembeli membayar barang yang dipesan setelah barang tersebut tiba di tempat;

2. Transfer Bank

Transfer Bank, jika memilih untuk membayar melalui transfer, dapat mentrasferkan uang ke rekening Penjual. Pembeli mentransfer (transfer dapat dilakukan dengan cara setor tunai, transfer via ATM atau melalui klikbca) jumlah yang di order paling lama 3 hari setelah melakukan transaksi dan mengirimkan bukti transfer via email atau melalui faks. Setelah dana yang ditransfer masuk dan bukti transfer di terima sanur, barang yang di pesan segera dikirimkan.

3. Sistem Debit

Sistem ini mengharuskan konsumen terlebih dahulu mempunyai rekening di suatu bank. Apabila ia akan melakukan suatu pembayaran maka pembayaran itu akan diambil dari rekening tersebut dengan cara di debit. Contoh dari sistem ini adalah: *Bank Internet Payment System* (BIPS), FSTC *Electronic Check* (Echeck) (www.echeck.org), *Open Financial Exchange* (OFX). (www.ofx.org)

4. Kartu Kredit (*Credit Card*)

Penjual dapat menggunakan jasa bank yang mempunyai hubungan dengan jaringan *Credit Card* Internasional, misalnya *Mastercard*, *JSB* dan *Visa*. Setelah order selesai dan pembeli memilih pembayaran dengan kartu kredit, maka pembeli akan terhubung ke Bank selaku *payment gateway*. Pengisian semua data mengenai kartu kredit dilakukan pada *payment gateway* tersebut. Tugas Penjual hanya meng-chek apakah ada transaksi dengan CC dan cross chek dengan Bank apakah CC yang digunakan valid. Sistem ini mengalihkan kewajiban pembayaran kepada pihak ke3 (kredit) baru kemudian kredit ini akan ditagih kepada orang yang bersangkutan. Pedagang akan melakukan proses *capture* yaitu meminta pembayaran dari pihak

ke-3 yang menjadi perantara. Sistem ini terdiri dari *Credit Card Over HTTP/SSL* dan *SET*. Sistem yang menggunakan SSL banyak digunakan oleh internet *merchant* pada saat ini. Internet *merchant* akan menggunakan SSL dalam meng-*encrypt* proses capture dari nomer kartu kredit yang digunakan.

Kata “kredit” lazim dipergunakan dalam Perbankan untuk pemberian fasilitas yang berkaitan dengan pinjaman. Kata “kredit” dijumpai pula dalam penerbitan kartu yang dikeluarkan oleh lembaga keuangan, baik Bank atau Lembaga Keuangan Bukan Bank (LKBB). Asal kata “kredit” berasal dari bahasa Romawi “credere” yang berarti percaya atau “credo” atau “creditum” yang berarti saya percaya.

Black's Law Dictionary memberi pengertian bahwa kredit adalah, yang Artinya: “Kemampuan seoang pelaku usaha untuk meminjamkan uang, atau memperoleh barang-barang secara tepat waktu, sebagai akibat dari argumentasi yang tepat dari pemberi pinjaman, seperti halnya keandalan dan kemampuan membayarnya.⁹⁶

Sedangkan menurut Undang-Undang No. 10 Tahun 1998 tentang Perbankan Pasal 1 ayat 11 menyebutkan bahwa kredit adalah penyediaan uang atau tagihan yang dapat dipersamakan dengan itu, berdasarkan persetujuan atau kesepakatan pinjam meminjam antara bank dengan pihak lain yang mewajibkan pihak peminjam untuk melunasi hutangnya setelah jangka waktu tertentu dengan pemberian bunga.

⁹⁶ Johannes Ibrahim, 2004, *Dilematis Antara Kontrak Dan Kejahatan*, Refika Aditama, Bandung, hlm. 7.

Pengertian kartu kredit menurut Peraturan Bank Indonesia No.14 /2/PBI/2012 tanggal Januari 2012, perihal Perubahan atas Peraturan Bank Indonesia No. 11/11/PBI 2009 tentang Penyelenggaraan Kegiatan Alat Pembayaran dengan Menggunakan Kartu, pasal 1 ayat 4, Kartu kredit adalah alat pembayaran dengan menggunakan kartu (APMK) yang dapat digunakan untuk melakukan pembayaran atas kewajiban yang timbul dari suatu kegiatan ekonomi, termasuk transaksi pembelanjaan dan/atau untuk melakukan penarikan tunai, dimana kewajiban pembayaran pemegang kartu dipenuhi terlebih dahulu oleh acquirer atau penerbit, dan pemegang kartu berkewajiban untuk melakukan pembayaran pada waktu yang disepakati, baik dengan pelunasan secara sekaligus (change card) ataupun dengan pembayaran secara angsuran.⁹⁷

Menurut A. F. Elly Erawaty dan J. S. Badudu kartu kredit adalah “Kartu yang dikeluarkan oleh bank atau lembaga lain yang diterbitkan dengan tujuan untuk mendapatkan uang, barang atau jasa secara kredit ”.⁹⁸

Emmy Pangaribuan br. Simanjuntak mengatakan kartu kredit adalah suatu kartu yang memberikan hak kepada pemegangnya atas penunjukan dari kartu itu dan dengan menandatangani formulir rekening pada suatu perusahaan dapat memperoleh barang atau jasa tanpa perlu membayar secara langsung. ⁹⁹

⁹⁷ Indonesia, Ikatan Bankir. 2015. *Bisnis Kredit Perbankan*. Jakarta: Gramedia Pustaka Utama. hlm. 193

⁹⁸ A. F.Eddy Erawaty dan J. S. Badudu, 1996, *Kamus Hukum Ekonomi*, Jakarta: ELIPS, hlm. 27

⁹⁹ Emmy Pangaribuan br Simanjuntak, 1991, *Surat Berharga*, Jakarta: Media Cipta, hlm. 2

Muhammad Djumhana memberikan definisi kartu kredit adalah alat pembayaran pengganti uang tunai.¹⁰⁰ Munir Fuady mengatakan kartu kredit merupakan suatu kartu yang pada umumnya dibuat dari plastik dengan dibubuhkan identitas dari pemegang dan penerbit (card issuer) yang memberikan hak terhadap siapa kartu kredit diisukan untuk menandatangani tanda pelunasan pembayaran harga dari jasa atau barang yang dibeli dari tempat-tempat tertentu seperti toko, hotel, restoran, penjual tiket pengangkutan dan lain-lain.¹⁰¹

Menurut *Dictionary of economic* kartu kredit adalah "Kartu plastik atau sejenis kartu pembiayaan yang digunakan pembelian produk secara kredit. Kartu kredit dikeluarkan oleh bank komersial, jaringan hotel dan pedagang".¹⁰² Menurut A. F. Elly Erawaty dan J. S. Badudu kartu kredit adalah "Kartu yang dikeluarkan oleh bank atau lembaga lain yang diterbitkan dengan tujuan untuk mendapatkan uang, barang atau jasa secara kredit".¹⁰³

Dari definisi di atas, dapat disimpulkan bahwa kartu kredit atau *credit card* adalah uang plastik yang diterbitkan oleh suatu institusi yang memungkinkan pemegang kartu untuk memperoleh kredit atas transaksi yang dilakukannya dan pembayarannya dapat dilakukan secara angsuran dengan membayar sejumlah bunga (*finance charge*) atau sekaligus pada

¹⁰⁰ Muhammad Djumhana, 2000, *Hukum Perbankan di Indonesia*, Bandung: Citra Aditya Bakti, hlm. 192

¹⁰¹ Munir Fuady, 1995, *Hukum tentang Pembiayaan dalam Teori dan Praktik*, Bandung: Citra Aditya Bakti, hlm. 217

¹⁰² Collins, 1988, *Dictionary of Economics*, Collins Reference, Cambrige, h. 105.

¹⁰³ A. F. Elly Erawaty dan J. S. Badudu, 1996, *Kamus Hukum Ekonomi*, ELIPS, Jakarta, hlm.

waktu yang telah ditentukan. Nasabah hanya akan dikenai iuran tahunan yang besarnya ditetapkan oleh pihak bank.

Fungsi kartu kredit antara lain adalah sebagai berikut:¹⁰⁴

- a. Kartu kredit sebagai dana *emergency*, dana *emergency* berbeda dengan dana tambahan ataupun dana cadangan. Yang dimaksud dengan dana *emergency* yaitu dana yang dapat digunakan untuk keperluan yang sifatnya gawat darurat atau mendadak, misalnya seperti: harus operasi mendadak, mau melahirkan tapi belum ada biaya dan lain-lain, itulah kegunaan dana *emergency*.
- b. Kartu kredit sebagai dana *opportunity*, yang dimaksud dengan dana *opportunity* yaitu untuk mengambil peluang bisnis ataupun berinvestasi, yang belum tentu saat peluang atau kesempatan itu datang kita ada dana untuk mengambilnya.
- c. Kartu kredit dapat digunakan untuk mengumpulkan semua bentuk pengeluaran belanja dalam satu tagihan, sehingga waktu yang kita keluarkan dapat lebih efisien. Bahkan saat ini ada kartu kredit yang memiliki fasilitas untuk membayar pengeluaran rutin, misalnya seperti: tagihan listrik, tagihan telepon, tagihan air dan tagihan lainnya.
- d. Kartu kredit dapat digunakan untuk mencatat biaya yang kita keluarkan secara rutin, sehingga dapat mempermudah kita dalam mengelola keuangan. Biaya yang di keluarkan atau pengeluaran akan tertera jelas di rekening giro, dapat melakukan cross checking di rumah pada akhir bulan.

¹⁰⁴ <http://www.bnicalcenter.co.id/Aplikasi-Merchant/Joint-erchant/Ketentuan-Umum.aspx> diakses pada tanggal 17 mei 2016

- e. Kartu kredit tertentu dapat memberikan servis asuransi kesehatan, pencurian, perjalanan maupun kerusakan barang yang dibeli dengan kartu tersebut (hal ini perlu dibicarakan pada bank ketika transaksi).
 - f. Kartu kredit dapat digunakan untuk transaksi tarik tunai melalui mesin EDC (Electronic Data Capture) di merchant-merchant yang menyediakan jasa gesek tunai maupun melalui ATM (Automatic Teller Machine) atau teller bank.
 - g. Kartu kredit dapat dipergunakan dalam berbagai transaksi elektronik (di dunia maya), yang menyediakan sistem pembayaran yang dapat menerima sistem pembayaran dengan kartu kredit.
5. Uang digital (e-money) "Tunai" atau "electronic "cash"/digital cash
- a. Uang Digital

Sistem pembayaran baru seperti halnya uang digital ini hanya berhasil apabila keberadaannya diterima oleh banyak orang. Untuk meraih penerimaan ini semua pihak yang terlibat harus memetik cukup banyak keuntungan melebihi dari "biaya" yang harus ditanggungnya:

 - 1) Minat utama *customer* adalah membawa alat pembelian ini senyaman mungkin. Pembayaran harus dapat dilakukan dari rumah dengan cara yang mudah dan efisien.
 - 2) Dealer (merchant) bisa saja memetik fee dari transaksi (namun sebaiknya tidak). Di lain pihak, keuntungan yang diraihnya adalah memperbaiki citra sebagai merchant yang inovatif dan mungkin meningkatkan

penjualan. Ia barangkali bisa juga mengurangi kantor cabang dan orang-orang penjualan.

- 3) Arsitek sistem bertanggung jawab terhadap pengembangan sistem pembayaran. Keuntungan mereka adalah *royalty* dan *fee* dari layanan. Prasyaratnya adalah penerimaan yang luas dari sistem mereka dan penggunaannya.
- 4) Penyedia sistem (*system provider*) menjadi pihak penengah. Penjualan dealer diteruskan ke institusi keuangan. Penyedia sistem bertanggung jawab terhadap *clearance* transaksi. Ia menyediakan pula layanan (manajemen problem, pelatihan pengguna). Pendapatan berasal dari *fee* dan tarikan (charge) atas layanan yang ia sediakan.
- 5) Institusi keuangan dapat mempromosikan sistem tertentu. Kepercayaan terhadap sistem pembayaran elektronik merupakan kunci keberhasilan. Hambatannya barangkali adalah masalah know how.
- 6) Trust center mengontrol kunci signature digital. Bertanggung jawab terhadap integritas data yang ditransmisikan dan otentifikasi. Trust center memberikan pengamanan pada sistem pembayaran tertentu. Penerimaan mereka berasal dari *royalty* dan *fee* layanan-layanan lain.

b. Sistem *Micro* dan *Pico Payment*

- 1) Sistem yang terbuka membutuhkan fasilitas *security* untuk menangani pembayaran elektronik. Security dapat diwujudkan dengan metode kriptografi yang berhubungan dengan nomor transaksi.

- 2) Sejumlah besar customer harus dapat melakukan transaksi pembayaran secara serentak. Sistem harus dapat melayani banyak pengguna dan mudah untuk dikembangkan. Scalability merupakan kriteria yang penting.
- 3) Pembayaran skala kecil (micro dan pico payment) semestinya dimungkinkan. Sistem akuntansi yang berkaitan dengannya mesti efektif dan efisien. Oleh karenanya, baiya per transaksi harus rendah.
- 4) Sistem harus transparan. Customer mesti tahu kalau telah terjadi pembayaran. Penggunaan sistem mesti sederhana dan gampang dimengerti.
- 5) Rumah tangga semestinya bisa menerima uang digital ini (sebagai micro merchant misalnya).
- 6) Uang digital terdiri atas susunan bit. Adalah mungkin untuk membuat duplikasi koin dan kemudian meletakkanya ke dalam sirkulasi uang digital. Fenomena ini dikenal dengan "pembelanjaan ganda" atau "menggandakan uang digital". Sistem pembayaran harus menyediakan mekanisme untuk mengetahui atau mencegah adanya pembelanjaan ganda.
- 7) Uang digital harus dapat dikonversi kembali menjadi uang nyata, jika dibutuhkan.
- 8) Untuk menjamin tingkat kepercayaan, nilai tukar antara uang digital dan uang nyata harus stabil (demikian pula antar uang digital itu sendiri).

9) Uang digital disimpan di hard disk lokal atau media lain. Pada kasus disk crash atau media yang rusak, harus tersedia suatu cara untuk memulihkan kembali.

Sistem ini merupakan salah satu perkembangan yang paling akhir dalam internet payment. Sistem ini dalam penggunaannya mirip dengan pemakaian uang tunai dalam kegiatan sehari-hari. Kemiripan ini adalah dalam hal konsumen akan membayar koin atau uang kertas kepada penjual dalam proses pembayaran sehari-hari.

Dalam sistem ini uang tunai ini akan digantikan oleh digital token atau suatu nilai digital (digital value) kepada penjual. Beberapa sistem memungkinkan penjual untuk langsung membelanjakan "uang" yang didapatnya untuk membayar suatu barang atau jasa.

Sistem yang lain mengharuskan "uang" tersebut disetorkan terlebih dahulu ke dalam suatu rekening baru setelah itu bank akan menerbitkan token yang baru yang dapat dipakai untuk berbelanja. Beberapa contoh dari sistem ini adalah Mondex, (<http://www.mondex.com>) Proton, VisaCash Ecash (<http://www.digicash.com>), Millicent (<http://www.millicent.digital.com>), CyberCoin (<http://www.cybercash.com>), WorldPay.

c. Millicent

Produk dari *Digital Equipment Corp (DEC)*, *Millicent* berbasis *scrip*. Tidak seperti *scrip* tradisional yang setiap pedagang (*merchant*) menjual *scrip* langsung ke calon pembeli, *Millicent* mengandalkan *scrip broker*. Pialang (*broker*), bisa berupa bank atau asosiasi bank, adalah pihak

ketiga yang menerima pembayaran dari konsumen di *front-end* dan kredit *scrip* dari *merchant* di *back-end*. Pialang menerbitkan *scrip*-nya sendiri ke konsumen. Dengan demikian, antara merchant dan konsumen tidak perlu memiliki hubungan sebelum melakukan transaksi.

Seperti halnya uang receh, yang dipakai pada pembayaran skala kecil yang ringan, Millicent juga didesain sebagai sarana pembayaran *e-commerce* kelas ringan. Agar biaya transaksi yang ringan ini tidak menjadi lebih besar dari nilai transaksinya itu sendiri dan efektif dari segi biaya, Millicent mengorbankan *security*. Para perancangnya mengasumsikan bahwa *fraud* pasti akan terjadi, tetapi jumlahnya akan kecil saja dan dapat diabaikan. Secara teknis, sebetulnya *Millicent* bisa saja menerapkan teknik enkripsi (penyandian) yang lebih rumit dan mekanisme prosedur sekuriti yang lebih berlapis dan ketat, namun ongkos komputasi dan administratif mungkin akan lebih besar dari nilai transaksinya itu sendiri.

Skema mini *payment* berbentang transaksi dari angka sekitar 0,25 US\$ sampai 10 US\$. Dari aspek sekuriti, asumsi pengabaian dari para perancangnya merupakan celah [STEWA99]. Jika saja seorang hacker dapat berperan sebagai pialang dan memfilter tiap sepersepuluh sen US\$ dari setiap transaksi scrip, maka hasil yang diperolehnya bisa saja banyak sekali. Sedikit demi sedikit kan lama-lama jadi bukit.¹⁰⁵

¹⁰⁵ www.research.digital.com/SRC/personal/stev eg/millicent/millicent.html diakses pada tanggal 23 Desember 2022 Pukul 19.00 WIB

d. *Cash dari DigiCash*

DigiCash meluncurkan satu sistem yang disebut dengan *eCash*, merupakan sistem pembawa sertifikat (*certificate bearer*), yang berarti siapapun yang saat itu sedang memegang *eCash* adalah yang memegang nilai moneternya. Mark Twain Bank di St Louis adalah yang pertama (mungkin masih satu-satunya) penerbit *eCash* di AS, tetapi telah menandatangani kesepakatan-kesepakatan dengan beberapa bank. Dengan *eCash*, konsumen membangkitkan token *eCash* lewat perangkat lunak “dompet” (purse software) yang diedarkan *DigiCash*. Konsumen membangkitkan token *eCash*, lalu mengirimkannya (tersembunyi dalam amplop digital) ke bank guna sertifikasi. Bank kemudian mencap token-token yang dikirim oleh konsumen tadi dengan signature untuk setiap token, mendebet rekening konsumen untuk setiap *eCash* yang dicapnya, lalu mengirimkannya kembali ke konsumen lewat Internet. Bank tidak akan melihat lagi token-token tersebut, sampai token tersebut hadir kembali setelah dibawa oleh penagih ke bank.

Karena seluruh sistem ini berbasis perangkat lunak, maka menduplikasi token *eCash* yang telah disertifikasi oleh bank, bukan perkara yang mustahil. Bukankah uang digital hanyalah sekadar susunan bit belaka? Tidak ada yang dapat menghentikan konsumen untuk melakukan duplikasi token *eCash* yang sudah disertifikasi.

Oleh karena itu, setiap kali terjadi transaksi *eCash*, *merchant* harus melakukan koneksi *online real-time* ke bank penerbit untuk memastikan bahwa token tersebut belum

pernah dipakai, belum dibelikan oleh konsumen, atau belum ditagihkan oleh *merchant* lain. Masing-masing token yang sedang dibelanjakan tadi dicocokkan dengan daftar token-token yang sudah ditagih. Jika konsumennya jujur dan bermain sesuai aturan main, maka tentu saja tidak ada token yang sama, dan transaksi pun boleh berlangsung. Jika ada token yang sama, transaksi gagal (karena konsumen barangkali telah menggandakan uangnya).

e. CyberCoin dari CyberCash

CyberCash meluncurkan uang digitalnya sendiri bulan Oktober 1996. *CyberCoin* bersandar pada sistem notasional, bukan model certificate bearer. Seperti halnya skema uang digital lainnya, konsumen harus membayar terlebih dulu (prepay) *CyberCoin*.

Kunci pembeda antara *CyberCoin* dan model-model lainnya adalah nilai uang digital tidak ditransfer ke PC konsumen, kartu chip, atau *CyberCash Wallet*. Ketika konsumen melakukan transaksi dengan merchant, *CyberCoin* ditransfer dari *CyberCash Wallet* milik konsumen ke *CashRegister* milik merchant, menggunakan *CyberCash* sebagai prosesor sentral dari transaksi ini. *CyberCash* cukup merekam siapa konsumen yang membayar ke merchant mana dan berapa jumlahnya.

Lantaran setiap transaksi tidak membutuhkan kliring antar bank dan settlement, menjadikan *CyberCash* bahkan cocok untuk transaksi ringan mulai dari 0,25 US\$. Sistem *CyberCash* menawarkan solusi yang beresiko kecil bagi institusi finansial. Merchant ataupun konsumen tidak akan bisa memalsu *CyberCoin*, sebab sistem ini bukan bearer

certificates. Tidak ada yang dapat memasukkan nilai uang ke sistem. CyberCash mengetahui secara pasti berapa besar CyberCoin yang telah dibeli atau ditransfer, dan mengendalikan dananya.

Barangkali resiko terbesar adalah dari sisi konsumen, bila orang lain dapat mengakses PC-nya, kemudian melakukan pembelian menggunakan CyberCoin. Namun resiko ini dijumpai di semua sistem berbasis perangkat lunak. CyberCash berupaya keras untuk mendistribusikan perangkat lunak *Wallet* miliknya lewat produk-produk perangkat lunak macam *browser Netscape*. Distribusi *Wallet* yang besar akan membantu mensolidkan posisi *CyberCash* sebagai prosesor pembayaran untuk transaksi lewat Internet.

f. Mondex

Tidak seperti sistem-sistem pembayaran Internet lainnya, Mondex dilahirkan dari dunia off-line dan bermigrasi ke Internet. Mondex sepenuhnya berbasis chip card, dan ia unik sebab mampu melakukan transfer card-to-card.

Seperti sistem eCash, Mondex memakai model pembawa sertifikat, yaitu dana disimpan secara remote di kartu setiap pengguna. Namun tidak seperti eCash, dana-dana Mondex dapat ditransfer dari satu card ke card yang lain, tanpa membutuhkan kliring terpusat atau verifikasi oleh bank. Sehingga dari sudut pandang dunia nyata, Mondex inilah uang digital yang paling dekat dengan uang nyata. Kunci pembeda antara Mondex dan uang nyata adalah jejak audit yang disediakan oleh Mondex. Kartu

Mondex merekam setiap transaksi dengan penciri unik yang dapat dimanfaatkan untuk menjelaki dana bila dibutuhkan. Kunci Mondex adalah sekuritinya, yang terdapat pada dua aspek primer sistem: perangkat keras card dan proses transfer nilai. Dana tidak dapat berada di mana saja, kecuali di dalam kartu Mondex. Bahkan penerbit sentral Mondex pun mengandalkan pada card-card Mondex untuk menyimpan nilai uang masing-masing.

Kartu Mondex mampu mendeteksi spoof dan menolak transfer uang ke card palsu. Andalannya adalah bahwa setiap kartu disertifikasi dengan digital signature Mondex. Proses transfer nilai juga aman. Ketika terjadi transfer antara konsumen dan merchant umpamanya, dua kartu itu tidak hanya melakukan verifikasi otentikasi satu sama lain, tetapi transfer hanya terjadi secara sekuensial sehingga tidak mungkin dana berada di dua tempat pada saat yang sama. Dana ditarik dari kartu konsumen sebelum dituliskan ke kartu merchant.

Satu-satunya hambatan dari sistem Mondex, karena sistem ini adalah sistem yang berbasis card, barangkali adalah bahwa ia membutuhkan card reader di tangan konsumen dan merchant. Ini bukan perkara yang remeh. Boleh jadi ini menjadi salah satu faktor mengapa DigiCash hanya berbasis perangkat lunak.

Mondex memahami hambatan ini dengan berusaha memperkenalkan peranti seperti *VeriFone VeriSmart card reader* dengan harga sekitar 100 US\$ dan harganya cenderung menurun dari waktu ke waktu.

Yang dianggap justru lebih signifikan adalah penghalang ekonomi; masih belum jelas bagaimana bank dapat menarik keuntungan dari transaksi dengan Mondex. Mulai dari penerbitan uang Mondex, mungkin bisa diperoleh bila institusi finansial membeli (“kulakan”) lebih dulu uang Mondex dari Mondex sendiri, baru kemudian menjualnya ke konsumen. Setelah uang Mondex beredar di pasaran, tipis sekali kemungkinan institusi keuangan akan memperoleh keuntungan karena pertukaran uang Mondex tidak membutuhkan keterlibatan insitusi finansial, sehingga mereka tidak dapat menarik *fee* transaksi.

g. Visa Cash

Visa Cash menjawab beberapa pertanyaan ekonomi yang diajukan kepada Mondex, terutama tentang bagaimana institusi keuangan dapat memetik keuntungan. Visa Cash adalah produk bearer certificate dari Visa yang berbasis chip card. Sembarang bank Visa dapat menerbitkan Visa Cash dan menikmati keuntungan, dan dalam kasus kartu Visa Cash yang dibuang adalah nilai sisa yang terlupakan atau terbuang oleh konsumen.

Visa Cash memang lebih mudah dijual ke industri perbankan dari perspektif finansial, tetapi tidak memiliki keleluasaan sebebas Mondex. Dengan Mondex, pengguna dapat mentransfer uang dari satu kartu ke kartu lain tanpa batas, sesuatu yang tidak dapat dinikmati oleh pengguna Visa Cash.

DAFTAR PUSTAKA

BUKU

- A. F.Elly Erawaty dan J. S. Badudu. 1996, Kamus Hukum Ekonomi, Jakarta:
ELIPS
- Abdul Halim Barkatullah & Teguh Prasetyo. 2005 Bisnis E-Commerce:
Studi Sistem Keamanan dan Hukum di Indonesia Yogyakarta:
Pustaka Pelajar
- Abdul Wahid dan Mohammad Labib. 2005. Kejahatan Mayaantara
(Cybercrime), Bandung : PT Refika Aditama,
- Abu Bakar Munir. 1999. Cyber Law Policies and Challenges.
- Ahmad M Ramli. 2004. Prinsip-prinsip Cyber Law Dan Kendala Hukum
Positif Dalam Menanggulangi Cyber Crime, Fakultas Hukum
Universitas Padjajaran
- Ahmad M. Ramli. 2004. Cyber Law dan HAKI dalam Sistem Hukum
Indonesia, Bandung: Refika Aditama
- Andi Hamzah. 1993. Hukum Pidana yang berkaitan dengan komputer,
Jakarta : Sinar Grafika Offset,
- Anonymous. 2008 "Konsideran Undang-undang Nomor 11 Tahun 2008
tentang Informasi dan Transaksi Elektronik". Surabaya : Kesindo
Utama.
- Bajaj, Kamlesh K., Debjani Nag. 2000. E-Commerce: The Cutting Edge of
Business, Tata McGraw-Hill Book Co-Singapore : International
Editions.
- Christine S.T. Kansil, SH. 1997, Modul Hukum Administrasi Negara,
Jakarta : PT Pradnya Paramita

- Celina Tri Siwi Kristiyanti. 2009. "Hukum Perlindungan Konsumen". Jakarta : Sinar Grafika.
- Collins. 1988. Dictionary of Economics, Collins Reference. Cambridge
- David Bainbridge. 1996. Introduction to Computer Law, 3 nd Edition Landon: Pitman Publishing,
- E.K.M. Masinambow, ed, 2000 Hukum dan Kemajemukan Budaya, Sumbangan Karangan Untuk Menyambut Hari Ulang Tahun ke-70 Prof. Dr. T.O. Ihromi Jakarta: Yayasan Obor Indonesia
- Edmon Makarim, 2005. Pengantar Hukum Telematika Suatu Kajian Kompilasi. Jakarta : PT Raja Grafindo Persada,
- Emmy Pangaribuan br Simanjuntak, 1991, Surat Berharga, Jakarta: Media Cipta,
- F.Eddy Erawaty dan J. S. Badudu. 1996. Kamus Hukum Ekonomi. ELIPS, Jakarta
- G.Salim HS. 2010. Perkembangan Teori Dalam Ilmu Hukum. Jakarta: PT Raja Grafindo Persada,
- Global Connection. 1997. International Telecommunications Infrastructure and Policy, New York : Thomson Publishing Company,
- Haris Faulidi Asnawi, 2004, Transaksi Bisnis E-Commerce: Perspektif Islam, Yogyakarta: Magistra Insania Press,
- I.S. Susanto, "Studi Kritis atas Eksistensi Korporasi Pada Era Nasional dan Global", dalam Khudzaifah Dimyati dan Kelik Wardiono, ed. Problem Globalisasi:Perspektif Sosiologi Hukum Ekonomi dan Agama, Surakarta: Muhammadiyah University Press
- I.S. Susanto. 1995. Krirninologi, Semarang : FI-I UNDIP ,

Indonesia. Ikatan Bankir. 2015. Bisnis Kredit Perbankan. Jakarta: Gramedia Pustaka Utama.

J. E Sahetapy dalam Abdul Wahid, 2002, Kriminologi dan Kejahatan Kontemporer, Malang : Lembaga Penerbitan Fakultas Hukum Unisma

J. Smelser. 1990. The Sociology of Economic Life, diterjemahkan oleh A. Hasymi Ali, Wira Sari

Jack Febrian. 2003. Menggunakan Internet, Bandung: Informatika

Jerry Kang. 1998. Information Privacy in Cyberspace Transaction, Stanford Law.

Johanes Gunawan. 1999. Hukum Perlindungan Konsumen, Bandung : Universitas Katolik Parahyangan

Johannes Ibrahim. 2004, Dilematis Antara Kontrak Dan Kejahatan, Bandung : Refika Aditama

Jonathan. 1996. CyberLaw: The Law of The Internet, New York : Springer-Verlag

Kurniawan. 2006. Penegakan Hukum Tindak Pidana Kartu Kredit. Skripsi. Unair

Lance Castles, 1982, Politic dan Economic Behavior in Java: The Kudus Cigarette Industry, diterjemahkan oleh J. Sirait,. Th. Jakarta: Sinar Harapan

Mahfud M.D, 2000, Poitik Hukum Nasional, Bandung: Alumni .

Mieke Komar Kantaatmadja, 2001, Cyberlaw, Suatu Pengantar, cet.1, Bandung : ELIPS,

- Muhammad Djumhana, 2000, Hukum Perbankan di Indonesia, Bandung:
Citra Aditya Bakti,
- Mulyana W. Kusuma, 1982, Realitas Sosial Kejahatan, Jakarta : Prisma,
LP3ES
- Munir Fuady, 1995, Hukum tentang Pembiayaan dalam Teori dan Praktik,
Bandung: Citra Aditya Bakti,
- Mustafa Bachsan, 2001, Sistem Hukum Administrasi Negara Indonesia,
Bandung,
- Naisbitt, John; Nasibitt, Nana; dan Douglas Philips, 2001, High Tech, High
Touch, Pencarian Makna di Tengah Perkembangan Pesat Teknologi,
Bandung: Mizan
- Nawawi Arief, 1994, Kebijakan Legislatif Dalam Penanggulangan
Kejahatan Dengan Hukum Pidana, Semarang : BP UNDIP.
- Nindyo Pramono, "Revolusi Dunia Bisnis Indonesia Melalui E-Commerce
dan E-Business: Bagaimana Solusi Hukumnya"
- Philipus M. Hadjon, 1987, Perlindungan Bagi Rakyat diIndonesia,
Surabaya : PT.Bina Ilmu
- Ratminto, dkk., 2006, Manajemen Pelayanan & Pengembangan Model
Konseptual, Penerapan Citizen's Carhter dan Standar Pelayanan
Minimal,
- Ronni R Nitibaskara dalam Didik M. Arief Mansur dan Elisatris Gultom.
2005. Cyber Law Aspek Hukum Teknologi Informasi, Bandung : PT
Refika Aditama,

Samuel P. Huntington, The Thad Wave: Democratization in the Late Twentieth Century, Alih bahasa, Asril Marjohan Jakarta: Midas Surya Grafindo

Satjipto Rahardjo. 2009. Penegakan Hukum Suatu Tinjauan Sosiologis. Cetakan 1, Yogyakarta : Genta Publishing

SB. Marsh dan J. Soulsby, 2006, Business Law Hukum Perjanjian, alih bahasa Abdulkadir Muhammad, Bandung: PT Alumni,

Soerjono Soekanto et.al., 1986. Kriminologi, Suatu Pengantar, ctk. Pertama. Jakarta : Ghalian Indonesia

Soerjono Soekanto. 1984. Pengantar Penelitian Hukum, Jakarta : Ui Press

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

Subekti. 1984. Pokok-Pokok Hukum Perdata, Jakarta : Intermasa

Sudikno Mertokusumo. dan A. Pitlo. 1993, Bab-bab tentang Penemuan Hukum, Yogyakarta : Citra Aditya Bakti

Terpetik dalam. 2005. Kitab Undang-undang Hukum Perdata, Jakarta : Pradnya Paramita

VISA International. 2002. Credit Card Fraud Trend & Legislation, Bandung

PERATURAN PERUNDANG-UNDANGAN

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah kedalam Undang-Undang Nomor 19 Tahun 2016 Informasi dan Transaksi Elektronik

Undang-Undang Nomor 7 Tahun 1971 tentang Ketentuan Pokok Kearsipan

Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan
Undang-Undang nomor 36 Tahun 1999 tentang Telekomunikasi
Undang-Undang nomor 23 Tahun 2006 tentang Administrasi
Kependudukan

JURNAL

Anonymous. 2005. Pendekatan Hukum untuk Keamanan Dunia Cyber serta Urgensi Cyberlaw bagi Indonesia, Makalah mahasiswa teknologi informasi, Teknik Komputer, Universitas Indonesia.

Atip Latifulhayat, "Perlindungan Data Pribadi dalam Perdagangan Secara Elektronik (E-Commerce), Artikel dalam Jurnal Hukum Bisnis, 2002

Bambang Sutiyoso, "Penyelesian Sengketa Bisnis Melalui online Dispute Resolution dan Pemberlakuan di Indonesia", Mimbar Hukum, 2008 Journal of Criminal Law and Criminology, Volume 76, Issue 3, Article 7

Cf. Ahmad M. Ramli. 2003. Kekuatan Akta Elektronik Sebagai Alat Bukti Pada Transaksi E-Commerce Dalam Sistem Hukum Indonesia, Makalah.

Fakih Fahmi Mubarok, 2006, Tinjauan Hukum Penyelesaian Sengketa Perkara Melalui Arbitrase Online Berdasarkan Undang-undang No. 30 Tahun 1999, makalah, Yogyakarta: Fakultas Hukum UIL,

Karlina P. A. Soebroto. 1991. Kejahatan Komputer dalam Perbankan, Temu Karya Ilmiah Tindak Pidana Perbankan, Majalah Hukum Varia Peradilan

Rizkia Nurdinisari. 2013. Skripsi berjudul "Perlindungan Hukum Terhadap Privasi Dan Data Pribadi Pengguna Telekomunikasi Dalam

Penyelenggaraan Telekomunikasi Khususnya Dalam Menerima Informasi Promosi Yang Merugikan”, Jakarta

Rahadi Wasi Bintoro, “Tuntutan Hak Dalam Persidangan Perkara Perdata”, Jurnal Dinamika Hukum, Vol. 10 No. 2, 2010

Sigid Suseno dan Syarif A. Barmawi. Kebijakan Pegaturan Carding dalam Hukum Pidana di Indonesia. Jurnal Sosiohumaniora, Vol. 6, No. 3.

Tetanoe Bernada, “Upaya Perlindungan Hukum Pada Konsumen Dalam Transaksi E-commerce Untuk Mendukung Pertumbuhan Ekonomi Digital Di Indonesia”, Jurnal Hukum Dan Peradilan, Uph, Banten Vol. 6 No.1,2017

MEDIA ELEKTRONIK

Daniar Supriyadi. 2017. “Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya”.<https://www.hukumonline.com/berita/baca/lt59cb4b3feba88/data-pribadi-dan-dua-dasar-legalitas-pemanfaatannya-oleh--daniar-supriyadi/>. Diakses pada 16 Maret 2020. Pukul 18.04 WIB.

Harnad, Steven, Post-Gutenberg Galaxy: The Fourth Revolution in the Means of Production of Knowledge, Public-Access Computer System Review 2 (1): 39-53, versi elektronik dapat dibaca pada <http://cogprints.org/1580/00/> harnad91. postgutenberg.html

<http://www.bniscardcenter.co.id/Aplikasi-Merchant/Joint-erchant/Ketentuan-Umum.aspx> diakses pada tanggal 17 Desember 2022

<https://economy.okezone.com/read/2018/01/19/320/1847340/pengaduan-ylki-2017-paling-banyak-belanja-online?page=1> Diakses tanggal 24 Desember 2022 pukul 11.22 WIB

KBBI. "Pengertian Data". <https://kbbi.web.id/data> diakses pada 03 Desember 2019 Pukul 16.00

KBBI. "Pengertian kata Pribadi". <https://kbbi.web.id/pribadi> pada 03 Desember 2019 Pukul 21.30 WIB

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.

Prof. Dr. Ahmad M. Ramli, S.H., M.H., FCBArb, "Dinamika Konvergensi Hukum Telematika dalam Sistem Hukum Nasional", <http://ditjenpp.kemenkumham.go.id/hukum-teknologi/668-dinamika-konvergensi-hukum-telematika-dalam-sistem-hukum-nasional.html>, diakses pada Rabu 23/12/2022 pukul 15.00 WIB.

www.research.digital.com/SRC/personal/stev
[eg/millicent/millicent.html](http://www.research.digital.com/SRC/personal/stev/millicent/millicent.html) diakses pada tanggal 23 Desember 2022 Pukul 19.00 WIB