**UNIVERSITAS INDONESIA**

# PERAN PENEGAKAN HUKUM OLEH PUBLIK DALAM TINDAK PIDANA MAYANTARA

## (Studi Sosiologi Hukum Mayantara)

**TESIS**

**SYAFRUDDIN RIFA'IE**
**0906620833**

**FAKULTAS HUKUM**
**PROGRAM PASCASARJANA**
**JAKARTA**
**2011**

**UNIVERSITAS INDONESIA**

# PERAN PENEGAKAN HUKUM OLEH PUBLIK DALAM TINDAK PIDANA MAYANTARA (Studi Sosiologi Hukum Mayantara)

**TESIS**

**Diajukan sebagai salah satu syarat untuk memperoleh gelar Magister Hukum**

**SYAFRUDDIN RIFA'IE**

**0906620833**

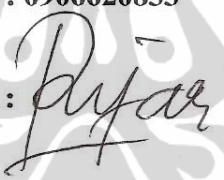
**FAKULTAS HUKUM**
**PROGRAM STUDI ILMU HUKUM**
**KEKHUSUSAN HUKUM DAN SISTEM PERADILAN PIDANA**
**JAKARTA**
**2011**

## HALAMAN PERNYATAAN ORISINALITAS

**Tesis ini adalah hasil karya saya sendiri,**
**dan semua sumber baik yang dikutip maupun dirujuk**
**telah saya nyatakan dengan benar.**

**Nama** : **Syafruddin Rifa'ie**

**NPM** : **0906620833**

**Tanda Tangan** : 

**Tanggal** : **11 Juli 2011**

# HALAMAN PENGESAHAN

Tesis ini diajukan oleh :

| | |
|---|---|
| Nama | : Syafruddin Rifa'ie |
| NPM | : 0906620833 |
| Program Studi | : Ilmu Hukum |
| Judul Tesis | : Peran Penegakan Hukum oleh Publik dalam Tindak Pidana Mayantara (Studi Sosiologi Hukum Pidana Mayantara) |

**Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister Hukum (M.H.) pada Program Pascasarjana Fakultas Hukum, Universitas Indonesia.**

## DEWAN PENGUJI

Pembimbing : Dr. Jufrina Rizal, SH.,MA ( )

Ketua Sidang/ Penguji : Prof. H. Mardjono Reksodiputro, SH., MA

Penguji : Dr. Surastini Fitriasih, SH.,MH ( )

Ditetapkan di : Jakarta

Tanggal : 11 Juli 2011

## KATA PENGANTAR/UCAPAN TERIMA KASIH

Dengan penuh syukur kepada ALLAH SWT, berkat Rahmat dan Hidayah-Nya tesis ini terselesaikan tepat waktu meski masih dengan berbagai keterbatasan di dalamnya. Tesis ini disusun untuk memenuhi tugas akhir perkuliahan Program Pascasarjana Fakultas Hukum Universitas Indonesia, dan untuk memenuhi syarat meraih gelar Magister Hukum. Tak dipungkiri selama penyusunan tesis secara khusus, maupun selama perkuliahan, penulis mendapatkan begitu banyak bantuan yang sangat berarti dalam menyelesaikannya dengan baik. Oleh karenanya dalam kesempatan ini penulis ingin mengucapkan banyak terima kasih kepada:

(1) Kedua guru hukumku yang pertama, Bapak Sohirin, SH. dan Ibu Maryati, S.,Pd., kedua orang tuaku yang dengan penuh bakat alaminya menanamkan dasar-dasar konsep hukum dalam hidupku, dan dengan penuh cinta membimbing dan mendidik penulis, tanpa cacat dan penuh kebaikan, barakAllah;

(2) Ibu Dr. Jufrina Rizal, SH.,MA., dengan penuh hormat, yang telah membimbing penyusunan tesis ini dengan penuh kesabaran dan ketelatenan hingga tesis ini selesai dengan baik, meskipun beliau tengah menjalankan tugas di Paris, Perancis. Ketegasan beliau dalam mengarahkan penulisan tesis ini juga memberikan banyak pelajaran kepada penulis terutama dalam melakukan riset sosiologis dalam bidang hukum;

(3) Prof. H. Mardjono Reksodiputro, SH.,MA., selaku Ketua Peminatan Sistem Peradilan Pidana pada Program Pascasarjana Fakultas Hukum Universitas Indonesia, sekaligus ketua sidang/penguji tesis ini. Dengan keterbukaan dan luasnya wawasan beliau, penulis belajar banyak selama perkuliahan;

(4) Ibu Dr. Surastini Fitriasih, SH.,MH., selaku penguji dan pengajar, yang juga membantu penulis dalam penyelesaian tesis ini;

(5) Yang terhormat para pengajar pada Program Pascasarjana Fakultas Hukum Universitas Indonesia;

(6) (Alm.) Theodorus Sardjito S.H., M.A., dan (Alm.) Dr. Rudy Satriyo Mukantardjo S.H., M.H., dua pengajar di Program Pascasarjana FH-UI yang

telah berpulang terlebih dahulu. Semoga seluruh kebaikan ilmu yang mereka ajarkan dengan kritis dapat memberikan banyak manfaat;

(7) Para narasumber dalam penelitian ini, Bapak Onno W. Purbo, Day Milovich, Blie Dessy, Psychozetic, Mas Kurniawan YF, Xadpritox, dan dukungan teman-teman di berbagai komunitas *hacker* dan *hacker underground* di Indonesia, terutama Indonesiancoder Team, Magelangcyber Team, Yogyafree Family Code, Komunitas Hacker Cisadane, Jasakom-Perjuangan. Selain itu penulis juga ingin mengucapkan terima kasih pada teman-teman yang secara tidak langsung membantu pengumpulan data, *thanks to*: Kamtiez, Jundab, S'to, dr.Cruzz, Kampreto, dan teman-teman di ruang-ruang publik *underground* mayantara;

(8) Kakak tercinta Sofiati Hasna dan M. Mansur Chisni, serta keponakan-keponakan, Rama dan Mada, yang membantu penulis selama perkuliahan dan penyelesaian tesis ini. Dan Keluarga di Semarang, mbak Santi Herrini dan mas Faozan, serta putra mereka Daffa, barakAllah;

(9) Teman-teman kelas Sistem Peradilan Pidana (SPP) angkatan 2009 tanpa terkecuali yang selama perkuliahan dan di luar perkuliahan saling mendukung, terutama Pak Ismet Karnawan, Mas Ainul Syamsu, Mas Sidharta, Pak Simplexius Asa, Mas Agung, Mas Rizvan Imanuddin, Mas Endang Tirtana, Mbak Juwita Kayana, Mas Anton Sutrisno, Mas Eddy Sumarman;

(10) Teman-teman di Desantara, Depok, Mas Ing Wuri Handayani, dan Rustam.

(11) Ms. Elif Bilici, dan teman-teman di International University of Sarajevo, Bosnia, dan Istanbul, Turki, yang turut mendukung penulis selama ini. Gerakan *hacker* dan *cybercrime* di Turki merupakan tantangan selanjutnya.

Akhir kata, penulis berharap ALLAH SWT berkenan membalas segala kebaikan semua pihak yang telah membantu. Dan terutama, semoga tesis ini bermanfaat untuk siapa saja. Amin.

Bogor, 11 Juli 2011

Penulis

## HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah
ini:

| | | |
|---|---|---|
| Nama | : | Syafruddin Rifa'ie |
| NPM | : | 0906620833 |
| Program Studi | : | Ilmu Hukum |
| Fakultas | : | Hukum |
| Jenis karya | : | Tesis |

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul:

**PERAN PENEGAKAN HUKUM OLEH PUBLIK DALAM TINDAK PIDANA MAYANTARA (STUDI SOSIOLOGI HUKUM PIDANA MAYANTARA)**

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada tanggal : 11 Juli 2011
Yang menyatakan,

( Syafruddin Rifa'ie )

# ABSTRAK

Nama : Syafruddin Rifa'ie
Program Studi : Ilmu Hukum
Judul : Peran Penegakan Hukum oleh Publik dalam Tindak Pidana Mayantara (Studi Sosiologi Hukum Pidana Mayantara)

Untuk menciptakan legitimasi hukum pidana dalam mayantara perlu melalui beberapa tahap. Perlu dibuka ruang-ruang komunikasi sehingga antara pihak aktifis mayantara dengan pemerintah sebagai pihak penentu kebijakan, komunikasi ini harus dibuat sedemikian rupa sehingga masing-masing pihak dapat menyampaikan klaim-klaim kesahihan tentang pandangan masing-masing. Kemudian akan menuntun kepada konsensus yang membimbing kepada pembentukan kebijakan-kebijakan penegakan hukum pidana yang sesuai dengan pemahaman dan pengamatan teknis para profesional komunitas *cyber* (*hacker*). Dan terbukanya kemungkinan konsensus tidaklah mungkin tanpa adanya pemahaman yang baik oleh satu pihak terhadap pihak lainnya dan sebaliknya. Karena pengaruh media yang tidak selalu benar dalam memberitakan tentang komunitas *hacker*, maka perlu adanya kajian terhadap komunitas *hacker* dengan lebih baik, agar proses komunikasi yang berkelanjutan dengan tujuan pemulihan ketertiban bersama dapat terwujud dengan baik. Dengan tujuan utama terciptanya peran serta yang positif oleh para *hacker* dan komunitasnya yang mewakili publik mayantara dalam turut serta membantu perangkat penegak hukum dalam penegakan hukum dengan kemampuan dan keutamaannya, secara khusus dalam penanganan *cybercrime*.

Kata kunci:
Hukum Pidana, Tindak Pidana Mayantara, *Hacker*, Publik.

## ABSTRACT

Name : Syafruddin Rifa'ie
Study Program : Law
Title : The Law Enforcement Role by the Public in Cybercrime (Study on Sociology of Cybercrime)

To create the legitimacy of criminal law in cyberspace, its need to go through several stages. Need to creat open communication spaces between cyberspace activists with the government as the policy maker, this communication must be made in such a way that each sides may submit claims to the validity of their respective views. Then it will lead to the consensus that led to the formation of policies that criminal law enforcement in accordance with the understanding and technical professionals observation cyber community (hackers). And opening the possibility of consensus is not possible without a good understanding by one side against the other side and vice versa. Because of the influence of media, it is not always true in preaching about the hacker community, it is necessary to study the hacker community with better understanding, so that an ongoing communication process with the goal of restoration of order can be realized together very well. With the main objective for created positive participation by the hackers and the community who represent the public of cyberspace participation in helping law enforcer in law enforcement with their abilities and virtues, specifically in handling cybercrimes.



Key words:
Criminal law, Cybercrime, Hacker, Public.

## DAFTAR ISI


Halaman

HALAMAN JUDUL ..... i
HALAMAN PERNYATAAN ORISINALITAS ..... ii
HALAMAN PENGESAHAN ..... iii
KATA PENGANTAR ..... iv
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS ..... vi
ABSTRAK ..... vii
ABSTRACT ..... viii
DAFTAR ISI ..... ix
DAFTAR GAMBAR ..... xii
DAFTAR TABEL ..... xiii
DAFTAR GRAFIK ..... xiv

**1. PENDAHULUAN** ..... 1
1.1 Latar Belakang ..... 1
1.2 Perumusan Masalah ..... 4
1.3 Pertanyaan Penelitian ..... 5
1.4 Tujuan Penelitian ..... 6
1.5 Kerangka Teori ..... 7
1.6 Kerangka Konsepsional ..... 13
1.7 Metode Penelitian ..... 15
1.8 Sistematika Penulisan ..... 16

**2. TINJAUAN PUSTAKA** ..... 18
2.1 Sistem Peradilan Pidana ..... 18
2.1.1 Model Sistem Peradilan Pidana ..... 21
2.1.1.1 *Crime Control Model* ..... 21
2.1.1.2 *Due Process Model* ..... 22
2.1.2 Model SPP Indonesia ..... 23
2.1.3 Penelitian sebagai Upaya Perbaikan Sistem Hukum ..... 27
2.2 Pendekatan Hukum Responsif ..... 28
2.3 Pengantar Kepada Sosiologi Hukum ..... 32
2.3.1 Hukum sebagai *Social Control* ..... 35
2.3.1.1 Kontrol Sosial Informal ..... 36
2.3.1.2 Kontrol Sosial Formal ..... 37
2.3.2 Hukum sebagai *Conflict Resolution* ..... 38
2.3.2 Hukum sebagai Sarana *Social Engineering* ..... 40
2.4 Publik Mayantara ..... 41
2.4.1 Pengertian Publik ..... 41
2.4.2 Konsep Publik Mayantara ..... 43
2.4.3 Penelitian terhadap Publik Mayantara untuk Perbaikan Sistem Hukum ..... 48
2.5 Pengantar Kepada Pemikiran Jurgen Habermas ..... 51
2.5.1 Latar Belakang Historis Sekolah Frankfurt ..... 53

2.5.2 Latar Belakang Teoritis Sekolah Frankfurt ..... 55
2.5.2.1 Kritisisme Kant ..... 56
2.5.2.2 Kritisisme Hegel ..... 58
2.5.2.3 Kritisisme Marx ..... 60
2.5.2.4 Kritisisme Freud ..... 62
2.5.3 Diskursus dan Demokrasi Deliberatif Habermas ..... 65
2.5.3.1 Berangkat dari Marx ..... 65
2.5.3.2 Pengetahuan dan Kepentingan ..... 67
2.5.3.3 Etika Diskursus ..... 69
2.5.3.4 Demokrasi Deliberatif ..... 70
2.5.4 Konsep Opini Publik Jurgen Habermas ..... 71
2.5.4.1 Klarifikasi Sosiologis Opini Publik ala Habermas ..... 76
2.5.4.2 Peran Opini Publik dalam Negara Demokratis ..... 79
2.5.4.3 Peran Opini Publik dalam Pembentukan Hukum ..... 81
2.5.4.4 Fungsi Kritis Opini Publik Terhadap Sistem Sosial ..... 83
2.5.4.5 Peran Publik dalam Penegakan Hukum Pidana Mayantara 85

**3. DINAMIKA SOSIAL MAYANTARA DAN *CYBERCRIME*** ..... 90
3.1 Struktur Sosial Mayantara ..... 90
3.1.1 Sekilas tentang Sejarah Internet ..... 91
3.1.2 Ilmu Pengetahuan di Dalam *Cyberspace* ..... 96
3.1.3 Memahami Struktur Sosial Masyarakat Mayantara ..... 100
3.1.3.1 Internet: Komunitas Dunia *Cyber* ..... 105
3.1.3.2 *Hacker*: Sub-Kultur Dunia *Cyber* ..... 106
3.2 *Cybercrime* ..... 129
3.2.1 Persepsi tentang *Cybercrime* ..... 135
3.2.2 Mendefinisikan *Cybercrime* ..... 139
3.2.3 Akibat dari *Cybercrime* ..... 142
3.2.3.1 Pengaruh Ekonomi ..... 144
3.2.3.2 Pengaruh Psiko-Sosial ..... 149
3.2.4 Statistik Global Kejahatan *Cyber* ..... 169
3.2.4.1 *Cyber-Tresspass* ..... 169
3.2.4.2 *Cyber-deception/theft* ..... 175
3.2.4.3 *Cyber-pornography/obscenity* ..... 179
3.2.4.4 *Cyber-violence* ..... 183

**4. PENEGAKAN HUKUM TERHADAP *CYBERCRIME*** ..... 186
4.1 Peran Publik Mayantara dalam Penegakan Hukum ..... 186
4.1.1 Pelaksanaan Penegakan Hukum dan Tantangannya ..... 188
4.1.2 Partisipasi Publik (Masyarakat) ..... 196
4.1.3 Optimisme Penegakan Supermasi Hukum dalam Mayantara ..... 203
4.2 Kendala Penegakan Hukum Pidana Mayantara Indonesia ..... 206
4.2.1 Perkembangan Kriminalitas di Mayantara ..... 209
4.2.2 Kurangnya Kemampuan Penegak Hukum ..... 214
4.2.3 Perlunya Undang-undang Khusus *Cybercrime* ..... 217
4.3 Peran Hacker dalam Penegakan Hukum Pidana Mayantara Perspektif Teori Diskursus Habermas ..... 221
4.3.1 Teorema Diskursus Habermas ..... 223

4.3.2 Hukum dan Proseduralisme ..... 228
4.3.3 Demokrasi Deliberatif dan Legitimasi Hukum ..... 232
4.4 Bentuk Kerjasama Penegakan Hukum Pidana antara Agen Sosial Mayantara dan Lembaga Penegak Hukum ..... 234
4.4.1 Tanggung Jawab Sosial ..... 235
4.4.2 Peran Teknis ..... 237
4.4.3 Peran Politis ..... 240

**5. PENUTUP** ..... 249
5.1 Simpulan ..... 249
5.2 Saran-saran ..... 256

DAFTAR PUSTAKA ..... 258

## DAFTAR GAMBAR


| Gambar: | | Halaman |
|---|---|---|
| Gambar 2.1. | Lapisan-lapisan dalam sistem peradilan pidana. | 18 |
| Gambar 2.2. | Bagan alir sistem peradilan pidana. | 19 |
| Gambar 3.1. | Filosofi arsitektur sosial, budaya, dan hukum di dunia maya. | 97 |
| Gambar 3.2. | Siklus pemurnian pengetahuan. | 99 |
| Gambar 3.3. | Monitor refleksif atas tindakan (Giddens, 1984). | 114 |
| Gambar 3.4. | *Taxonomy of cybercriminal behaviors*. | 150 |
| Gambar 3.5. | *Model circumplex.* | 157 |
| Gambar 4.1. | Dalam komunikasi diambil tiga macam sikap performatif terhadap dunia. Konsensus dapat tercapai hanya jika ketiga klaim kesahihan itu serentak dipenuhi. | |
| Gambar 4.2. | Perkembangan *Lebenswelt* terhadap sistem. | 227 |
| Gambar 4.3. | Dalam negara hukum demokratis hukum menjadi poros proses pertukaran antara sistem dan *Lebenswelt*. | 231 |
| Gambar 4.4. | Perbandingan kuantitas dan kemampuan teknis yang melingkupi kemampuan pengawasan. | 235 |
| Gambar 4.5. | Opini publik yang berasal dari ruang publik masuk ke dalam sistem politik melalui saringan atau prosedur yang dapat dibayangkan sebagai bendungan. | 242 |

## DAFTAR TABEL


| Tabel: | | Halaman |
|---|---|---|
| Tabel 2.1. | Packer's *due process and crime control models: a comparison*. | 24 |
| Tabel 3.1 | Komunitas *underground* di Indonesia (2006). | 123 |
| Tabel 3.2 | Komunitas *underground-hacker* di Indonesia (2011). | 124 |
| Tabel 3.3. | *Economic impact of malicious code attacks, by incident.* | 145 |
| Tabel 3.4. | *Economic impact of malicious code attacks, by year*. | 145 |
| Tabel 3.5. | *Defacement attack by month*, 2010 (zone-h). | 170 |
| Tabel 3.6. | *Defacement special attack by month*, 2010 (zone-h). | 171 |
| Tabel 3.7. | *Defacement single attack by month*, 2010 (zone-h). | 172 |
| Tabel 3.8 | *Defacement mass attack by month*, 2010 (zone-h). | 172 |
| Tabel 3.9. | *Attack Methods*, 2010 (zone-h). | 174 |
| Tabel 3.10. | *Attack Reasons*, 2010 (zone-h). | 174 |
| Tabel 3.11. | *Uptime for the last three years* (2008-2010). | 179 |
| Tabel 3.12. | *Pornography time statistics*. | 180 |
| Tabel 3.13. | *Pornography statistic* (2005-2006). | 181 |
| Tabel 3.14. | *Children internet pornography statistic* (2005-2006). | 183 |
| Tabel 4.1 | *Notifier Statistic* Zone-h.org Juni 2011. | 190 |
| Tabel 4.2 | Klasifikasi *cyberattack* berdasarkan sumber geografis. | 191 |
| Tabel 4.3 | *Coplaints – referrals: cybercrimes* (2008-10) di Amerika Serikat. | 191 |
| Tabel 4.3. | *Defacement* pada nama domain '.id'. (Zone-H.org). | 215 |
| Tabel 4.4. | Tahap-tahap perkembangan hukum. | 230 |

## DAFTAR GRAFIK

Grafik: Halaman

Grafik 3.1. *Historic trend phishing site uptime* (2008-2010). 178

# BAB I
# PENDAHULUAN

## 1.1 LATAR BELAKANG

Revolusi teknologi informasi, sebagai tahap lanjut dari revolusi industri, telah memberikan tatanan baru kepada dunia dan menciptakan paradigma-paradigma baru dalam lingkup sosial, budaya, ekonomi dan politik. Para penggunakan komputer kini dapat berkomunikasi satu sama lain dari belahan bumi dengan cara yang jauh lebih ringkas. Pengembangan dan penggunaan teknologi dalam membantu aktifitas manusia dalam hiburan, pendidikan, perdagangan, pemerintahan dan komunikasi dapat dipahami secara umum sebagai suatu kewajaran demi efektifitas dan efisiensi.

Menjalankan beberapa aktifitas secara majemuk dalam satu waktu merupakan upaya meringkas aktifitas, dan komputer menjadi alat bantu yang efektif. Selanjutnya perkembangan teknologi internet telah menggeser komputer dari alat sekunder menjadi alat primer dalam beraktifitas.

Berbagai 'alat' kemudian lahir dalam tradisi masyarakat informasi, yang dalam dunia komputer biasa disebut dengan *program*, atau *application*. Alat-alat tersebut telah menggantikan cara lama dalam bekerja, mendapatkan hiburan, bahkan pengetahuan. Manusia dan teknologi informasi berkembang dan terus memperbaiki alat yang digunakan, sebagaimana kita dapatkan gambarannya dari berbagai artefak sejarah perkembangan peradaban manusia. Referensi kehidupan pada teknologi telah melibatkan perangkat yang mengurangi sifat sosial dalam berbagai sisi kehidupan, dan keterlibatan ini telah dapat diterima secara luas.

Pada saat yang hampir bersamaan dengan kemunculan internet, mereka yang peduli kepada tatanan hidup yang tertib dan teratur, serta konstruksi kehidupan dengan keamanan dan kenyamanan dalam menjelajah dunia maya pun semakin menonjol. Sebagian melihat bahwa internet adalah wilayah yang sama sekali berbeda dari dunia kenyataan, banyaknya kemungkinan di dalamnya dan

berbagai kebutuhan yang dikelola menjadikannya cukup mudah dan rentan untuk dimanfaatkan sebagai media kejahatan.

Kemudian, tanggungjawab sosial dalam menjaga tiap-tiap organnya dari perkembangan modus kejahatan pun semakin berat, terlebih jika peran negara sebagai wadah dan ikatan sosial yang lebih besar belum siap menjangkau wilayah-wilayah yang terus berkembang pesat secepat laju waktu. Sedangkan kini Indonesia berkembang sebagai negara dengan jumlah kejahatan internet yang tinggi.[1]

Dikatakan Thomas X. Grasso, *"The average take on a bank robbery is $3,000. The persons committing that crime run an extremely high risk of something bad happening to them. You can run a phishing scam and make hundreds of thousands of dollars."*[2] Pelaku kejahatan selalu berusaha mencari cara yang lebih meminimalisir resiko dalam melakukan tindakan kejahatannya, terutama akibat fisik yang mungkin terjadi saat melakukan kejahatan, dan *phising scam* adalah salah satunya. Peningkatan aktifitas sosial di internet dan kelemahan yang masih banyak di dalam konstruksi kontrol sosial terhadap tiap individu di dalamnya, pastilah memberikan daya tarik watak jahat para pelaku kejahatan yang berpotensi melakukannya.

Pada kenyataannya pertempuran antar para pakar internet dalam dunia maya dan penyelesaian atau penangkalan kejahatan yang seringkali terjadi adalah karena adanya solidaritas yang kuat antar sesama *hacker* atas serangan kelompok

---

[1] Pendapat bahwa Indonesia memiliki tingkat *cybercrime* tertinggi di dunia pada 2009, salah satunya disampaikan oleh Brigjen Anton Taba, Staf ahli Kapolri, lihat: http://nasional.kompas.com/read/2009/03/25/18505497/Cyber.Crime..Indonesia.Tertinggi.di.Dunia, namun pernyataan ini rupanya memerlukan revisi dengan pengamatan empiris, mengingat permasalah dalam menentukan pelaku kejahatan mayantara bukanlah hal sederhana. Di dalam http://www.oversecurity.net/2010/12/01/web-hacking-statistiche-2010-1%C2%B0-puntata-da-dove-originano-gli-attacchi-globali/, merupakan laporan statistik serangan atas situs internet (*web hacking*), menunjukkan Indonesia ada di urutan ketujuh dunia dengan persentase serangan 1,27%. Dari keseluruhan persentase yang ada di dalam laporan ini urutan pertama adalah 77% dengan penjelasan *Origine non determinata*, atau wilayah tidak terdeteksi. Secara singkat pernyataan oleh Brigjen Anton Taba tidak dapat dipertanggungjawabkan secara pasti, karena selain tidak mudah mendeteksi asal pelaku kejahatan seluruhnya, kejahatan mayantara juga terus berkembang.

[2] McAfee North America Criminology Report; Organized Crime and the Internet 2007, McAfee. Hal. 3.

*hacker* lain. Dengan demikian kita dapat mendapat kesan bahwa pencegahan dan penyelesaian kasus pidana khusunya, yang terjadi hampir tidak pernah sampai pada tangan para penegak hukum.

Penegakan hukum global tengah memperkuat hukum-hukum nasional dan internasional bekerjasama untuk menangkap, menuntut, dan mencegah kejahatan mayantara.[3] Meski dengan fakta yang sedemikian rupa, tindak pidana mayantara terus berlanjut dan berkembang. Internet meningkat nilainya sebagai kebutuhan dari hari ke hari, tetapi keamanan yang dibangun di dalamnya seringkali tidak mampu mengimbangi. Bahkan memungkinkan pelaku kejahatan muncul tanpa identitas dan berada dalam wilayah yang tak perlu lagi adanya kekhawatiran untuk mengoperasikan kejahatannya.

Banyak korban enggan melaporkan kejahatan mayantara yang dialaminya. Terutama bagi perusahaan atau bank, pertimbangan terancamnya reputasi keamanan yang mereka bentuk lebih mengemuka dibandingkan upaya untuk menangkal serta menangkap pelaku kejahatan. Penanganan pribadi terhadap sistem keamanan mereka dengan pandangan yang demikian bisa menjadi penyulut meningkatnya *criminal case mortality*.[4]

---

[3] Sebagaimana ada dalam Penjelasan Umum Undang-undang Nomor 11 Tahun 2008, tentang Informasi dan Transaksi Elektronik (ITE), "Hukum siber atau *cyberlaw*, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan telekomunikasi… Istilah lain yang juga digunakan adalah hukum teknologi informasi (*law of information technology*), hukum dunia maya (*virtual world law*), dan hukum mayantara." Dan pembahasan tentang virualitas tersebut meliputi komunikasi lokal maupun global (Internet). Istilah mayantara juga banyak ditemukan dalam buku karya Prof. Dr. Barda Nawawi Arif, SH., *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*, (Jakarta: PT. Raja Grafindo Perkasa, 2007). Kata 'mayantara' dipakai menggantikan kata 'cyber', sebagaimana dalam halaman v buku tersebut, "Perkembangan *cyber crime* (tindak pidana mayantara) sering dibahas dalam forum internasional."

[4] Prof. Mardjono Reksodiputro menjelaskan:

"Dalam kenyataan maka dari sejumlah kejahatan yang mencatat pada kepolisian hanya sebagian saja yang selesai dengan ditangkapnya "tertuduh pelaku" dan diserahkan perkaranya kepada kejaksaan. Dari jumlah perkara ini maka tidak semuanya dapat diajukan oleh jaksa ke pengadilan. Dan dalam pemeriksaan pengadilan, maka hanya sebagian perkara saja yang dinyatakan terbukti. Dari mereka yang dinyatakan terbukti bersalah, maka hanya sebagian saja yang masuk dalam lembaga-lembaga pemasyarakatan. Keadaan ini dikenal dengan istilah 'penyusutan perkara kriminal' (*criminal case mortality*)." Mardjono Reksodiputro, *Kriminologi dan Sistem Peradilan Pidana*, (Jakarta: Pusat Pelayanan Keadilan dan Pengabdian Hukum Universitas Indonesia, cet. Kedua, 2007), hal. 17.

Tetapi apakah hanya akan berhenti di sana saja. Sinergi dengan para penegak hukum dan masyarakat, dengan memanfaatkan tenaga para pakar internet kian menjadi suatu keniscayaan. Perkembangan teknologi menciptakan kejahatan-kejahatan baru dan permasalahan-permasalahan baru dalam penegakan hukum. Demi tegaknya hukum yang responsif terhadap perkembangan zaman dan responsif terhadap kemuslihatan tindak kejahatan yang kian meningkat maka perlu dibangun pondasi yang kuat dalam memulainya. Saat alat-alat penegakan hukum yang ada terbatas dalam melaksanakan kewajibannya, pemikiran Prof. Dr. Satjipto Rahardjo, SH. tentang hukum progresif merupakan salah satu jalan.

Beliau mengungkapkan, pertama, disadari kemampuan hukum itu terbatas. Mempercayakan segala sesuatu kepada hukum adalah sikap tidak realistis dan keliru. Kedua, masyarakat ternyata menyimpan kekuatan otonom untuk melindungi dan menata diri sendiri.[5] Kedua pernyataan ini merupakan saripati dari gagasan 'hukum progresif' yang beliau kembangkan. Bagi Prof. Satjipto, hukum bukanlah suatu skema yang final (*finite scheme*), namun terus bergerak, berubah, mengikuti dinamika kehidupan manusia. Karena itu, hukum harus terus dibedah dan digali melalui upaya-upaya progresif untuk menggapai terang cahaya kebenaran dalam menggapai keadilan.[6]

## 1.2 PERUMUSAN MASALAH

Hukum pidana sebagai lingkaran terluar dari hukum,[7] harus memberikan peran lebih terhadap hukum sebagai kontrol sosial. Dalam hal ini penetapan sistem hukum mayantara yang memiliki kemampuan dalam menanggulangi kejahatan internet adalah merupakan bagian dari kebijakan kriminal atau politik kriminal.

---

[5] Satjipto Rahardjo, *Penegakan Hukum Progresif*, cet. Ketiga, (Jakarta: Kompas, 2010), hal. 209.

[6] Ibid, hal. vii.

[7] Pendapat G.E. Mulder, dalam Jan Remmelink, *Hukum Pidana* (*Inleiding tot de Studie van het Nederlanse Strafrecht*), diterjemahkan oleh Tristam Pascal Moeliono, (Jakarta: Gramedia, 2003), hal. 7.

Pada kenyataannya penanganan berbagai tindak pidana mayantara menunjukkan bahwa para penegak hukum tidak dapat lagi berjalan sendiri, penegakan hukum memerlukan partisipasi publik bersama para penegak hukum untuk menciptakan kesejahteraan sosial. Di saat minimnya kemampuan aparat penegak hukum dan keterbatasannya dalam menangani berbagai tindak pidana mayantara seperti sekarang ini menyebabkan keadilan akan sulit ditemukan dan hukum kehilangan banyak waktu untuk berbenah. Namun, di sisi lain, peran masyarakat umum untuk bahu-membahu mengatasi berbagai permasalahan hukum terlihat berjalan secara otonom dan berkelanjutan.

Sulitnya mengontrol dunia maya secara keseluruhan dan kurangnya kemampuan dalam melakukan tindakan terhadap berbagai tindak pidana mayantara memerlukan cara yang lebih responsif dan memerlukan keterlibatan publik dengan lebih terarah. Perancangan yang matang dan kemampuan melihat kemungkinan di masa yang akan datang menempatkan hukum pidana sebagai kontrol yang baik dalam mengantisipasi kejahatan yang akan berkembang, terutama di dunia maya. Pemberian peran-peran kontrol hukum kepada para pemakai internet secara umum dan mereka yang memiliki kemampuan lebih dalam bidang teknologi *cyber*, secara umum akan meningkatkan kewaspadaan sosial dalam mayantara terhadap kejahatan pidana yang potensial terjadi.

Kemudian, seberapa strategiskah peran publik membantu perangkat hukum dalam upaya penegakan hukum dalam dunia maya, mengingat bahwa, tujuan politik kriminal yang sangat luas dan ideal yaitu penanggulangan kejahatan dengan segala aspeknya untuk tujuan perlindungan dan peningkatan kesejahteraan masyarakat.[8]

## 1.3 PERTANYAAN PENELITIAN

Berdasarkan pokok permasalahan tersebut maka dapat diuraikan pertanyaan-pertanyaan penelitian (*research questions*) sebagai berikut:

---

[8] Barda Nawawi Arif, *Kebijakan Legislatif dalam Penanggulangan Kejahatan dengan Pidana Penjara*, (Yogyakarta: Genta Publishing, 2010), hal. 4.

1. Bagaimana struktur sosial masyarakat mayantara dan dinamika masyarakatnya?
2. Bagaimana pengaturan dari *cybercrime* dalam perundang-undangan di Indonesia?
3. Bagaimana penegakan hukum terhadap *cybercrime* dan peran-peran sosial apa sajakah yang dapat dilakukan publik mayantara dalam menciptakan sistem peradilan pidana yang responsif dalam mayantara?
4. Kendala-kendala apa saja dalam penegakan hukum terhadap *cybercrime*?

## 1.4 TUJUAN PENELITIAN

Penelitian ini berusaha mengungkapkan beberapa permasalahan penegakan hukum pidana mayantara di Indonesia. Menguraikan permasalahan yang berkesesuaian dengan kenyataan yang dihadapi oleh publik mayantara. Selama ini penelitian mengenai permasalahan penegakan hukum pidana mayantara serta kendala umum di dalamnya seringkali menggunakan pendekatan hukum positif yang terkungkung dalam definisi-definisi yang seringkali hanya mengutip dan menterjemahkan pengertian dari sumber asing, akan tetapi pemahaman tentang karakteristik sosial sangat kurang mendapatkan perhatian. Keterbatasan dalam mengamati dinamika masyarakat dan dialektikanya terhadap hukum serta penerapannya tidak dapat dilakukan hanya dengan mengamati definisi dan mencocok-cocokkan dengan pengandaian mengenai lingkungan sosialnya. Pergerakan masyarakat yang demikian dinamis dan terus bergerak cepat memerlukan pemahaman pengamatan dari dalam atau setidaknya perlu pembauran dengan lingkungan sosial, hal ini bertujuan untuk mendapatkan kesahihan pemahaman masyarakat dan kendala yang dihadapi dengan lebih baik dan bukan hanya pengandaian.

Penelitian ini akan berusaha mengungkapkan bagaimana publik mayantara menjalankan mekanisme penyelesaian permasalahan-permasalahan hukumnya ketika penegakan hukum belum berjalan efektif. Penelitian ini juga akan mengungkapkan berbagai permasalahan sosial mayantara dan besarnya ancaman

tindak pidana di dalamnya, yang dengan menjelaskannya akan memberikan gambaran bahwa masyarakat mayantara dengan berbagai jalinan sosialnya memiliki keteraturan mereka sendiri yang lebih baik daripada pengandaian dari hukum positif terhadapnya yang menyederhanakannya seakan dapat diatur sebagaimana hukum ditegakkan dalam dunia nyata.

Dengan memahami lebih baik mekanisme di dalam lingkungan sosial mayantara yang meliputi struktur sosial, alur komunikasi, serta peran-peran sosial di dalamnya, maka akan terungkapkan bagaimana cara yang lebih baik dalam penegakan hukum pidana mayantara dalam publik mayantara. Yang di dalamnya aparat penegak hukum tentu tidak dapat berjalan sendiri dalam menegakkan hukum, keterlibatan publik baik secara pasif maupun aktif senantiasa diperlukan dalam penegakan hukum untuk membangkitkan legitimasi hukum.

Penelitian ini diharapkan dapat memberikan gambaran dan memberikan pemahaman bagaimana peranan hukum dalam mengatur dunia maya dan seberapa besar peranannya sebagai kontrol sosial dengan pembahasan kajian pada penanganan tindak pidana di dalamnya. Dunia mayantara tidak semestinya menjadi wilayah yang berkembang tanpa jaminan dan keselamatan penggunanya dari ancaman pelaku kejahatan, karena mayantara bukanlah ranah tanpa hukum.

Dengan penelitian ini diharapkan adanya pemahaman lebih baik tentang perlunya sistem hukum pidana yang responsif dan progresif terhadap tindak pidana di dunia mayantara. Dengan mengkaji lebih jauh tentang konsep sosiologi hukum dalam dunia maya yang semakin berkembang, untuk menciptakan masyarakat taat hukum di dalam dunia yang kian cepat akan perkembangan kebutuhan dan sekaligus kejahatan di dalamnya. Lebih jauh lagi, penelitian ini bertujuan dapat memberikan perspektif kebijakan hukum dalam politik hukum pidana untuk pembentukan sistem peradilan pidana yang lebih baik.

## 1.5 KERANGKA TEORI

Upaya penegakan hukum dan penanggulangan berbagai bentuk kejahatan harus dilakukan secara keseluruhan, dan menjadi bagian usaha masyarakat untuk menciptakan keadilan bersama. Pengkajian masalah pencegahan kejahatan dan penegakan hukum memerlukan pemahaman mendalam mengenai format kebijakan yang digariskan, karena dengan demikian dapat diketahui seperti apa bentuk penegakan hukum yang akan dituju. Dalam dunia mayantara (internet) terdapat bentuk masyarakat yang dalam beberapa definisi mengalami perubahan dari pengertian mengenai masyarakat dalam berbagai literatur sosiologis yang berkembang sejak masa Ibnu Khaldun (abad ke-14 M) maupun sejak dimunculkan istilah 'sosiologi' oleh Auguste Comte (1798 – 1857 M) hingga perkembangan sosiologi modern terus berlanjut.[9] Dengan demikian, semestinya kebijakan hukum dalam penanggulangan kejahatan dan penegakan hukum di dalamnya perlu dikaji lebih lanjut untuk menyesuaikan perkembangan masyarakat.

Prof. Satjipto Rahardjo dengan konsep hukum progresifnya menekankan perlunya kreatifitas penegak hukum untuk tercapainya tujuan hukum, dengan cara yang progresif. Berangkat dari keinginan agar ilmu hukum lebih relevan dan lebih hidup, maka harus ada reintegrasi antara teori hukum, teori politik, dan teori sosial. Demikianlah semangat optimisme Philippe Nonet dan Philip Selznick yang menular dalam konsep hukum progresif Prof. Satjipto, yaitu semangat pengalaman empiris dengan berupaya menyusun kembali isu-isu dalam ilmu hukum dalam prespektif sosial. Oleh karenanya hukum tidak dilihat dari kacamata hukum itu sendiri, melainkan dilihat dan dinilai dari tujuan sosial yang

[9] Beberapa pemikir memfokuskan pandangan mereka tentang sosiologi kepada Barat, namun sesungguhnya penelusuran terhadap sosiologi telah dimulai oleh para sarjana dari Timur dan salah satunya adalah Ibnu Khaldun. Ritzer mengatakan bahwa Ibnu Khaldun telah menghasilkan sekumpulan karya yang mengandung berbagai pemikiran yang mirip dengan sosiologi zaman sekarang. Tentang Auguste Comte, ia lebih tepat disebut sebagai pencipta istilah 'sosiologi', namun tentang perkembangan modern dari sosiologi itu sendiri baru muncul di era-era sesudahnya. Lihat George Ritzer dan Douglas J. Goodman, *Teori Sosiologi Modern* (*Modern Sociological Theory*), diterjemahkan oleh Alimandan, (Jakarta: Kencana, cet. Keenam, 2010).

ingin dicapainya serta akibat-akibat yang timbul dari bekerjanya hukum.[10] Dengan pendekatan sosial akan memberikan gambaran bahwa segala tertib dalam bentuknya yang penuh kepastian pastilah memiliki relativitas dengan melihat secara langsung kehidupan sosial. Dengan pendekatan ilmu sosial, hukum menjadi sebuah pengalaman yang selalu berubah sesuai konteks dan tidak dapat secara sederhana diseragamkan begitu saja.

Sesuai dengan konsep keterpaduan sistem hukum—yang juga melibatkan sistem sosial, segala tindakan yang diambil oleh lembaga penyidik dalam menangani suatu pelanggaran aturan pidana sangat berpengaruh terhadap tindakan-tindakan selanjutnya yang akan diambil oleh subsistem peradilan pidana lainnya. Dalam masyarakat internet yang berubah dan semakin membedakan diri dari definisi masyarakat yang populer sejak berabad-abad silam, pola penegakan hukum pun perlu menyesuaikan dengan keadaan masyarakatnya. Dengan semangat pengalaman empiris untuk mengamati relativitas dalam masyarakat, pada gilirannya akan memberikan kesadaran baru untuk melibatkan masyarakat pelaku internet secara lebih sistematis dalam proses penegakan hukum, hal ini akan terkait erat dengan upaya penemuan bentuk kontrol sosial dari hukum mayantara yang efektif, juga akan membentuk sistem penegakan hukum yang efektif pula.

Prof. Soerjono Soekanto melengkapi konsep keterpaduan sistem hukum dengan menjelaskannya dalam faktor-faktor. Menurutnya bahwa masalah pokok penegakan hukum sebenarnya terletak pada faktor-faktor yang mungkin mempengaruhinya. Faktor-faktor tersebut mempunyai arti yang netral, sehingga dampak positif atau negatifnya terletak pada isi faktor-faktor tersebut. faktor-faktor tersebut adalah sebagai berikut: 1) Faktor hukumnya sendiri, yang dalam penjelasan Soerjono Soekanto dibatasi pada undang-undang; 2) Faktor penegak hukum, yakni pihak-pihak yang membentuk maupun menerapkan hukum; 3)

[10] Philippe Nonet dan Philip Selznick, *Hukum Responsif* (*Law and Society in Transition: Toward Responsive Law*), diterjemahkan oleh Raisul Muttaqien (Bandung: Nusamedia, 2010), hal. 4. Lihat juga, Satjipto Rahardjo, *Hukum Progresif*, cet. pertama, (Yogyakarta: Genta Publishing, 2009), hal. 7

Faktor sarana atau fasilitas yang mendukung penegakan hukum; 4) Faktor masyarakat, yakni lingkungan di mana hukum tersebut berlaku atau diterapkan; 5) Faktor kebudayaan, yakni sebagai hasil karya, cipta, dan rasa yang didasarkan pada karsa manusia di dalam pergaulan hidup.[11]

Kelima faktor tersebut saling berkaitan dengan eratnya, oleh karena merupakan esensi dari penegakan hukum, juga merupakan tolok ukur daripada efektivitas penegakan hukum.[12] Dalam penelitian ini akan berusaha menangkap pesan tersebut dan menerapkannya pada permasalahan penegakan hukum pidana mayantara, yang diharapkan dengan kelengkapan faktor-faktor yang mendukung tersebut dalam penegakan hukum, akan dapat menciptakan kepastian hukum dan legitimasi hukum dalam ruang mayantara. Dan dalam hal ini akan lebih memfokuskan pembahasan pada faktor masyarakat mayantara, yang tentu saja tidak dapat dipisahkan dari keempat faktor lainnya dalam menyusun logika pemahamannya, karena kelima faktor yang dijabarkan Soerjono Soekanto tersebut bukan terpisah-pisah tetapi terikat dan saling mendukung satu sama lain. Oleh karenanya perlu pemikiran kritis dalam mendalami ruang publik mayantara.

Perubahan sistem masyarakat juga akan meningkatkan kompleksitas badan-badan penegak hukum, hal ini kemudian tidak dapat bersikap setengah hati memperhatikan peran masyarakat. Prof. Satjipto mencoba mengadaptasi pemikiran Chambliss dan Seidman tentang pemilahan dua golongan besar dan keterlibatannya dalam penegakan hukum. Pembagian ini diadaptasi sebagai golongan yang terlibat dekat dan golongan yang terlibat jauh. Di dalam golongan yang terlibat dekat, meliputi legislatif yang berperan dalam pembentukan undang-undang dan kepolisian dalam penegakan hukum secara normatif. Kemudian dalam golongan yang terlibat jauh, mengelompokkan pribadi dan masyarakat dalam unsur lingkungan dalam satu golongan.[13] Kedua golongan ini

---

[11] Soerjono Soekanto, *Faktor-faktor yang Mempengaruhi Penegakan Hukum*, (Jakarta: Rajawali Press, 2010), hal. 8.

[12] *Ibid*., hal. 9.

[13] Satjipto Rahardjo, *Penegakan Hukum: Suatu Tinjauan Sosiologis*, (Yogyakarta: Genta Publishing, 2009). Hal. 24.

memiliki pengaruh dalam penegakan hukum dan menentukan dalam berhasil atau tidaknya tujuan penegakan hukum.

Pembenahan sistem hukum dengan meningkatkan kemampuan sosial erat dengan konsep yang dibawa oleh Jürgen Habermas (1929 – sekarang). Perunutan tentang konsep 'ruang publik', 'masyarakat komunikatif', atau pun 'krisis legitimasi'-nya yang muncul dalam masa-masa awal pemikirannya, juga akan terkait erat dengan ulasan Nonet dan Selznic tentang legitimasi dalam hukum.[14] Dalam mempertautkan kajian hukum dan juga sosiologi perlu pisau analisis yang kuat dari dua sisi tersebut secara kritis. Nonet dan Selznic diikuti oleh Satjipto Rahardjo di Indonesia dengan uraian panjang tentang penegakan hukum yang responsif dan progresif memberikan sederetan penelaahan kritis sepanjang era mereka, yang tidak luput juga beberapa pemikir sosiologi hukum yang meliputi mereka.

Dan dalam wacana kajian sosiologi kritisnya, keluar lalu masuk lagi dalam aliran Frankfurt di Jerman, Jürgen Habermas selama beberapa tahun menjadi pemikir neo-Marxis paling terkemuka di dunia. Tidak hanya melulu dalam pembahasan neo-Marxis, Habermas juga memasukkan banyak pemikiran baru ke dalam teori-teorinya tentang masyarakat modern.[15] Begitu pun pandangan dari hukum progresif yang melihat hukum bukan sebagai suatu konsep paripurna dan terus berkembang, menurut Habermas konsep manusia modern pun juga tak pernah usai. Dua bidang ini saling mengkritisi wilayahnya masing-masing dan memiliki pertautan dalam sosiologi, dengan semangat pendekatan empiris.

Pemikiran Jurgen Habermas yang dapat kita gunakan membedah karakter modernitas dalam dunia mayantara dan bagaimana peran ruang publik dalam

---

[14] Di Indonesia pemikiran Jurgen Habermas banyak dipromosikan oleh F. Budi Hardiman dalam berbagai bukunya. Kajian Budi Hardiman yang dikenal otoritatif terhadap pemikiran Habermas, di antaranya dalam buku-buku karyanya: Kritik Ideologi: Pertautan Pengetahuan dan Kepentingan (1990), Menuju Masyarakat Komunikatif (1993), Demokrasi Deliberatif (2008). Karya Jurgen Habermas mendapat tempat secara langsung, sebuah buku dari pemikiran awalnya: 'Krisis Legitimasi' (Qalam: 2004), terjemahan dari *Legitimation Crisis* (1975). Mengingat Habermas hanya menulis dalam bahasa Jerman karya-karyanya, kemungkinan itu adalah karya yang telah diterjemahkan dalam bahasa Inggris.

[15] Ritzer, *op.cit.*, hal. 579.

pembentukan kebijakan hukum dan dalam penegakan hukumnya. Dengan perangkat analisis sosialnya yang kritis kepada realitas masyarakat modern, gagasan masyarakat komunikatif, dan bagaimana Habermas berusaha menciptakan demokrasi mendialogkan hukum dengan konsep diskursusnya. Sebuah ruang bagaimana hukum kolektif yang diciptakan dari kesatuan pengertian tentang keadilan dan bagaimana mengupayakannya dengan komunikasi baik ruang publik maupun ruang privat. Dalam peta pemikiran Habermas, tanpa komunikasi yang intens, atau dengan kata lain, tanpa adanya kepedulian sosial tentang hukum dalam solidaritas yang mengoptimalkan komunikasi sebagai bentuk intimitas, maka masyarakat akan hancur karena fungsi hukum tidak berjalan dengan baik.

Landasan teoritis tersebut akan membantu dalam menyusun argumen untuk menjelaskan peran publik dalam penegakan hukum pidana mayantara, khususnya di Indonesia. Semangat pengalaman empiris meliputi penelitian ini, pengamatan lebih dekat akan memberikan gambaran lebih mendalam tentang sistem masyarakat mayantara, berbagai permasalahan pidana di dalamnya, dan terutama bagaimana setiap masalah diantisipasi dan diatasi di dalamnya dengan mencocokkannya dengan tujuan hukum itu sendiri.

Karena penegakan hukum tidak hanya berpegang pada keharusan-keharusan sebagaimana tercantum dalam ketentuan-ketentuan hukum, karena hanya akan memperoleh gambaran stereotipis yang kosong. Membahas penegakan hukum akan menjadi lebih berisi apabila dikaitkan pada pelaksanaannya yang kongkrit oleh manusia.[16] Dan masyarakat mayantara merupakan unsur dominan penegakan hukum pidana mayantara.

Mendesaknya kebutuhan masyarakat (publik) mayantara mengenai penegakan hukum pidana mayantara menjadikan sedemikian pentingnya dukungan masyarakat, posisi publik tidak semata-mata sebagai bagian di luar penegakan hukum dan juga tidak dalam pengertian ‘peran aktif’ dalam penegakan hukum yang ada selama ini, yang memposisikannya sebagai ruang

[16] Rahardjo, *op.cit.,* hal. 26.

pencegahan tindak pidana. Akan tetapi, saat faktor penegak hukum dan faktor hukumnya itu sendiri (undang-undang, dalam penjelasan Soerjono Soekanto) belum siap, sedangkan pemahaman dan arus pengetahuan mayantara sedemikian luas tersebar dan dipahami secara lebih baik oleh publik, maka integrasi antara peran-peran penegakan hukum semestinyalah mampu membuka kemungkinan penegakan hukum mayantara yang lebih baik.

Dengan memanfaatkan karakter dinamis dari hukum progresif, maka kondisi hukum akan lebih mudah dalam menyerap dinamika perubahan sosial, hal inilah yang mampu menciptakan kemungkinan-kemungkinan hukum yang mampu beradaptasi dengan cepatnya perubahan sosial dan perkembangan kejahatan. Akan tetapi hukum progresif yang disampaikan oleh Prof. Satjipto Rahardjo adalah konsep teoritis dengan mengamati serta mengkaji bagaimana semestinya hukum bertindak dalam dinamika masyarakat yang terus berubah.

Oleh karenanyalah diperlukan kerangka konseptual untuk memberikan perhitungan-perhitungan logis tentang bagaimana interaksi antara hukum, penegak hukum, dan masyarakat itu mungkin. Habermas menawarkan gagasannya tentang tindakan komunikatif dan diskursus yang berciri khas deliberatif. Konsep inilah yang melengkapi rasionalisasi pembentukan hukum pidana mayantara yang responsif terhadap keadaan dan bisa mengawal keadaan, serta menjamin kepastian hukum. Gagasan-gagasan Habermas yang senantiasa ‘terjaga’ dalam menghadapi logika modernitas inilah sekiranya yang mampu menjaga hukum berdiri pada tempatnya, sebagai kesahihan konsesual, meskipun ruang sosial dan masyarakat senantiasa bergolak dengan modernitas. Tentunya dengan memperhatikan batasan-batasan di dalamnya.

## 1.6 KERANGKA KONSEPSIONAL

Penegakan hukum berkaitan erat dengan ketaatan bagi para pihak terkait yang melaksanakan dan menggunakan undang-undang, yaitu masyarakat luas dan para penegak hukum yang mewakili peran negara. Penegakan hukum pidana dalam mayantara tidak terlepas dari pemahaman yang sama dari kedua pihak

tersebut sebagaimana konsepsi-konsepsi yang terdapat dalam hukum pidana. Dari kerangka konsepsional tersebut akan diberikan definisi atau batasan operasional dalam penelitian.

Penelitian ini mengkaji tentang penegakan hukum pidana mayantara, dengan ruang lingkup aktifitas publik mayantara. Pengertian mayantara merupakan adaptasi dari pengertian *cyberspace.* Sebagaimana ada dalam Penjelasan Umum Undang-undang Nomor 11 Tahun 2008, tentang Informasi dan Transaksi Elektronik (ITE), "Hukum siber atau *cyberlaw*, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan telekomunikasi… Istilah lain yang juga digunakan adalah hukum teknologi informasi (*law of information technology*), hukum dunia maya (*virtual world law*), dan hukum mayantara." Dan pembahasan tentang virualitas tersebut meliputi komunikasi lokal maupun global (Internet). Namun penelitian ini bertolak dari konsep globalnya, yang tentu memiliki tempatnya juga dalam lokalitas, dengan fokus pada komunitas mayantara.

Mengenai penegakan hukum pidana adalah upaya menegakkan hukum pidana sebagaimana peran-peran yang dimiliki oleh organ-organ dalam sistem peradilan pidana. Dan dalam penelitian ini menfokuskan pada penegakan hukum pidana terhadap berbagai tindak pidana dalam mayantara, dengan memperhatikan peran sosial untuk menciptakan stabilitas sosial dan legitimasi hukum dalam mayantara.

Dan secara khusus mengenai *cyberlaw* dalam membahas *cybercrime* sebagaimana dijelaskan oleh David S. Wall.[17] Bahwa kejahatan cyber (mayantara) adalah kejahatan yang dijalankan dengan menggunakan peran jaringan internet sebagai sarananya. Hal ini memiliki pengertian yang lebih luas dari pengertian tentang telematika. Telematika lebih spesifik sebagai ICT (*Information and Communication Technology*) yang berkaitan erat dengan pengiriman, penerimaan, dan penyimpanan informasi melalui alat komunikasi yang menggunakan kontrol, termasuk kontrol jarak jauh. Sedangkan pengertian

[17] David S. Wall, ed., *Crime and The Internet,* (New York: Routledge, 2001).

*cyber* tidak cukup dalam pengertian telematika, '*cyber'* memiliki makna yang lebih luas. *Cyber* meliputi segala bentuk interaksi maya yang mensimulasikan serta menyederhanakan aktifitas dunia nyata dalam berbagai bentuk simulasi di ruang maya. Oleh karenanya dapat dikatakan bahwa segala bentuk kejahatan di dunia nyata dapat dilakukan dalam ruang mayantara.

Penelitian tentang 'publik' lebih fokus kepada komunitas *hacker*, dikarenakan mereka memiliki kompetensi yang lebih sesuai dengan permasalahan tindak pidana mayantara, baik dalam pemahaman konsep, pembentukan komunitas, penyelesaian masalah secara otonom, serta pemberian pengaruh terhadap anggota ruang publik mayantara yang lainnya. Penjelasan mengenai hal ini akan lebih jauh dijabarkan dalam uraian pembahasan di bab-bab selanjutnya.

## 1.7 METODE PENELITIAN

Penelitian ini bertujuan untuk memberikan gambaran seaktual mungkin mengenai konsep pencegahan dan penanggulangan kejahatan mayantara melalui kacamata sistem peradilan pidana. selain itu, penelitian juga dimaksudkan untuk memahami seobjektif mungkin kedudukan dan peran masyarakat mayantara dalam melakukan pencegahan dan penanggulangan kejahatan melalui pemberdayaan sistem peradilan pidana, dengan memfokuskan terhadap pencegahan dan penanggulangan tindak pidana mayantara.

### 1.7.1 Bentuk dan jenis penelitian

Penelitian ini merupakan penelitian hukum normatif, yang bersifat deskriptif. penelitian ini mencoba menjelaskan hal ihwal pencegahan dan penanggulangan kejahatan pada umumnya, khususnya kejahatan internet, berdasarkan peraturan perundang-undangan yang berlaku, dengan memperhatikan perkembangan teori hukum yang paling mutakhir dalam membangun perspektif perkembangannya pada masa mendatang. Penelitian ini bersifat sosiologis/non doktrinal dengan pendekatan

interaksional dengan analisis kualitatif terhadap lingkungan sosial publik mayantara dalam menghadapi tindak pidana mayantara.

### 1.7.2 Alat-alat Pengumpulan Data

Data penelitian ini dikumpulkan melalui dua cara, yaitu penelitian kepustakaan dan penelitian lapangan.

a. Penelitian kepustakaan dilakukan terhadap bahan hukum primer (peraturan perundang-undangan), bahan hukum sekunder (pendapat para pakar hukum dan pakar sosial terkemuka) dan bahan hukum tersier (ensiklopedia dan kamus hukum yang relevan dengan objek penelitian) untuk mendapatkan data sekunder.
b. Penelitian lapangan dilakukan untuk mendapatkan data primer, dilakukan melalui wawancara terhadap para penggiat dunia maya serta aktivis-aktivis berbagai komunitas mayantara di Indonesia, para pengamat sosial yang memberikan kajian terhadap kehidupan mayantara. Wawancara dilakukan dengan alat pedoman wawancara. Dengan pengamatan yang telah lama dilakukan, observasi lapangan dilakukan dengan peran *observer as participant,*[18] yang secara definitif peneliti dapat merekam informasi yang muncul, dan informasi yang bersifat '*private'* secara selektif tidak ikut dilaporkan.

### 1.7.3 Analisis Data

Analisis data dilakukan baik secara doktrinal maupun non doktrinal. analisis data secara doktrinal dilakukan dengan memperhatikan asas-asas hukum, peraturan perundang-undangan dan yurisprudensi mengenai objek penelitian. analisis nondoktrinal dilakukan dengan menggunakan konsep metode ilmu sosial lainnya, seperti filsafat, politik, sosiologi dan juga kriminologi.

## 1.8 SISTEMATIKA PENULISAN

[18] John W. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, second edition, (London: Sage Publication, 2003), hal. 186.

Bab 1: Pendahuluan yang menguraikan latar belakang permasalahan rumusan permasalahan, pertanyaan penelitian, tujuan penelitian, kerangka teoritis, kerangka konsepsional, metode penelitian yang akan digunakan dalam penelitian ini, dan sistematika penulisan laporan penelitian.

Bab 2: Membahas tentang tinjauan pustaka terhadap masyarakat mayantara dan tindak pidana mayantara. Dalam bab ini akan dibahas mengenai sistem peradilan pidana, pendekatan hukum responsif, pengantar kepada sosiologi hukum, dan pembahasan pemikiran Jurgen Habermas yang akan digunakan dalam mengkaji peran publik dalam penegakan hukum pidana mayantara.

Bab 3: Dinamika sosial mayantara dan *cybercrime*. Dalam bab ini akan membahas mengenai pengamatan empiris atas sistem sosial masyarakat mayantara di Indonesia, dan perkembangan tindak pidana dalam masyarakat mayantara.

Bab 4: Penegakan Hukum terhadap *cybercrime*. Dalam bab ini akan dibahas mengenai peran publik mayantara dalam pengakan hukum, kendala penegakan hukum pidana mayantara di Indonesia, peranan *hacker* dalam penegakan hukum pidana mayantara dengan perspektif teori diskursus Jurgen Habermas, serta memberikan gambara tentang bentuk-bentuk kerjsama yang mungkin dapat dijalin antara agen sosial mayantara dengan lembaga penegak hukum.

Bab 5: Penutup dan Kesimpulan. Bab ini merupakan bab penutup dan kesimpulan dari hasil penelitian, serta rekomendasi dan saran-saran yang telah dirumuskan dari hasil penelitian dan pembahasannya.

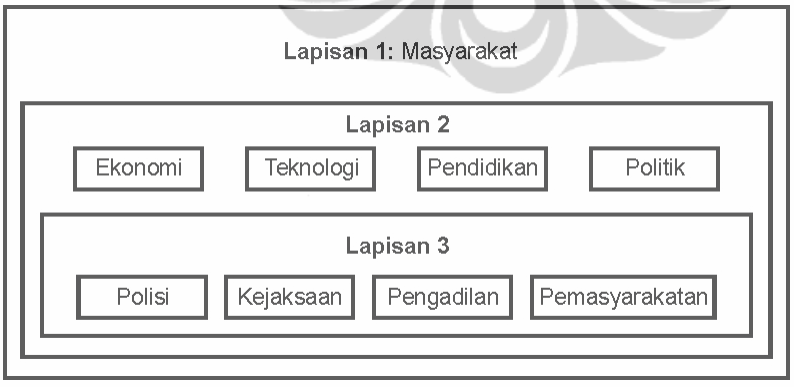
# BAB II

# TINJAUAN PUSTAKA

## 2.1 Sistem Peradilan Pidana

Prof. Mardjono Reksodiputro mendukung alasan untuk terus menuju perbaikan sistem peradilan pidana di Indonesia, beliau menekankan perlunya riset-riset baru untuk menemukan fakta baru dan untuk menyempurnakan pengertian tentang fakta-fakta baru yang diamati. Ketelitian dalam prosedur sistem peradilan pidana merupakan bagian penting, sehingga evaluasi pada hasil penelitian akan lebih terarah dan memiliki tujuan yang tidak melenceng dari standarisasi tersebut.

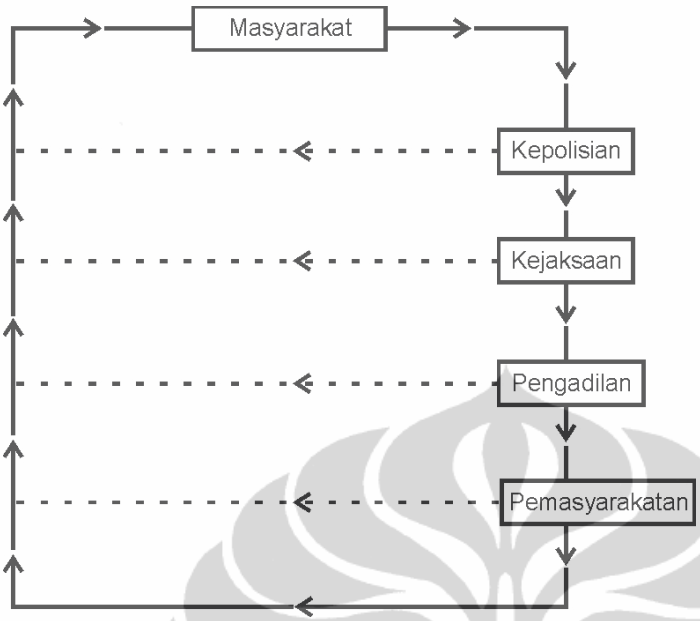
Mardjono Reksodiputro menjelaskan gambaran struktur hukum dalam masyarakat bersama dengan unsur-unsur yang mempengaruhinya dalam skema. Skema tersebut memperlihatkan bahwa proses peradilan pidana itu adalah suatu sistem, dengan kepolisian, kejaksaan dan pengadilan, serta pemasyarakatan sebagai sub-sub sistem. Pelanggar hukum berasal dari masyarakat dan akan kembali kepada masyarakat, baik sebagai warga yang taat kepada hukum (non residivis), maupun mereka yang kemudian akan mengulangi kembali perbuatannya (residivis). Proses terpadu dari peradilan pidana ini mewajibkan pendekatan sistemik dalam riset-riset.[19]




*Gambar 2.1. Lapisan-lapisan dalam sistem peradilan pidana.*[20]

[19] Mardjono Reksodiputro, *Kriminologi dan Sistem Peradilan Pidana*, (Jakarta: Pusat Pelayanan Keadilan dan Pengabdian Hukum Universitas Indonesia, cet. Kedua, 2007), hal. 98-99.

[20] *Ibid.*, hal. 99.




*Gambar 2.2. Bagan alir sistem peradilan pidana.*[21]

Dalam proses penegakan hukum pidana, alur yang digambarkan memperlihatkan luasnya sistem. Tidak hanya sebatas pada institusi-institusi penegak hukum saja, akan tetapi juga turut menarik peran masyarakat dalam sistem peradilan pidana. Luhut M. P. Pangaribuan mendukung gambaran tersebut, ia menyatakan bahwa SPP merujuk pada suatu cakupan substansi yang lebih luas bila dibandingkan dengan hukum acara pidana. Oleh karena itu dapat dikatakan bahwa SPP adalah hukum acara pidana dalam arti luas sementara istilah hukum acara pidana saja adalah SPP dalam arti sempit.[22]

Keluasan wilayah dari SPP ini memungkinkan banyak permasalahan dalam penyelesaian berbagai masalah hukum, keterkaitannya dengan masyarakat luas bukanlah hal yang sesederhana membahas empat lembaga hukum saja. Dengan berbagai gejolak dalam masyarakat Mardjono Reksodiputro menekankan pentingnya administrasi keadilan pidana untuk senantiasa mampu mengendalikan sikap emosional dan terus berusaha lebih rasional.[23] dan dengan cara menemukan

[21] *Ibid.*

[22] Luhut M. P. Pangaribuan, *Lay Judges & Hakim Ad Hoc*, (Jakarta: Program Pascasarjana Fakultas Hukum Universitas Indonesia, 2009), hal. 70.

[23] Reksodiputro, *op.cit.*, hal. 100.

fakta-fakta baru serta mengevaluasi fakta-fakta lama melalui berbagai riset terhadap masyarakat dan permasalahan kejahatan yang ada di dalamnya akan memberikan cara pandang yang lebih rasional menurut jamannya.

Dengan orientasi kesisteman ini Mardjono Reksodiputro mengatakan bahwa sistem peradilan pidana dapat digambarkan secara singkat sebagai suatu sistem yang bertujuan untuk "menanggulangi kejahatan", salah satu usaha masyarakat untuk mengendalikan terjadinya kejahatan agar berada dalam batas-batas toleransi yang dapat diterima. Sistem ini dianggap berhasil, apabila sebagian besar dari laporan dan keluhan masyarakat bahwa mereka yang telah menjadi korban kejahatan dapat diselesaikan dengan diajukannya pelaku ke muka sidang pengadilan dan menerima pidana. menjadi bagian dari tugas sistem adalah mencegah seseorang menjadi korban kejahatan, dan mencegah seseorang mengulang kejahatannya. Dengan demikian tugasnya adalah: (a) mencegah masyarakat menjadi korban kejahatan, (b) menyelesaikan kejahatan yang terjadi, sehingga masyarakat puas bahwa keadilan telah ditegakkan dan yang bersalah dipidana, serta (c) berusaha agar mereka yang pernah melakukan kejahatan tidak mengulangi lagi perbuatannya.[24]

Di sisi lain ada pertimbangan jika sistem tidak bekerja dengan baik, dan ini akan menimbulkan berbagai kerugian yang akan terjadi di dalam mengoreksi kesalahan sistem, yang berkisar pada:

(a) Kesukaran dalam menilai sendiri keberhasilan atau kegagalan masing-masing instansi, sehubungan dengan tugas mereka;
(b) Kesulitan dalam memecahkan sendiri masalah-masalah pokok masing-masing instansi (sebagai sub-sistem); dan
(c) Karena tanggungjawab masing-masing instansi sering kurang jelas terbagi, maka setiap instansi tidak terlalu memperhatikan efektivitas menyeluruh dari sistem peradilan pidana.[25]

[24] Reksodiputro, *ibid.*, hal. 140. Lihat juga, Pangaribuan, *op.cit.*, hal. 72.
[25] Reksodiputro, *op.cit.*, hal. 142.

Pertimbangan bagaimana sulitnya mengurai permasalahan dan memilah-milah kesalahan kinerja secara utuh dengan melihat satu persatu kesalahan adalah karena keempat lembaga penegakan hukum tersebut bekerja dalam satu keterpaduan kerja dalam sistem peradilan pidana.[26] Sebagaimana mekanisme sistemik yang digambarkan dalam *Gambar.2* di atas memperlihatkan bahwa kinerja tiap lembaga meskipun terlihat terpisah-pisah akan tetapi berada dalam satu alur dan satu tujuan bersama untuk menciptakan keadilan dalam masyarakat.

Peranan lembaga tersebut saling berhubungan satu sama lain, Mardjono Reksodiputro mengibaratkannya seperti yang digambarkan dalam model Jepang sebagai "seperangkat roda-gigi yang harus cermat dan ulet menjaga kombinasi yang baik antara masing-masing roda-gigi tersebut".[27] Tentunya akan fatal jika salah satu roda-gigi mengalami kerusakan, hal ini dapat merusak kinerja sistem peradilan pidana secara menyeluruh, baik itu melambat ataupun terhenti di tengah jalan. Maka, kinerja efektif dan mengikuti tertib sistem akan menjaga mekanisme yang ada tetap stabil, karena kesalahan satu roda-gigi dapat merugikan utuhnya tujuan sistem.

### 2.1.1 Model Sistem Peradilan Pidana

Herbert Packer-lah yang mengidentifikasikan dan menjelaskan dua model atau *"value systems that compete for priority in the operation of the criminal process."* Dia menamainya dengan *Crime Control Model* dan *Due Process Model*.[28] Dalam sistem diperlukan nilai-nilai yang menjadi patokan prioritas untuk menjalankan prosesnya dengan baik dan terarah.

#### *2.1.1.1 Crime Control Model*

Penjelasan mendasar tentang *crime control model* adalah: *The repression of criminal conduct is by far the most important function to be performed by the criminal process*. Menurut model

[26] *Ibid.*, hal. 142.
[27] *Ibid.*, hal. 145.
[28] N. Gary Holten dan Lawson L. Lamar, *The Criminal Courts*, (New York: McGraw-Hill, 1991), hal. 3.

ini, kesalahan dalam penegakan hukum untuk menyeret pelaku kriminal di bawah kontrol ketat dapat mengarah kepada keruntuhan aturan publik dan karenanya menjadikan hilangnya sebuah kondisi penting dari kebebasan manusia. Jika hukum berjalan tanpa ditegakkan—dengan maksud, jika ada anggapan bahwa terdapat sebuah presentase yang tinggi dari kegagalan menahan dan memenjarakan dalam proses pidana—sebuah sikap tak acuh secara umum terhadap kontrol hukum akan cenderung terbangun. Warga masyarakat yang taat hukum kemudian akan menjadi korban dari semua bentuk serangan kepentingan-kepentingan yang tidak bisa dibenarkan. Keamanan mereka atas pribadi dan properti secara tajam akan berkurang dan, karenanya, begitu juga kemerdekaan mereka sebagai anggota suatu masyarakat.[29]

Packer menjelaskan bahwa beberapa hal penting bagi pendekatan ini untuk bisa berhasil: (1) harus ada penahanan dan pemidanaan dalam tingkat tinggi; (2) harus ada "keutamaan pada kecepatan dan ketegasan"; (3) harus ada pengakuan pada kenyataan bahwa kecepatan tergantung pada informalitas dan kebersamaan, sedangkan ketegasan tergantung pada minimalitas peluang bagi tantangan; dan (4) "proses seharusnya tidak dikusutkan oleh ritual seremonial yang tidak mendukung kemajuan sebuah kasus." Oleh karenanyalah proses yang ideal, menurut model ini, akan menekankan pada ekstrajudisial dibandingkan pada prosedur judisial.[30]

#### *2.1.1.2 Due Process Model*

Due process model lebih tampak sebagai *obstacle course*. Model ini berangkat dari sebuah ideologi bahwa ini bukanlah

[29] *Ibid.*
[30] *Ibid*., hal. 4.

lawan dari apa yang digarisbawahi oleh *crime control model*, karena ini juga mengasumsikan bahwa represi terhadap kejahatan merupakan sesuatu yang diharapkan secara sosial. Terlebih, ideologi di balik *due process model* adalah "menyusun sebuah komplek dari berbagai ide" melibatkan kemanjuran dari *crime control* dan sejumlah kecil pertimbangan yang berbeda.[31]

Jika dalam *crime control model* menegaskan bahwa kesalahan faktual (*factual guilt*) merupakan pertimbangan penting, sedangkan dalam *due process model* menekankan pada doktrin *legal guilt*. Model ini dinyatakan sebagai yang paling keras sebagai sebuah serangan terhadap gagasan bahwa terdakwa mendapatkan keadilan yang bisa mereka dapatkan.[32] Dengan demikian sejak awal proses dalam *due process model judicial scrutiny* adalah suatu keharusan dan tidak boleh ditunda. Sebab *probative data* dari penyidik itu, sebagai dasar untuk menangkap dan menahan, *is subject to subsequent judicial scrutiny*.[33]

### 2.1.2 Model SPP Indonesia

M. Yahya Harahap dalam "Pembahasan Permasalahan dan Penerapan KUHAP,"[34] mendefinisikan bahwa apa yang didukung dalam hukum acara pidana Indonesia (KUHAP/ Undang-undang No. 8 Tahun 1981) adalah konsep *due process*.

Hal ini dipaparkan pada awal pembahasan oleh M. Yahya Harahap, bahwa dalam melaksanakan fungsi "penyelidikan" dan "penyidikan", konstitusi memberi "hak istimewa" atau "hak privilese" kepada Polri untuk: "memanggil-memeriksa-menangkap-menahan-menggeledah-menyita" terhadap tersangka dan barang uang dianggap berkaitan dengan

[31] *Ibid*., hal. 4-5.
[32] *Ibid*., hal. 6.
[33] Pangaribuan, *op.cit.*, hal. 95.
[34] M. Yahya Harahap, *Pembahasan Permasalahan dan Penerapan KUHAP: Penyidikan dan Penuntutan*, (Jakarta: Sinar Grafika, cet. Kedelapan, 2009), hal. 95.

tindak pidana. Akan tetapi, dalam melaksanakan "hak" dan "kewenangan istimewa" tersebut, harus taat dan tunduk kepada prinsip: *the right of due process.* Setiap tersangka berhak diselidiki dan disidik di atas landasan "sesuai dengan hukum acara".[35]

Penegasan konsep due process dalam hukum acara pidana kita perlu disuarakan lebih lantang, karena kenyataannya terdapat banyak permasalahan pelanggaran HAM disuarakan oleh masyarakat yang menghadapi tindakan penegak hukum, terutama dalam seluruh proses penyelidikan dan penyidikan. Dengan memahami arti pentingnya penegak hukum untuk taat pada tertib beracara, maka masyarakat juga akan memahami arti pentingnya memahami hukum acara itu sendiri dengan memperhatikan hak-hak mereka dan kewajiban para penegak hukum terhadap mereka dalam menjalankan tugasnya. Dan M. Yahya Harahap menjelaskan hak ini sebagai *right of due process*.

Hak *due process* dalam melaksanakan tindakan penegakan hukum, bersumber dari cita-cita "negara hukum" yang menjunjung tinggi "supremasi hukum" (*the law is supreme*), yang menegaskan: "kita diperintah oleh hukum" dan "bukan oleh orang" (*government of law and not of men*).[36] Konsep *due process* yang melekat dalam sistem peradilan pidana Indonesia dapat diambil penegasan dalam beberapa bagian perbandingan yang dikutip oleh N. Gary Holten:

| ***Due Process Model*** | ***Crime Control Model*** |
|---|---|
| *Personal autonomy is more highly valued than overall societal freedoms; personal privacy rights are paramount; certain criminal violations (e. g., victimless crimes) are more difficult to detect.* | *Overall societal freedom are more highly valued than personal autonomy; there is less attention paid to personal privacy rights; all criminal violations (including victimless crimes) are more easily detected.* |
| *Presumption of innocent is attached* | *Presumption of guilty is attached* |

[35] *Ibid*.
[36] *Ibid*.

| | |
|---|---|
| *to all persons involved in the system.* | *to those persons not screened out of the system.* |
| *The central importance of the fact finding attaches to the formal, adjudicative, adversarial fact-finding process in which the factual case against the defendant is publicly heard by an impartial tribunal and is decided only after the accused has full opportunity to discredit the charges.* | *The central importance of fact finding attaches to informal, pretrial, administrative, fact-finding processes, which lead to exoneration of the suspect or entry of a guilty plea. The criminal process is characterized by routinized operations designed to screen out the innocent and convict the guilty as quickly as possible.* |
| *There is distrust of any fact-finding process, with corresponding deemphasis on speed and finality.* | *There is a basic trust in the fact-finding process, with a corresponding premium placed on speed and finality.* |
| *Legal guilt is paramount.* | *Factual guilt is paramount.* |
| *It sees the criminal process as an obstacle course.* | *It sees the criminal process as an assembly line.* |
| *Emphasis is placed on the individual, on preventing victimization of the defendant by the system, and on protecting the factually and legally innocent.* | *Emphasis is placed on the group, society, or the system, on preventing victimization of the public by criminals, and on convicting the factually guilty.* |

Tabel 2.1. *Packer's* due *process and crime control models: a comparison.*[37]

Karakter-karakater dalam due process model dalam perbandingan di atas terdapat pula dalam sistem peradilan pidana Indonesia, yang sebagian di antaranya telah dirumuskan dalam Bab VI KUHAP (M. Yahya Harahap mengurainya):

1) *The right of self incrimination.* Tidak seorang pun dapat dipaksa menjadi saksi yang memberatkan dirinya dalam suatu tindak pidana.

[37] Holten, *op.cit.*, hal. 7. Lebih lengkap ada dalam, Herbert L. Packer, *The Limit of Criminal Sanction*, (Stanford: Stanford University Press, 1968), hal. 149-173.

2) "Dilarang mencabut" atau "menghilangkan" (*deprive*) "hak hidup" (*life*), "kemerdekaan" (*liberty*) atau "harta benda" (*property*) tanpa sesuai dengan ketentuan hukum acara (*without the process of law*).
3) Setiap orang harus "terjamin hak terhadap diri" (*person*), "kediaman, surat-surat" atas pemeriksaan dan penyitaan yang "tidak beralasan" (*unreasonable searches and seizures*).
4) "Hak konfrontasi" (*the right to confront*) dalam bentuk "pemeriksaan silang" (*cross examine*) dengan orang yang menuduh (melaporkan).
5) "Hak memperoleh pemeriksaan (peradilan)" yang cepat (*the right to a speedy trial*).
6) "Hak perlindungan yang sama" dan "perlakuan yang sama dalam hukum" (*equal protection and equal treatment of the law*).
7) "Hak mendapat bantuan penasihat hukum" (the right to have assistance of councel) dalam pembelaan diri. Hak ini merupakan prinsip yang diatur dalam Pasal 56 KUHAP. Dan apa yang diatur dalam Pasal 56 ini merupakan bagian yang tidak terpisah dari asas *presumption of innocent* serta berkaitan dengan pengembangan *Miranda Rule* yang juga telah diadaptasi dalam KUHAP.[38]

Dengan perbandingan unsur-unsur penanda dan penegasan dalam KUHAP yang dipilah-pilah oleh M. Yahya Harahap, tampak lebih jelas bahwa usaha untuk mencapai keadilan di dalam hukum memerlukan proses *law enforcement* yang manusiawi dan menghargai setiap subjek hukum, mereka yang terlibat dalam suatu perkara. Oleh karena itu kesadaran masyarakat untuk melakukan berbagai tindakan hukum semestinya mendapat pengarahan lebih baik untuk menyadari hak-haknya, dan menghindari pelanggaran atasnya. Di samping itu SDM penegak hukum juga perlu terus diperbaiki untuk memberikan dukungan pada sistem dengan baik.

[38] Harahap, *op.cit.*, hal. 96.

### 2.1.3 Penelitian Sebagai Upaya Perbaikan Sistem Hukum

Pendekatan terhadap SPP dan melakukan pemahaman ulang seiring perkembangan zaman akan memberikan wawasan baru. Riset dan survei juga akan memberikan keterbukaan pada fakta-fakta baru kriminalitas dalam masyarakat. Mardjono Reksodiputro mendorong hal tersebut untuk memberikan sikap dan cara pandang yang lebih rasional terhadap proses sistem peradilan pidana. Karena, bukanlah fakta yang dapat dan untuk dihindari, bahwa kriminalitas selalu berkembang, seiring berkembangnya tingkat kehidupan dan teknologi maka akan berkembang pula kemuslihatan manusia di dalam hidup.

Riset dalam bidang sistem peradilan pidana dapat didekati dari berbagai aspek, misalnya:

(a) Tentang perkembangan kriminalitas pada umumnya, maupun perkembangan dari delik-delik tertentu;
(b) Tentang pelaksanaan penegakan hukum terhadap kriminalitas pada umumnya, maupun terhadap delik-delik tertentu;
(c) Tentang cara kerja badan-badan penegakan hukum: kepolisian, kejaksaan dan pengadilan;
(d) Tentang usaha pembinaan terhadap para terpidana, baik di dalam maupun di luar lembaga, dan termasuk dalam hal ini cara kerja dari badan-badan yang menangani usaha pembinaan ini;
(e) Tentang partisipasi masyarakat dalam usaha penanggulangan kriminalitas, maupun dalam usaha pembinaan ex-terpidana; dan
(f) Tentang faktor-faktor budaya dan sosial yang mempengaruhi atau dapat mempengaruhi perkembangan kriminalitas, usaha-usaha penegakan hukum (termasuk pembuatan maupun penghapusan undang-undang pidana), dan pembinaan terpidana maupun ex-terpidana.[39]

[39] Reksodiputro, *op.cit.*, hal. 105.

Penelitian ini berusaha membuka hal-hal baru dalam kriminalitas dan kemungkinan baru dalam mekanisme sistem peradilan pidana. Dengan memahami wawasan baru dalam wilayah mayantara dan aktifitas di dalamnya akan memberikan gambaran bahwa begitu pesatnya teknologi dan kriminalitas di dalamnya. Dan pola sosial yang berkembang akan memberikan petunjuk menemukan ikatan sosial (*social bond*) mungkin (*possible*) dalam upaya menguatkan sistem peradilan pidana di dalamnya.

M. Yahya Harahap memberikan tiga faktor pertimbangan yang menjadi dukungan bagi perbaikan sistem peradilan pidana (KUHAP):

1) Keterbatasan manusia memprediksi secara akurat apa yang terjadi di masa yang akan datang.
2) Kehidupan masyarakat manusia baik sebagai kelompok dan bangsa—nasional, regional, dan internasional—mengalami perubahan "dinamik". Selalu terjadi perubahan masyarakat (*social change*).
   Di dalam bidang hukum berlaku ajaran sosiologis yang memperingatkan *mutual interactive between social change and law development.*
3) Pada saat undang-undang diundangkan, langsung "konservatif".
   Undang-undang yang telah diterapkan cukup lama berhadapan dengan masyarakat yang kian hari kian berubah dengan cepat.[40]

## 2.2 Pendekatan Hukum Responsif

Nonet dan Selznick mengutip perkataan Jerome Frank, bahwa tujuan utama kaum realisme hukum adalah untuk membuat hukum "menjadi lebih responsif terhadap kebutuhan-kebutuhan sosial." Menjelaskan bahwa perkembangan hukum responsif telah menjadi kegiatan hukum modern yang terus berkelanjutan. Perkembangan hukum yang tanggap terhadap kebutuhan sosial adalah untuk memberikan kemampuan bagi institusi hukum "untuk secara lebih menyeluruh

[40] Harahap, *op.cit.*, hal. 12-13.

dan cerdas mampertimbangkan fakta sosial yang di situ hukum tersebut berproses dan diaplikasikan."[41]

Munculnya bentuk-bentuk hukum: represif, otonom, dan responsif, dapat dipahami sebagai tiga respon terhadap dilema yang ada antara integritas dan ketebukaan.[42] Hukum responsif ini untuk menunjukkan suatu kapasitas beradaptasi yang bertanggungjawab, dan dengan demikian adaptasi yang selektif dan tidak serampangan. Suatu institusi yang responsif mempertahankan secara kuat hal-hal yang esensial bagi integritasnya sembari tetap memperhatikan keberadaan kekuatan-kekuatan baru dalam lingkungannya. Untuk melakukan hal ini, hukum responsif memperkuat cara-cara bagaimana keterbukaan dan integritas dapat saling menopang walaupun terdapat pertentangan di antara keduanya. Nonet dan Selznick menekankan bahwa, lembaga responsif menganggap tekanan-tekanan sosial sebagai sumber pengetahuan dan kesempatan untuk melakukan koreksi-diri.[43]

Dengan mengingat kembali peran dan pentingnya kajian pidana terhadap lingkungan sosial, terutama peran pemasyarakatan dan pemulihan kondisi sosial, di dalam kajian-kajian sosiologis sebagaimana diingatkan oleh Jan Remellink. Nonet dan Selznick juga mengingatkan bahwa, walaupun hukum responsif mempunyai visi diharmonisasikannya kekuasaan-kekuasaan dan dikaburkannya batas-batas institusional, pembedaan antara keputusan hukum dan keputusan politik tidak dihapuskan.[44]

Nonet dan Selznick mensyaratkan kepada pemerintah sebagai aktor politik untuk tetap memberikan objektifitas yang maksimal bagi elaborasi kebijakan publik, termasuk definisi yang lebih pasti mengenai tujuan yang diterima dan klarifikasi progresif terhadap pilihan-pilihan politik serta pilihan-pilihan

[41] Philippe Nonet dan Philip Selznick, *Hukum Responsif* (Law and Society in Transition: Toward Responsive Law), diterjemahkan oleh Raisul Muttaqien (Bandung: Nusamedia, 2010), hal. 83.
[42] *Ibid.*, hal. 86.
[43] *Ibid.*, hal. 87.
[44] *Ibid*., hal. 123-124.

strategis. Kekuatan pada objektifitas yang harus dipenuhi, maka pemerintah akah dapat melampaui politik kekuasaan.[45]

Dalam Publik mayantara yang sedemikian majemuknya, yang terangkum dalam satu ruang sosial *cyber*. Kekuasaan di dalamnya bukan sekedar kekuasaan akan ruang publik itu sendiri, melainkan juga kekuasaan akan pengetahuan. Peran kritik dan peran opini publik dari publik mayantara akan mampu menjadi bentuk komunikasi antara mereka yang memiliki kekuasaan dan yang tidak di dalam ruang publik. Konsep yang dimiliki hukum responsif ini juga menjadi kesatuan dalam konsep ruang publik dan diskursus Habermas. Bahkan lebih jauh lagi dijabarkannya dalam konsep legitimasi, yang jika dijalankan secara praktis di dalam ruang publik dalam bentuk diskursus, akan menjadi sebuah kekuatan legitimasi hukum dalam real politik.

"Menjadi lebih responsif terhadap kebutuhan-kebutuhan sosial" adalah visi yang kita butuhkan bagi hukum nasional dari pandangan hukum responsif. Dengan memandang lebih baik kepada fakta-fakta sosial dan berusaha membenahi cara hukum berjalan. Satjipto Rahardjo menilai, bahwa apa yang disinggung Nonet dan Selznick konsep fleksibilitas interpretasi yang memandang peraturan-peraturan sebagai cara hukum berlaku terhadap masalah dan konteks-konteks spesifik, dan berusaha mengidentifikasikan nilai-nilai yang dipertaruhkan dalam perlindungan yang bersifat prosedural, dalam pemahaman Nonet dan Selznick adalah suatu kritik terhadap doktrin *due process od law*.[46] Pada satu sisi memang dibutuhkan kritik terhadap kurang fleksibelnya *due process* terhadap dinamisnya perubahan di masyarakat, akan tetapi *due process* merupakan kebutuhan dalam meraih tujuan-tujuan hukum di dalam masyarakat.

Luasnya ranah hukum dalam upaya perubahan masyarakat (*social engineering* dan *social control*) memerlukan kerangka kuat dalam cakupan luas, dengan generalisasi tujuan inilah yang diperlukan untuk menciptakan fleksibilitas. Nonet dan Selznick mendorong untuk tetap adanya proses saling

[45] *Ibid*., hal. 124-125.

[46] Satjipto Rahardjo, *Hukum Progesif*, (Yogyakarta: Genta, 2009), hal. 7. Lihat juga: Nonet, *op.cit.*, hal. 90.

mempengaruhi antara aturan dan asas, karena dalam proses inilah suatu sumber perubahan dibangun ke dalam tatanan hukum. Ketika lingkungan berubah, peraturan-peraturan harus ditata ulang, bukan untuk memenuhi kebutuhan kebijakan namun juga untuk melindungi otoritas peraturan itu sendiri dan integritasnya ketika diaplikasikan.[47]

Konsep tentang kesinambungan antara aturan dan asas untuk saling mengkoreksi memiliki kesan *auto-reference*, seperti dalam konsep autopoiesisnya Niklas Luhman, dimana koreksi selalu ada dan berjalan sebagai mekanisme organis. Kiranya bentuk yang demikianlah yang akan menjadikan penegakan hukum senantiasa responsif terhadap perubahan-perubahan dalam ruang publik (sosial).

Pemahaman atas responsifitas khas Nonet dan Selznick sekiranya tidak akan cukup dilakukan dengan pengamatan atas fenomena-fenomena perubahan dalam ruang sosial, karena pada kenyataannya saat hukum berusaha dijalankan terjadi keadaan lembaga penegak hukum *vis a vis* struktur sosial, dan lembaga hukum itu juga merupakan bagian dari lingkup sosial dan memberi peran sosial. Di sinilah pemahaman karakter serta pengenalan psikologis atas strata-strata sosial yang dihadapi diperlukan. Hal ini pernah disinggung oleh John Rawls saat membahas institusi dan keadilan formal. Rawls bermaksud membedakan antara aturan tunggal (atau sekelompok aturan), institusi (atau bagian utamanya), dengan struktur dasar sistem sosial secara keseluruhan. Alasan untuk melakukan hal ini adalah karena satu atau beberapa aturan penataan bisa menjadi tidak adil tanpa institusinya menjadi tidak adil. Tidak hanya ada kemungkinan bahwa aturan dan lembaga tunggal tidak dengan sendirinya penting namun bahwa dalam struktur institusi atau sistem sosial satu ketidakadilan menggantikan ketidakadilan yang lain.[48]

Alih-alih berusaha menyingkir dari bentuk hukum otonom dan bergerak menuju hukum yang responsif, rasionalitas hukum terhadap kenyataan sosial

[47] *Ibid*., hal. 92.

[48] John Rawls, *Teori Keadilan* (*A Theory of Justice*), diterjemahkan oleh Uzair Fauzan dan Heru Prasetyo, cet. Pertama, (Yogyakarta: Pustaka Pelajar, 2006), hal. 68.

semestinya terus-menerus diasah. Hukum sebagai alat mencapai keadilan sosial, maka di dalamnya akan menyimpan harapan-harapan yang terus diupayakan, dan itu kemudian didefinisikan sebagai indeks nilai sosial primer yang diharapkan dan masyarakat mampu menilainya 'memang bisa diharapkan'. Rawls menyimpulkan, prospek seseorang diperbaiki ketika ia dapat mengantisipasi sekumpulan nilai tersebut.[49] Nilai antisipatif sosial terhadap nilai yang diusung oleh hukum inilah wujud rasionalitas hukum terhadap realitas sosial, yang bisa kita kembalikan kepada pandangan Nonet dan Selznick tentang perlunya proses saling mempengaruhi antara asas dan peraturan.

Hukum dalam memandang realitas perubahan sosial memerlukan responsifitas, terlebih saat menyadari dunia maya berkembang teramat pesat. Pemahaman tentang karakter sosial dan ruang publik mayantara diperlukan. Di lain sisi peranan publik, yang memiliki kesadaran hukum dan telah lebih dahulu 'hadir' dalam ruang publik maya, diperlukan dalam memahami lebih baik situasi di dalamnya. Dalam keadaan yang demikianlah bentuk masyarakat komunikatif *a la* Habermas memiliki peran dalam pembenahan hukum, sekaligus menjadikannya bergerak dari karakter otonom kepada responsif.

## 2.3 Pengantar Kepada Sosiologi Hukum

Dragan Milovanovich memberikan pengantar kepada dasar sosiologi hukum dengan mengawalinya menggunakan pemikiran tiga tokoh sosiologi klasik, yakni Emile Durkheim, Max Weber, dan Karl Marx, tiga tokoh besar dalam sosiologi yang darinya oleh Dragan disarikan pola-pola masyarakat dalam mengatur dan mengembangkan dirinya, kemudian dilanjutkan beberapa perspektif kontemporer dalam kajian sosiologi hukum.

Beberapa kajian sosiologi hukum justru seringkali ditemukan terselip dalam berbagai jurnal atau naskah bidang ilmu sosiologi *an sich*, jika dibandingkan dengan publikasi kajiannya di dalam berbagai studi mengenai hukum secara langsung. Sebagian juga menunjukkan kuatnya dasar pemikiran

[49] *Ibid*., hal. 113.

dalam memahami masyarakat secara langsung, memahami berbagai aspek yang tumbuh dari diri masyarakat itu sendiri, atau pun juga berbagai tekanan dari luar mereka yang mampu memberikan pola sosial dan memberikan keteraturan. Semestinya hukum sebagai salah satu cabang ilmu sosial, mampu menyatu dan beradaptasi secara lebih organik dengan masyarakat.

Para pejabat di bidang hukum seringkali berkutat dengan kajian jurisprudensi, menekankan pengetahuan yang didapatkan dari pendidikan hukum yang sudah ditempuhnya dan menerapkan penegakan hukum itu dalam kehidupan sehari-hari, dengan berbekal kemampuan menjelaskan dua struktur, yang oleh Dragan disebut dengan *morphological structure* dan *syntatical structure*. Penerapan *morphological structure* adalah dengan mengerti tiap penjelasan yang disampaikan oleh undang-undang tentang definisi setiap istilahnya. Sedangkan kemampuan *syntatical structure* adalah kemampuan menerapkan metode yang benar secara konstruksi linier dari kata-kata dalam sebuah peraturan perundang-undangan ke dalam bentuk narasi maupun teks.[50]

Saat para akademisi dalam bidang jurisprudensi mengolah berbagai perdebatan dan mengembangkannya dengan kemampuan analisis hukum doktrinalnya, dan terus berdebat mengenai penjelasan itu di dalam mengembangkan teorinya. Di sisi lain para sosiolog hukum lebih berargumentasi dan menerapkan berbagai teori sosial, peraturan sosial, dan hal-hal yang membangun keduanya sebagai lahan untuk mengajukan konsep mereka tentang hukum dan kritisisme di dalamnya.

Pada bagian pembuka, Dragan menjelaskan tentang kajian sosiologi hukum yang menurutnya meliputi:[51]

*(1) The evolution, stabilization, function, and justification of forms of social control;*

*(2) The forms of legal thought and reasoning as they relate to a particular political economic order;*

[50] Dragan Milovanovic, *A Primer in the Sociology of Law*, (New York: Harrow and Heston:, 1994), hal. 3.

[51] *Ibid*., hal. 3-4.

(3) *The legitimation principles and the effects that evolve with them;*
(4) *The "causes" of the development of the form of social control and staff of specialists that are its promoters;*
(5) *The transmission of "correct" methods of legal reasoning;*
(6) *The creation of the juridic subject with formal, abstract and universal rights;*
(7) *The evolution of the juridico-linguistic coordinate system (legal discourse) in use and its nexus with the political economic sphere; and*
(8) *The degree of freedom and coercion existing in the form of law.*

Selanjutnya Dragan menjelaskan bahwa, semua definisi di atas adalah lebih dari sekedar mengambil kebijakan untuk mengatur, bentuk-bentuk hukum, hak-hak dan pernyataan-pernyataan yang menjabarkannya kepada subjek hukum sebagai sesuatu yang terberi (*given*), pendekatan ini lebih menguji evolusi dari bentuk-bentuk tersebut dan bagaimana itu semua menjadi faktor dominan dalam pemikiran hukum dan dalam resolusi konflik dalam masyarakat.[52]

Kita dapat menjabarkan beberapa ide itu dalam upaya untuk memahami masyarakat kemudian mengambil intisari pola yang ada untuk membantu pembentukan hukum, meregulasi masyarakat. Regulasi yang diformulasikan dari pola *native*-nya yang telah teruji secara nyata selama usia masyarakat tersebut, yang terus-menerus berbenturan dengan tantangan di setiap waktu. Sekaligus menghindari stagnasi hukum dengan perangkat analisis yang fleksibel terhadap perubahan sosial.

Dalam proses adaptasi masyarakat, hukum formal yang terkodifikasi semakin dibutuhkan saat suatu masyarakat menemui kemajemukannya. Kodifikasi mampu menyeragamkan aturan di dalam masyarakat yang kompleks, dengan tujuan agar lebih mudah mengorganisasi suatu masyarakat untuk ketertiban bersama. Dengan penjelasan Steven Vago, dalam konteks dan tujuan yang demikian, dapat dipahami bahwa peran hukum formal merupakan cara untuk memelihara aturan dan menawarkan pola kebiasaan masyarakat sehingga dapat diprediksi (*predictability of behavior*). *Predictability of behavior* ini

[52] *Ibid*., hal. 4.

muncul dari keseragaman aturan dan ketertiban, dan Vago menjadikannya sebagai pengertian sederhana dari "social control", dan hukum hanya salah satu dari sekian banyak bentuk kontrol sosial.

Vago memberikan penjelasan peran sosial hukum ke dalam tiga tema, yaitu: social control, conflict resolution, dan law as social change. Studi atas upaya mengatur masyarakat cyber dan menjalankan hukum di dalamnya, dengan penekanan pada peran serta masyarakat mayantara memerlukan penjabaran ketiganya untuk menjelaskan.

### 2.3.1 Hukum Sebagai *Social Control*

Hukum sebagai 'Kontrol Sosial' berarti hukum dapat mengendalikan masyarakat dan melakukan pengendalian terhadap kejahatan dan potensinya di dalamnya, baik dalam perspektif para pelaku sosial secara individual maupun secara kolektif dalam kesatuan sosial, baik dari dalam maupun dari luar masyarakat. Sebagaimana dua proses dasar kontrol sosial adalah internalisasi dan juga dengan tekanan dari luar masyarakat.

Kita telah mendapat pelajaran yang terukur dari Weber, Durkheim, dan Marx dalam perkuliahan, dalam kaitannya dengan hukum sebagai kontrol sosial. Dalam karya Steven Vago (1981) yang di dalamnya membahas tentang "Law as Social Control" serta pemikiran Weber dan Durkheim dalam Dragan Milovanivic (1994)—yang dalam membahas Weber menyinggung kedekatannya dengan Parson. Yang selanjutnya coba dikaitkan dengan pemikiran Niklas Luhmann yang memberi masukan atau sebuah kebaruan bagi teori sistem Parson, yang dirujukkan dari beberapa literatur sosiologi dan filsafat.

Penjelasan dari Steven Vago (1981), tentang Law and Social Control. Dalam tulisan tersebut Vago seakan memisahkan antara 'law' dan 'social control' dan menghubungkannya dengan kata 'and', ia tidak membahasakannya sebagai dua dalam satu kesatuan, tetapi Vago mengesankan seakan keduanya terpisah.

Sangat awal dari bab tersebut Vago menjelaskan, kontrol sosial merujuk pada cara para anggota sebuah masyarakat memelihara aturan dan meningkatkan kemungkinan untuk memperkirakan suatu tindakan.[53] Vago menjelaskan bahwa terdapat banyak bentuk kontrol sosial, dan hukum adalah salah satunya. Oleh karenanya ia menekankan pembahasan pada situasi ketika bentuk-bentuk mekanisme kontrol lain tidak dapat berjalan efektif atau memang tidak ada, dan hukum mengambil kesempatannya berperan sebagai kontrol sosial. Selanjutnya untuk memberikan penjelasan yang lebih baik dengan pemilahan kontrol sosial ke dalam dua bagian, yakni kontrol sosial informal dan kontrol sosial formal. Hal ini sengaja dilakukan Vago untuk menghindari *overlapping* antara keduanya, dan untuk membantu melakukan analisis secara lebih efektif.

#### 2.3.1.1 Kontrol Sosial Informal

> Kontrol sosial secara informal dicontohkan dengan fungsi-fungsi yang berjalan dalam cara kerakyatan (norma-norma yang dimunculkan dalam praktik keseharian sebagaimana mode pakaian tertentu, etiket, dan penggunaan bahasa) dan adat-istiadat (norma-norma sosial berasosiasi dengan perasaan-perasaan intens tentang benar atau salah dan aturan tertentu tentang tingkah laku yang secara sederhana tidak akan mengganggu, sebagai contoh, incest). Kontrol informal tersebut terdiri atas teknik-teknik yang oleh individu yang mengetahui satu sama lain dalam dasar keseuaian personal akan memuji kepada mereka yang mentaati harapan bersama dan menunjukkan ketidaknyamanan kepada mereka yang tidak mentaatinya.[54]
>
> Dengan demikian kontrol sosial yang sifatnya informal selalu merupakan bagian dari masyarakat dengan ciri keeratan sosial yang oleh Durkheim dikatakan memiliki *mechanical*

[53] Steven Vago, *Law and Society*, (New Jersey: Prentice Hall, 1991), hal. 135.
[54] *Ibid*, hal. 136

*solidarity*, yang oleh Dragan Milovanovic dikatakan sebagai tipe normal dalam masyarakat yang pemilahan tingkat pekerjanya masih sangat kecil, dan "perekat" ikatan sosial dalam kesamaan dan kesetaraan masih kuat.[55] Tetapi konteks kontrol sosial informal tidaklah hanya ada dalam bentuk masyarakat dengan mechanical solidarity dengan diferensiasi bidang pekerjaan yang masih minim sebagaimana dijelaskan Durkheim, nilai-nilai tentang solidaritas dan kesepakatan dalam masyarakat majemuk dengan konsep hukum tidak tertulisnya juga selalu memiliki potensi informal social controls. Yaitu dengan maksud menunjuk kepada masyarakat *cyber* yang memiliki diferensiasi tinggi, yang dalam tataran tertentu mereka memiliki mechanical solidarity.

Mekanisme informal dari kontrol sosial dirancang untuk lebih efektif dalam kelompok dan masyarakat dimana relasi bersifat *face to face* dan intimasi, dimana pembagian pekerjaan relatif sederhana. Selanjutnya, intensional interaksi *face to face* dalam masyarakat tertentu menciptakan konsensus moral yang dikenal oleh seluruh anggotanya; juga membawa tindakan menyimpang secara cepat menjadi perhatian setiap orang.[56] Konsep Durkheim ini perlu mendapatkan sedikit kritik pada pembahasan selanjutnya.

#### 2.3.1.2 Kontrol Sosial Formal

Sebagaimana konsep Durkheim yang memilah solidaritas ke dalam dua partisi, Vago pun memiliki kecenderungan yang sama. Ia menjelaskan bahwa konrol sosial formal biasanya merupakan karakteristik dari masyarakat yang lebih kompleks dengan pembagian tingkat pekerjaan yang lebih besar, heterogenitas populasi, dan sub-grup dengan nilai-nilai terkompetensi dengan

[55] Milovanovic, *op.cit.*, hal. 25
[56] Steven Vago, *Loc.Cit.*

bentuk berbeda dalam adat-istiadat dan ideologi. Kontrol yang bersifat formal muncul ketika kontrol informal tidak lagi sesuai diterapkan untuk memelihara kenyamanan pada norma-norma tertentu dan dicirikan dengan sistem yang mengenal spesialisasi agen-agen sosialnya dan dengan teknik-teknik yang standar.[57]

Seperti telah dijelaskan bahwa pengertian formal adalah saat yang informal tidak lagi mampu hadir dan memberikan fungsi kontrolnya. Maka formal selalu timbul dari kebutuhan akan keteraturan dan kontrol yang membuat segalanya kepada keadaan sebagaimana kondisi informal. Seperti menjelaskan bagaimana Durkheim berupaya mengganti secara perlahan 'solidaritas mekanis' sederhana dengan 'solidaritas organik' yang lebih kompleks, yakni solidaritas komplementer, berkat semakin tegasnya pembagian kerja dalam masyarakat.[58] Jika Durkheim berusaha menjaga tetap adanya solidaritas, maka demikian pula peran sosial kontrol selalu diupayakan tetap ada, karena eksistensinya yang menjadi urgensi dan kebutuhan sosial.

Formal dijelaskan sebagai kebutuhan yang tumbuh sebagai karena ketiadaan informal. Begitu pula hukum, informal mengenal formulasi kontrol pada hukum tak tertulis, sedangkan format formal adalah mulai dikenalnya konsep 'standarisasi' atau dalam hukum dikenallah hukum yang mengenal prinsip 'legalitas' atau ketertulisan. Sehingga logika kebenaran dan kesalahan, kebaikan dan kejahatan, yang sesuai definisi bersama, dituangkan ke dalam perundang-undangan untuk dijadikan sebagai alat kontrol sosial.

### 2.3.2 Hukum Sebagai Conflict Resolution

[57] Steven Vago, *op. cit.*, hal. 139
[58] Peter Burke, *Sejarah dan Teori Sosial*, (Jakarta: Yayasan Obor Indonesia, 2001), hal. 198

Steven Vago memberikan abstraksi menarik di awal pembahasannya tentang *Law as Method of Conflict Resolution*. Ia mengutip dari Kriesberg dan Aubert.

> *At every level in society conflict is ubiquitous. Sociologists consider social conflict as a relationship between two or more parties who (or whose representatives) believe they have incompatible goals* (Kriesberg, 1973:17). *This relationship is usually characterized by some overt signs of antagonism* (Aubert, 1963:26).[59]

Kutipan tersebut menggambarkan bahwa dalam segala tingkatan sosial senantiasa berpotensi terdapatnya konflik yang serupa. Di dalam pemikiran para sosiolog, sebagaimana disampaikan Kriesberg, menyatakan bahwa konflik adalah hubungan antara dua atau lebih kelompok yang yakin bahwa mereka memiliki tujuan-tujuan yang tidak berkesesuaian. Vago lalu melanjutkan bahwa, cakupan konflik dapat terbentang dari permasalahan keluarga hingga perang besar. Yang melibatkan berbagai tingkat kelompok, individu, grup, maupun organisasi.[60]

Seiring dengan pertumbuhan sosial, akan juga meningkatnya kemampuan dari mekanisme hukum untuk melakukan resolusi konflik, dan penciptaan berbagai bentuk pemulihan keadaan dan hak-hak yang dapat diberikan secara legal. Pengadilan memberikan forum untuk melakukan penyelesaian berbagai bentuk perselisihan baik privat maupun publik. Untuk menunjukkan kemampuan dari peran layanan-layanan pengadilan, setidaknya para penuntut perkara ke persidangan harus mampu untuk menunjukkan sisi rasa keadilan dalam perkaranya dan mampu mempertahankan diri.[61]

Sebagaimana layaknya metode yang berfungsi menjembatani antara teori dan kenyataan, hukum adalah metode untuk menyelesaikan berbagai konflik dalam masyarakat. Berbagai idealisme tentang keadilan yang ada di dalam masyarakat dan berbagai nilai-nilai di dalamnya, diberikan ruang

---

[59] Steven Vago, *op.cit.*, hal. 174.
[60] *Ibid*., hal. 174.
[61] *Ibid*., hal. 209.

oleh pengadilan bagi mereka yang menuntut keadilan atas berbagai perselisihan yang terjadi di dalam masyarakat dalam berbagai tingkatan sosial.

Hukum tidak sekedar pasif menjadi sebuah metode yang semacam monolog terhadap realitas sosial, hukum berkembang seiring dengan pertumbuhan sosial dan perselisihan yang berseliweran di dalamnya. Dan Vago menekankan, setidaknya ada prasyarat, bahwa kemampuan untuk menuntut rasa keadilan dan kemampuan untuk mempertahankannya di muka pengadilan adalah utama. Dan dengan cara itu pulalah hukum terus berkembang, dipertahankan, disanggah, dan terus beradaptasi untuk mampu menyelesaikan konflik dalam masyarakat.

### 2.3.3 Hukum sebagai Sarana Social Engineering

Perubahan sosial berarti modifikasi dalam cara orang bekerja, menyokong keluarga, mendidik anak mereka, mengatur diri mereka sendiri, dan mencari arti sesungguhnya dalam kehidupan. Hal ini juga berarti sebuah restrukturasi cara-cara mendasar bagi orang dalam hubungan kemasyarakatan satu sama lain dengan perhatian-perhatian atas kepemerintahan, ekonomi, pendidikan, agama, kehidupan keluarga, rekreasi, bahasa, dan berbagai aktifitas lainnya.[62]

Dalam sisi pandang ekstrim, melihat bahwa hukum adalah sebuah variabel yang tergantung dengan yang lainnya, ditentukan dan dibentuk dengan nilai-nilai kekinian dan opini-opini masyarakat. Merujuk pada hal ini, perubahan-perubahan hukum akan menjadi tidak mungkin meskipun diawali dengan perubahan sosial; reformasi hukum tidak dapat melakukan apapun selain mengkodifikasi kebiasaan. Ini jelasnya tidak demikian, dan mengacuhkan kenyataan bahwa melalui sejarah institusi-institusi hukum telah mulai menemukan dengan cara "memiliki sebuah aturan tertentu, meskipun kurang dimengerti, sebagai instrumen-instrumen yang dimatikan,

[62] *Ibid*., hal. 215.

pengawasan, atau dengan kata lain mengatur fakta atau langkang dari perubahan sosial".[63]

Hukum menciptakan norma-norma, bahan mentah bagi kontrol sosial. Kekuatan-kekuatan sosial melontarkan tekanan-tekanan; tuntutan-tuntutan ini "membentuk" hukum, namun institusi-institusi yang ada pada sistem hukum menuai tuntutan-tuntutan itu, menghablurkan (mengkristalkan) dan mengubahnya menjadi peraturan, prinsip, dan instruksi-instruksi bagi pegawai negeri dan penduduk pada umumnya. Dalam menjalankan hal ini, sistem hukum bisa bertindak sebagai instrumen perubahan yang tertata, rekayasa sosial (social engineering). Contoh yang paling jelas adalah fungsi legislatif. Pengadilan-pengadilan juga menciptakan peraturan – khususnya dalam sistem-sistem hukum umum, dan ada lusinan dewan, lembaga, komisi, dll. Dengan kekuasaan membuat-peraturan dalam pemerintahan modern, kebanyakan di antara mereka memiliki kekuasaan untuk mengarahkan dan mengontrol.[64]

## 2.4 Publik Mayantara

### 2.4.1 Pengertian Publik

Publik senantiasa berkaitan dengan 'politik' dan 'demokrasi'. Makna kata 'publik' dapat kita telusuri dalam sejarah Barat, di zaman Yunani dan Romawi Kuno. Konsep 'publik' muncul bersamaan dengan kemunculan *polis* (negara kota) Yunani secara evolusioner. Kata publik yang kita pakai dalam Bahasa Indonesia berasal dari bahasa Latin, '*publicus'*. Dalam masyarakat Romawi, kata *publicus* memiliki dua arti: Pertama, milik rakyat sebagai satuan politis atau milik negara; dan kedua, sesuai dengan rakyat sebagai seluruh penduduk atau—kata lain untuk itu adalah—'umum'.[65]

---

[63] *Ibid*., hal. 216.

[64] Lawrence M. Friedman, *Sistem Hukum: Perspektif Ilmu Sosial* (*The Legal System: A Social Science Perspective*), diterjemahkan oleh M. Khozim, cet. Kedua, (Bandung: Nusamedia, 2009), hal. 21.

[65] F. Budi Hardiman, ed., *Ruang Publik*, (Yogyakarta: Kanisius, 2010), hal. 3.

Kata-kata yang berkaitan dengan '*public'* mengacu pada suatu "ruang sosial" yang bisa dilibati oleh semua orang. Ruang itu di zaman Yunani Romawi terletak di luar rumah, yaitu di jalan-jalan, dan di alun-alun, di arena teater. Sementara itu 'ruang' yang berada di bawah kekuasaan *pater familias* (ayah) disebut *privatus*, maka kemudian tidak hanya ada *res publica* (hal publik), melainkan juga *res privata* (hal privat). Akan tetapi distingsi eksplisit tentang 'privat' dan 'publik' adalah gagasan modern yang belum berkembang dalam masyarakat kuno. Kita dapat menyimpulkan bahwa dalam kata *publicus* atau kata yang sekarang kita pakai dalam bahasa Indonesia, yaitu *publik*, dalam artinya yang paling tua sudah mengacu pada 'umum', 'terbuka', 'diumumkan' dan seterusnya. Di puncak Abad Pertengahan bahkan kata itu diperluas sebagai konsep filosofis, dengan menyebut manusia sebagai *creatura publica* (makhluk publik). Dengan demikian kata 'publik' yang kita pakai merupakan warisan Eropa untuk asas politis modern yang sekarang berlaku di manapun, termasuk negara kita, jika kita menyebutnya republik (hal publik) Indonesia.[66]

Kita menyebut peristiwa-peristiwa dan kejadian-kejadian tertentu sebagai peristiwa atau kejadian bersifat 'publik' jika terbuka bagi semua pihak. Berbeda dengan istilah 'bangunan publik'. 'Bangunan publik' apa pun tidak mesti terbuka lebar sebagai tempat publik, 'bangunan publik' bisa saja hanya sebuah bangunan bagi suatu institusi Negara. Namun dalam keadaan yang demikian pun dia sudah masuk dalam kategori 'publik', karena Negara adalah pengemban 'otoritas publik'.[67]

Pengertian 'publik' yang dijelaskan oleh Budi Hardiman telah mampu menjelaskan makna dasarnya secara historis. Demikianlah yang akan kita tautkan dalam pembahasan mengenai masyarakat mayantara,

---

[66] *Ibid*., hal. 4-5.

[67] Jurgen Habermas, *Ruang Publik: Sebuah Kajian tentang Kategori Masyarakat Borjuis* (*Public Sphere: An Inquiry into a Category of Borgeois Society*), diterjemahkan oleh Yudi Santoso, (Yogyakarta: Kreasi Wacana, 2010), hal. 3.

sehingga publik akan melingkupi masyarakat dan ruang di sekelilingnya dimana setiap orang dapat menyaksikan apa saja yang terjadi dalam ruang publik tersebut baik secara langsung ataupun tidak langsung, misalkan dengan melalui perantara, selama itu tidak melampaui batas-batas privasi.

### 2.4.2 Konsep Publik Mayantara

Dalam Neuromancer,[68] sebuah novel fiksi fenomenal karya William Gibson yang diterbitkan tahun 1982 menceritakan tentang sebuah dunia di masa depan, tentang rumitnya kehidupan dan bagaimana tekanan serta kontrol hidup telah sedemikian ketatnya. Di dalam Neuromancer, Gibson menuturkan tentang bagaimana kehidupan masa depan dengan memberikan pemaknaan-pemaknaan baru terhadap bentuk aktifitas publik di masa itu, Gibson secara menarik memakai berbagai konotasi simbolis aktifitas internet ke dalam peristilahan umum dalam kehidupan riil di masa depan. Novel Gibson tersebut memberikan pengertian baru ke dalam kehidupan modern, terutama kehidupan kita yang semakin terintegrasi dengan internet. Di dalam novel ini Gibson memperkenalkan peristilahan baru yang kini populer, *cyberlife*.

Dengan memperhatikan kompleksitas dan usaha manusia untuk berontak dari ancaman sistem hukum yang mencekik kehidupan, novel ini mengingatkan kita pada karya George Orwell, 1984.

Pemakaian istilah ‘mayantara’ sebagaimana di dalam buku “Tindak Pidana Mayantara” (Barda Nawawi: 2006) merupakan terjemahan kata *cyber* dalam bahasa Inggris. Prof. Barda sendiri menerjemahkan “*Cybercrime”* sebagai “Tindak Pidana Mayantara”, arti kata *crime* sendiri adalah kejahatan, yang secara khusus dalam konteks tujuan

[68] Sebuah novel yang memenangkan beberapa penghargaan, Hugo Award, Nebula Award, The Phillip K. Dick Memorial Award, dan SF Chronical Award, karya William Gibson, (William Gibson, *Neuromancer* (*Neuromancer*), diterjemahkan oleh Eman Prihatmo, (Yogyakarta: Jalasutra, 2010)).

pembahasannya, dalam *cybercrime*, kata *crime* diterjemahkan sebagai tindak pidana.[69]

Dalam pemakaiannya sebagaimana disebutkan dalam Oxford Dictionary, kata *cyber* secara umum merupakan prefiks atau kata awalan yang bergandengan dengan kata-kata tertentu untuk menciptakan pengertian baru dengan esensi makna yang serupa, pengertian baru tersebut menarik makna dasarnya menjadi makna yang bertalian langsung dengan teknologi komunikasi yang terintegrasi atau terinterkoneksi, secara khusus adalah internet.

Era Web 2.0 yang ditandai dengan kemampuan teknologi internet dalam memberikan tanggapan kepada pengguna, dengan kata lain, situs-situs internet dalam era web 2.0 memiliki kecerdasan buatan (*artificial intelegence*) untuk berinteraksi dengan para penggunanya. Dengan kian dinamisnya tampilan suatu situs internet akan memberikan kemudahan setiap orang untuk mengaksesnya, dan teknologi internet tidak lagi seperti masa-masa statisnya, saat kita hanya membuka situs seperti kita membuka sebuah katalog statis. Kini bahkan era web 3.0 telah menanti dengan konsep *semantic web*-nya, serta era *cloud computing* yang mampu menangani data yang lebih besar dari sebelumnya sudah mulai berjalan, dan dengan demikian pemrosesan lebih efektif dan menghemat waktu.

---

[69] Dalam Oxford advanced Learner's Dictionary of Current English menjabarkan makna '*crime*' sebagai *"1. offence for which there is severe punishment by law; [U] such offences collectively; serious law-breaking… 2. Foolish or wrong act, not necessary in againts the law… 3. (in the army) serious breaking of the regulations (not necessarily an offence against civil law)…"* maka pengertian *crime* adalah kejahatan pada umumnya, namun dalam pembahasan tema tentang tindak pidana, *crime* di sini adalah tindak pidana itu sendiri secara khusus. AS Hornby, *Oxford Advanced Learner's Dictionary of Current English*, (Oxford: Oxford University Press, 1987), hal. 204. Dalam Oxford Pocket Dictionary, menjelaskan makna *cyber* sebagai prefix atau awalan terhadap kata-kata yang digandengkan maknanya dengan kata ini, sehingga di dalam kamus tersebut dituliskan "*cyber-*" (dengan tanda sambung), yang bermakna: "prefix *connected with electronic communication networks, esp. the internet"*, atau sebagai awalan yang berhubungan dengan komunikasi elektronis dalam jaringan, yang secara khusus adalah internet. Kata ini bisa diikatkan dengan kata-kata umum lainnya dan menjadi seperti: *cybercafe, cyberspace, cybersquatting*, dan kata-kata bentukan lainnya yang berhubungan dengan kata *cyber* itu sendiri, dalam adaptasinya terhadap kebaruan kajian kultural dalam masyarakat, khususnya lingkungan sosial yang bertalian erat dengan dunia *cyber*. Victoria Bull, ed., *Oxford Learner's Pocket Dictionary*, 4th edition, (Oxford: Oxford University Press, 2009), hal. 111.

Dengan semakin meningkatnya kinerja situs-situs dunia maya, maka kemudahan untuk bersosialisasi dengan para pengguna lain juga semakin mudah. Dari sini mulailah berkembang berbagai bentuk aplikasi komunitas untuk memudahkan setiap orang bersosialisasi satu sama lain. Kita kemudian mengenal adanya twitter.com. facebook.com, plurk.com, tumblr.com, dan lain sebagainya. Orang-orang mulai berkumpul dan bertemu di dunia maya, menyelesaikan berbagai pekerjaan, menggantikan sosialisasi dalam ruang-ruang publik lama yang mengandalkan kemampuan dialog oral dan pertemuan.

Kata 'publik' merupakan ruang di luar privat, dan di dalam *cyberspace* (mayantara) memiliki ruang-ruang publiknya sendiri. Sebagaimana dijelaskan oleh Budi Hardiman bahwa publik bukanlah bermakna sekumpulan orang tetapi ia lebih mengacu pada 'umum', 'terbuka', 'diumumkan' dan seterusnya, maka makna 'publik mayantara' adalah ruang di mana individu-individu terlibat di dalamnya dan begitu juga sistem yang menjadikannya terkumpul atau bisa dikatakan sebagai diferensiasi dari privat itu sendiri secara *an sich*. Sehingga publik mayantara atau publik *cyber space* merupakan ruang dimana seluruh aktivitas tiap individu di dalam sistem *cyber* itu bertemu berinteraksi di luar keadaan-keadaan privatnya.

Bisa dikatakan bahwa pada awalnya semua yang berada dalam jejaring dunia maya (internet) adalah bersifat publik. Namun kemudian karena semakin meluasnya jaringan dan kapasitas di dalamnya, meluas pula pemanfaatannya, kemudian muncul pemilahan ruang-ruang yang memberikan sekat-sekat di dalamnya menurut kebutuhan yang bermacam-macam dan terus berkembang. Munculnya sekat-sekat tersebut memberikan batasan akses kepada setiap pengguna yang berlalu-lalang di dalamnya, sehingga memunculkan akun-akun dengan *password* dan *user name log-in*. Kemudian dunia maya (*cyberworld*) mulai muncul banyak aturan seperti dalam *The Matrix*.

Circa 2199, seluruh dunia dikuasai oleh *The Machine*, mesin ini menjejalkan sinyal berisi informasi lingkungan maya yang disebut Sang Matriks ke dalam hampir seluruh warga bumi. Warga bumi tidak menyadari kemayaan pengalaman mereka. Neo dan Morpheus, dua tokoh dalam cerita ini berusaha melawan Sang Matriks agar manusia kembali ke dunia nyata.

Di dalam Neuromancer pun digambarkan bagaimana Case, sang tokoh utama, adalah seorang jagoan dalam hal membobol satu ruangan ke dalam ruangan yang lain, menembus *firewall* dan memasuki gudang data.[70] Case pun digambarkan sebagai seorang pemuda yang terkadang larut dalam halusinasi mayanya dan melakukan pembobolan *firewall*, sedangkan kisah The Matrix adalah tentang bagaimana melawan halusinasi itu dan mengembalikan kesadaran manusia kepada kesadaran eksistensialnya dalam dunia nyata.

Ruang publik dalam mayantara adalah ruang dimana arus informasi begitu bebas dan mudah didapatkan. Jika dalam publik politis merupakan tempat menyuarakan aspirasinya kepada pemilik otoritas, tetapi di dalam ruang maya kemudahan dan kebebasan mendapatkan informasi yang melampaui lokalitas, seringkali membawa orang ke tumpukan informasi yang tidak berhubungan langsung dengan keprihatinannya. Akibatnya, publik terlibat dalam percakapan semu, dimana orang hanya sekadar meneruskan kata-kata asal bisa menjadi bagian publik.[71]

Dan demikianlah kiranya kenikmatan manusia dalam mengamini tiap *news-feeds,*[72] kemudian menjadi halusinasi bagi dirinya sendiri. Orang kemudian larut dalam hal yang dialami orang lain, keprihatinan yang bukan

---

[70] Gibson, *op.cit.*, hal. 7.

[71] Karlina Supelli, "Ruang Publik Dunia Maya," dalam F. Budi Hardiman, ed., *Ruang Publik: Melacak "Partisipasi Demokratis" dari Polis sampai Cyberspace*, (Yogyakarta: Kanisius, 2010), hal. 343.

[72] Istilah dalam internet untuk 'arus berita', walau *feed* secara literal berarti makanan. *News-feed* semisal dalam Facebook adalah tampilan tentang berbagai status dan aktifitas *friends* dan *groups*, atau berbagai berita terkini dari *pages* yang kita ikuti.

miliknya, atau solidaritas tanpa intimitas.[73] Yang oleh Martin Heidegger, dengan filsafat eksistensialisnya, dikatakan dengan *Mitdasein*, atau mengada (*dasein*) di tengah (*mit*) orang-orang. Ia memahami *mit* dalam konteks eksistensialis, sehingga keberadaan kita bersama orang-orang bukanlah kebetulan akan tetapi merupakan cara kita mengada dalam hidup. Tetapi ternyata itu menjadikan kita larut dalam keseharian yang lain, dan keadaan itu justru habis-habisan melarutkan kenyataan diri sendiri ke dalam orang-orang.[74] Dalam eksistensialisme Heidegger, situasi ini menjadikan kita tidak lagi otentik. Dan di dunia maya bukan sekedar menjadikan kita terlalu larut dalam pertukaran makna, lebih dari itu kita justru larut dalam keadaan orang lain.

Demikianlah ruang publik dalam dunia maya, kekuatan publik selalu larut dalam arus utama tema yang mengalir di dalamnya, yang cenderung melupakan manusia akan kebutuhan nyatanya. Terlalu banyak keprihatinan yang muncul di dalamnya, dan bukan dari diri sendiri. Di sinilah pentingnya mengembalikan kesadaran publik akan berbagai bahaya di dalamnya, kemuslihatan (kriminalitas) yang mengintai di keramaian mayantara, sebagaimana Neo bersama Morpheus dan Trinity berusaha mengembalikan kesadaran manusia dari halusinasi *Matrix*. Kesadaran tersebut sekiranya dapat dibangun dengan mengurai bentukan sosial dan penguasaan atas 'ruang' dari publik itu sendiri, yaitu mereka yang memiliki kemampuan utama di dalamnya, dalam memahami karakter ruang. Dengan demikian akan membantu peran hukum dalam mengelola 'ruang' dalam

[73] Solidaritas Tanpa Intimitas merupakan pembahasan B. Hari Juliawan yang menarik dalam kelemahan konsep demokrasi Habermas yang mengharapkan setiap anggota publik berada dalam posisi yang sama, sedangkan pada kenyataannya setiap manusia dalam dunia yang penuh hiruk-pikuk masalah ini selalu saja ada perbedaan. Akan tetapi Juliawan menutup tulisannya dengan kata-kata yang menarik, "Kendati ada kekurangan, pencarian Habermas terhadap ruang publik pantas dibela di hadapan situasi konflik … kita hanya punya dua pilihan: mengusahakan ruang publik atau menanggung akibatnya!" Lihat, B. Hari Juliawan, *Ruang Publik Habermas: Solidaritas Tanpa Intimitas*, dalam Basis (Edisi 75 tahun Jurgen Habermas), No. 11-12, tahun ke-53, November-Desember 2004, hal. 38-39.

[74] F. Budi Hardiman, *Heidegger dan Mistik Keseharian: Suatu Pengantar Menuju Sein und Zeit*, (Jakarta: Kepustakaan Populer Gramedia (KPG), 2008), hal. 58-62.

carut-marut publik yang kian gelisah karena tidak kunjung menentunya keteraturan di dalam ruang tersebut.

Memasukkan pemahaman eksistensialisme ke dalam pemahaman akan ruang publik mayantara merupakan kebutuhan, karena perubahan konsep ruang dan makna-makna di dalamnya, dari ruang nyata ke maya. Pemahaman eksistensialis membantu menegaskan 'keberadaan' person di dalam suatu ruang spasial, sebagai subjek dari suatu kajian hukum pidana mayantara.

### 2.4.3 Penelitian Terhadap Publik Mayantara untuk Perbaikan Sistem Hukum

Dalam penelitian tentang peran publik mayantara dalam penegakan hukum pidana ini dilakukanlah pengamatan terhadap beberapa komunitas *hacker* di Indonesia. Pengamatan tersebut berdasarkan jalinan sosial yang berlangsung cukup lama, dan pengamat berperan sebagai anggota beberapa komunitas, dan memanfaatkan ikatan sosial dengan para aktivis yang terjalin cukup lama, baik secara *online* (memanfaatkan internet sebagai alat komunikasi) maupun secara *offline* (pertemanan di dunia nyata).

Seperti dalam lingkungan sosial ruang nyata, yang terdapat kelas menengah dengan bekal akademis yang cukup untuk mengamati dan memberikan berbagai analisis terhadap lingkungannya dan kemudian mentransformasi lingkungan sosialnya untuk senantiasa adaptif dan waspada terhadap segala perubahan dan ancaman potensial terhadap anggota masyarakat, komunitas-komunitas *hacker* merupakan simpul-simpul pertemuan para agen-agen intelektual dunia maya (mereka yang menguasai pengetahuan tentang teknologi informasi mayantara). Agen-agen ini memiliki kemampuan teknis mengenai lingkungannya dengan baik, dan mereka juga senantiasa belajar untuk selalu waspada (*keep aware*) dengan lingkungannya.

Pada beberapa komunitas tersebut dilakukan wawancara terhadap beberapa pendiri (*founder*) komunitas *hacker*, pakar teknologi informasi,

dan aktivis *cyberspace* lain yang biasa berbaur dengan kehidupan para *hacker* dalam berbagai jenjang keahlian. Wawancara dilakukan untuk mendapatkan jawaban mengenai permasalahan ruang publik mayantara yang berkaitan dengan kriminalitas di dalamnya, peran alat-alat hukum selama ini, dan bagaimana potensi peran publik mayantara dalam penegakan hukum pidana dalam ruang mayantara. Hal ini untuk memberi pemahaman logis dari aktivis yang lebih akrab dengan suasana *cyberspace*.

Para narasumber adalah: DM dari Semarang, *ex-viruswriter* (mantan *virurwriter*) yang kini lebih aktif sebagai spesialis *cybersecurity* dan SEO (*search engine optimiser*); BD dari Magelang, seorang *hacker* otodidak sekaligus founder komunitas *hacker underground* 'Magelangcyber' dan aktivis pada komunitas *hacker underground* 'Indonesian Coder'; KYF dari Yogyakarta, seorang *founder* komunitas *white-hat hacker* 'YogyaFree'; PZ dari Jakarta, seorang administrator (moderator) komunitas *white-hat hacker* Jasakom sekaligus *co-founder* komunitas *white-hat hacker* Cisadane; XP dari Tangerang, *lead-founder* komunitas *white-hat hacker* Cisadane. Penyebutan kota adalah lokasi saat dilakukan wawancara. Di samping itu dilakukan pula interview dengan pakar teknologi informasi independen, Onno W. Purbo.

Wawancara yang dilakukan dengan DM, BD, dan PZ dilakukan dengan tatap muka secara langsung. Sedangkan wawancara dengan KYF, XP, dan Onno W. Purbo dilakukan melalui *e-mail*. Dengan kesibukan para aktivis tersebut di dalam komitmen masing-masing untuk sama-sama membina kesadaran publik, terutama dalam komunitasnya (bagi para penggiat komunitas), antusiasme mereka dalam memajukan internet sehat bagi negeri ini terus terasah dengan berbagai permasalahan yang semestinya hukum telah mengambil bagian. Namun keprihatinan atas lemahnya sistem internal, baik hukum maupun cyberspace, di Indonesia masih saja menjadi ganjalan.

Melihat masih rentannya keamanan dan jaminan keselamatan dalam ruang maya bagi individu-individu yang berinteraksi di dalamnya, maka pendekatan langsung kepada fakta sosial dan karakter ruang sosial ini akan membantu dalam menganalisa potensi supremasi hukum dalam *cyberspace*. Untuk menjembatani antara situasi riil kepada analisis yang proporsional maka diperlukan tinjauan pustaka dan penyajian data riil.

Berbagai kekecewaan akan kurang kuatnya sistem hukum dalam *cyberspace* menjadi hal yang mampu menyulut lemahnya optimisme pada semangat supremasi hukum. Krisis legitimasi hukum ini semestinya ditanggulangi dengan mendorong rasionalisasi fungsi hukum terhadap realitas, dengan demikian pemahaman ruang publik dan pentingnya peranan agen-agen perubahan. Satjipto Rahardjo mengisyaratkan bahwa dalam suatu sistem sosial terdapat lembaga-lembaga yang masing-masing peranannya tidak bisa berjalan sendiri-sendiri. Jika terdapat disharmoni antara perubahan sosial dengan perubahan hukum maka akan menimbulkan problem sosial, oleh karenanya perubahan dinamis di satu bidang seharusnya dilakukan pula penyesuaian pada bidang lain, agar keadaan kembali menjadi lancar.[75]

Dengan pemahaman para agen sosial mayantara tersebut dan sumbangsih yang sedikit tapi berkelanjutan yang mereka berikan, setidaknya pada komunitas mereka, penting kiranya berdialog dan menyerap wawasan mereka demi pembenahan sistem hukum pidana. Dalam pembahasan selanjutnya akan diuraikan bagaimana kebutuhan suatu sistem hukum untuk memperkuat jaringan sosialnya dalam ruang mayantara. Komunikasi dan aksi yang saling sejajar dan memahami dengan saling koreksi yang didukung dengan keterbukaaan antara masyarakat hukum dan negara, akan memberikan sumbangan berarti bagi perbaikan sistem hukum mayantara Indonesia.

---

[75] Satjipto Rahardjo, *Hukum dan Perubahan Sosial*, (Yogyakarta: Genta, 2009), hal. 35-37.

Dalam upaya penyesuaian inilah diperlukan kerjasama dan saling memahami. Dengan memanfaatkan konsep diskursus dalam teori tindakan komunikatif Habermas, serta bagaimana opini publik menjadi mungkin (*possible*) dan efektif dalam negara hukum dengan cakupan demokrasi deliberatif antara negara dengan para aktor/agen sosial mayantara yang lebih memahami karakter, mekanisme, dan realitas ruang publik yang sekaligus ruang dimana hukum semestinya ditegakkan, diharapkan dapat memberikan jalan keluar atas berbagai permasalahan penegakan hukum pidana dalam mayantara.

## 2.5 Pengantar kepada Pemikiran Jurgen Habermas

Thomas McCarthy dalam pengantar karya Jurgen Habermas, *Legitimation Crisis*, mengutip George Lichtheim dalam mengomentari tentang Habermas dan pemikirannya:

> Yang paling mengagumkan pada Habermas adalah, di usia ketika kebanyakan koleganya masih bersusah payah menguasai salah satu sudut intelektual, dia telah menjadikan dirinya sebagai guru atas semua wilayah pemikiran dengan kedalaman dan keluasan wawasan yang sudah tak terukur lagi. Dia tidak prenah salah dalam menafsir, namun tidak pernah pula mengelak ketika menemui kesulitan dalam memahami pernyataan atau kesimpulan yang menurutnya mengada-ada karena tidak didukung oleh penelitian. Sikap dewasa ini sangat tampak, misalnya, ketika dia membuktikan kesalahan Popper, mempreteli pramatisme Charles Pierce, menginvestigasi para guru metafisika Schelling di Abad Tengah, dan bahkan ketika dia memodernkan sosiologi Marxis. Jika Anda sempat membacanya, Anda akan melihat kemumpunian penguasaan Habermas yang tak terbantahkan atas sumber-sumber tersebut. Berpadu dengan talenta paripurna, Habermas mampu mengklarifikasi teka-teki logis alam pikiran yang sangat rumit sekalipun.[76]

[76] Thomas McCarthy (Boston University) menerjemahkan karya-karya besar Jurgen Habermas dari Bahasa Jerman ke dalam Bahasa Inggris. Kutipan ini dalam buku karya Jurgen Habermas, Krisis Legitimasi, Qalam: Yogyakarta, 2004, yang sudah diterjemahkan ke dalam bahasa Indonesia dari terjemahan McCarthy, *Legitimation Crisis*. Kutipan pendapat Lichtheim, *From Marx to Hegel* (New York, 1971), h. 175-176. Kalimat-kalimat yang dikutip ini aslinya ada di dalam analisis Habermas *Erkenntnis und Interesse* (Frankfurt, 1968), yang muncul juga di dalam *Times Literary Supplement*, 5 Juni 1969.

Keutamaan Habermas dalam mengawal pemikiran sosiologi kritis dewasa ini dinilai demikian otoritatif, bahkan Lichtheim menambahkan, "Lebih baik daripada Hegel, Habermas sendiri mampu menulis sejernih dan setepat kaum empiris."[77] Ketelitian Habermas dalam menganalisis permasalahan sosiologi modern dan mengkritisinya memang mampu menyisir berbagai lahan ilmu sosial yang bersentuhan dengan masyarakat dan logika modernitas yang melekat dan berkembang bersamanya, tetapi Habermas bukanlah seorang pemikir statis, seiring dengan George Ritzer,[78] bahwa melalui berbagai karya besarnya, Habermas seorang sosiolog yang konsisten pada grand theory tentang modernisme di tengah kian gencarnya serangan post-modernisme. Konsepnya tentang ruang publik dan konsep masyarakat komunikatif ini terus menunjukkan konsistensinya kepada modernitas dan optimisme Habermas sendiri kepada masa depan masyarakat modern.

Jurgen Habermas sebagai seorang pemikir sosial dan sebagai filosof, secara khusus dalam filsafat Jerman, yang penting dewasa ini, adalah tokoh besar dalam pemikiran Mazhab Frankfurt yang dikenal dengan Mazhab Filsafat Kritis. Perkembangan pemikiran dalam Mazhab Frankfurt penuh dengan pertarungan gagasan, Habermas terus menemui perdebatan panjangnya dengan arus pemikiran postmodernisme.

Postmodernisme dalam filsafat akan sulit dipahami tanpa terlebih dahulu mendalami pemikiran Mazhab Frankfurt dan Habermas. Mazhab Frankfurt bukan hanya menemui kemacetan Teori Kritisnya, melainkan juga menemukan jalan buntu proyek modernisasi yang terlalu memuja *Zweckrationalitaet* (rasionalitas tujuan), sebagaimana beroperasi dalam birokrasi, sains dan teknik modern. Postmodernisme dan Habermas bereaksi berbeda atas jalan buntu itu: Sementara postmodernisme bersikap skeptis terhadap modernitas dan bermaksud

[77] Dalam Jurgen Habermas, *Krisis Legitimasi* (*Legitimation Crisis*), diterjemahkan oleh Yudi Santoso, (Yogyakarta: Qalam, cet. Pertama, 2004), sebuah pengantar oleh McCarthy mengutip pendapat George Lichtheim tentang pemikiran Habermas.

[78] George Ritzer dan Douglas J. Goodman, *Teori Sosiologi Modern* (*Modern Sociological Theory*), diterjemahkan oleh Alimandan, (Jakarta: Kencana, cet. Keenam, 2010), hal. 579.

meninggalkan proyek modernisasi itu sendiri, Habermas mencari jalan keluar baru untuk melanjutkan modernisasi dengan paradigma baru.[79]

Kita akan secara singkat berusaha memahami alur pembentukan akar pemikiran Habermas yang merupakan tokoh Filsafat Kritis yang tersisa dari sekian banyak pemikir utama lainnya.

### 2.5.1 Latar Belakang Historis Sekolah Frankfurt

Mazhab Frankfurt, atau biasa juga disebut dengan Sekolah Frankfurt, menunjuk kepada sekelompok cendekiawan yang tergabung dalam *Institut für Sozialforschung* (*Institute for Social Research*). Institusi ini dipicu oleh Felix J. Weil putra tunggal seorang saudagar dagang *grain* (padi-padian, termasuk padi dan gandum) Hermann Weil, lelaki asli Jerman yang hijrah ke Argentina. Felix yang kelahiran Buenos Aires pada 1898, disekolahkan pada Goethe Gymnasium, dan juga merupakan sebuah Universitas yang benar-benar masih baru di Frankfurt. Ia belajar di sana hingga lulus *magna cum laude* pada program doktoral di bidang ilmu politik. Disertasinya sendiri adalah tentang permasalahan dalam penerapan sosialisme, yang kemudian diterbitkan secara serial dan diedit oleh Karl Korsch,[80] karyanya ini mengantarkannya kepada ketertarikan akan pemikiran Karl Marx. Sejak itulah Felix Weil bersama juga Korsch mulai mengadakan gerakan radikal di Jerman, Felix mengadakan pertemuan kajian tentang pemikiran Marx.[81]

Kemudian ambisi untuk membentuk sebuah institusi yang lebih mapan pun muncul dan beruntung kemudian Felix berteman dengan dua orang sahabat yang sama-sama *summa cum laude* dari program doktoral, Friedrich Pollock dari jurusan Ekonomi yang mengagas konsep uang oleh Marx, kemudian ada seorang yang kemudian menjadi penting dalam perjalanan sejarah Mazhab Frankfurt, Max Horkheimer dari jurusan filsafat

---

[79] Fransiskus Budi Hardiman, *Kritik Ideologi*, (Yogyakarta: Buku Baik, 2004), hal. v-vi.

[80] Korsch merupakan pemikir mandiri generasi pertama yang mendasarkan kepada pemikiran Karl Marx. Korsch dalam masanya ada bersama-sama (semasa) dengan Lukacs, Gramsci, dan Bloch. Lihat: Franz Magnis-Suseno, *Pemikiran Karl Marx*, (Jakarta:Gramedia, 2001), hal. 11.

[81] Martin Jay, *The Dialectical Imagination*: *A History of Frankfurt School and The Institute of Social Research 1923-1950*, (London: Heinemann Educational Book Ltd, 1976), hal. 5.

yang lulus dengan pembahasan tentang pemikiran Kant. Selanjutnya karena melihat adanya keinginan baik Felix akan keyakinan untuk membentuk lembaga pemikiran yang independen dari birokrasi hirarkis kampus, Hermann Weil bersedia membantu pendanaan lembaga ini.[82] Secara sederhana lembaga tersebut kemudian diberi nama Institut für Sozialforschung. Dalam tulisan Martin Jay tentang sejarah awal Mazhab Frankfurt ini dikatakan bahwa Hermann Weil dalam memberikan bantuannya tidak memiliki tujuan politis, dan meskipun tidak dalam jumlah besar, bantuan tersebut telah memberikan arti penting dalam merawat institusi tersebut dan menjadikannya mampu mandiri dan terbukti memberikan manfaat yang besar dalam sejarahnya.

Shindunata dalam "Dilema Usaha Manusia Rasional" mengungkapkan bahwa, sejak semula Weil ingin agar kelompok cendekiawan yang tergabung dalam institutnya benar-benar independen dari kelembagaan maupun kepartaian. Kelak institut tersebut memang berafiliasi dengan Universitas Frankfurt. Namun institut yang dibangun Weil itu tetap mempertahankan keindependenannya secara material maupun intelektual.[83]

Pada awal terbentuknya institut ini terdiri atas beberapa tokoh dari berbagai bidang yang cukup menonjol adalah: Friedrich Pollock (ahli ekonomi), Carl Grunberg (Direktur pertama Institut), Max Horkheimer (filsuf, sosiolog, psikolog dan direktur sejak 1930), Karl Wittfogel (sejarahwan), Theodor Wiesendrund-Adorno (filsuf, sosiolog, musikolog), Leo Lowenthal (sosiolog), Walter Benyamin (kritikus sastra), Herbert Marcuse (filsuf), Franz Neumann (ahli hukum), Erich Fromm (psikolog sosial), Otto Kircheimmer (ahli politik), Henryk Grossmann (ahli ekonomi dan politik), Arkadij Gurland (ahli ekonomi dan sosiologi).[84] F. Budi Hardiman memberikan tambahan, bahwa sejauh 'mazhab' atau 'aliran'

[82] *Ibid*., hal. 6-8.
[83] Sindhunata, *Dilema Usaha Manusia Rasional*, (Jakarta: Gramedia, 1982), hal. 20.
[84] Budi Hardiman, *op.cit.*, hal. 20.

dimengerti sebagai arus pemikiran yang sama, kita dapat memberi sebutan 'Mazhab Frankfurt' hanya pada Horkheimer, Adorno, Marcuse, Lowenthal dan Pollock. Dan di antara kelimanya, hanya Adorno, Horkheimer dan Marcuse, para komentator memberi sebutan Generasi Pertama Teori Kritis.[85]

Selanjutnya dari demikian banyak pemikir inti dari Sekolah Frankfurt ini memunculkan banyak karya yang berpengaruh terutama di Jerman dan Eropa. Pemikiran khas dari institut ini adalah garis besar pada Teori Kritis (*critical theory*) yang diterapkan kepada bidang-bidang humaniora yang dipimpin oleh tiap-tiap anggota institut, terutama mereka yang sebagaimana disebutkan oleh Budi Hardiman sebagai generasi pertama teori kritis.

### 2.5.2 Latar Belakang Teoritis Sekolah Frankfurt

Jantung dari Teori Kritis adalah sebuah penolakan untuk menutup berbagai sistem filosofis yang mungkin berkaitan. Teori Kritis, sebagaimana namanya, memberikan implikasi yang dimunculkan melalui serial dari beberapa kritik dari pemikir-pemikir lain dan berbagai tradisi filosofis. Pengembangannya adalah dengan memanfaatkan dialog, asal-usulnya sebagai metode dialektis dengan maksud untuk diterapkan dalam fenomena sosial.[86] Dan melalui cara mengkonfrontasikannya dengan berbagai situasi dan tantangan atau godaan pada masanyalah apa yang dihasilkan oleh kajian teori kritis ini lebih dapat dipahami dan mendapatkan apresiasi.

Sejak semula sekolah Frankfurt menjadikan Marxisme sebagai titik tolak pemikirannya. Namun sekolah Frankfurt juga meletakkan dirinya dalam perspektif idealisme Jerman, yang dirintis oleh Immanuel Kant (kritisisme) dan memuncak pada ajaran Hegel (dialektika). Ketika Horkheimer menjabat direktur, ia memasukkan ajaran Freud. Hal ini

[85] *Ibid*.
[86] Jay, *op.cit.*, hal. 41.

dianggap bertentangan dengan ortodoksi Marxisme, tetapi menurut Horkheimer ajaran Freud adalah kebutuhan mendesak bagi teori kritis untuk menghadapi tantangan kapitalisme monopolis dan fasisme.[87] Maka secara garis besar sumber utama teori kritis yang diterapkan oleh sekolah Frankfurt adalah Kritisisme Kant dan Hegel, Marxisme serta psikoanalisa Freud.

#### 2.5.2.1 Kritisisme Kant

Kant mengkritisi bagaimana ilmu pengetahuan disusun pada masa sebelumnya. Kant berusaha memeriksa bagaimana kesahihan pengetahuan telah dibentuk, tidak sekedar dengan metode empiris, melainkan dengan teknik yang transendental yaitu memeriksa secara teliti apakah pengetahuan itu hadir dari subyek pengetahuan itu sendiri dari dalam dirinya secara *a priori*. Dan Kant kemudian berusaha menemukan teknik untuk mengetahui bagaimana kemungkinan untuk menemukan pengetahuan yang *a priori* tersebut.

Kemudian Kant berusaha mencari tahu bagaimana kemungkinan rasio berkaitan dengan objek-objek dari luar rasio, yang kemudian disebut *die Bedingung der Moglichkeit* (syarat-syarat kemungkinan) dari pengetahuan kita. Syarat-syarat ini tidak lepas dari prinsip bahwa sebuah penelitian disebut "transendental" kalau memusatkan diri pada kondisi-kondisi yang murni dalam diri subjek pengetahuan.[88]

Dalam buku "Filsafat Modern," F. Budi Hardiman menjelaskan lebih lanjut bahwa, Kant sebenarnya ingin mensintesiskan antara empirisme yang bersandarkan pada pengetahuan *a posteriori* dengan rasionalisme yang bersandar

[87] Sindhunata, *op.cit.*, hal. 29.

[88] Fransiskus Budi Hardiman, *Filsafat Modern: dari Machiavelli sampai Nietzsche*, (Jakarta: Gramedia, 2007), hal. 132.

pada pengetahuan *a priori*.[89] Pada saat bersamaan dengan membaca filsafat Kant, kita diajak untuk berusaha melepaskan semua unsur di luar rasio yang mungkin dapat memengaruhi pengetahuan dan melepaskan pengetahuan dari kepentingan di luar pengetahuan itu sendiri, sekaligus berusaha memahami potensi rasio menerima perluasan pengetahuan dari objek-objek yang berada di luar rasio kita.

Istilah 'kritisisme' dalam filsafat Kant dipertentangkan dengan 'dogmatisme', karena sebelum masa Kant pengetahuan didapatkan dengan filosofi yang menerima begitu saja kemampuan rasio tanpa menguji batas-batasnya, kritisisme dipahami sebagai sebuah filsafat yang lebih dahulu menyelidiki kemampuan dan batas-batas rasio sebelum memulai penyelidikan.[90] Demikianlah ketertarikan utama Kant, menyelidiki bagaimana pengetahuan itu didapatkan, menyusurinya dari asal pengetahuannya, baik dari subyek maupun dari objek.

Jadi tidak ada sesuatu pada dirinya sendiri, semuanya ditentukan oleh keaktifan pengetahuan subjektif. Dengan demikian manusia tidak perlu lagi memahami alam sebagai semata-mata alamiah, tapi menggantikannya sebagai "kebudayaan", artinya alam yang telah dirasionalkan manusia. Sejarah pun tidak perlu lagi berjalan secara deterministis, sejarah harus dipahami secara kritis sebagai pengungkapan diri manusia secara rasional.[91]

Pada kenyataannya Kant tidak sepenuhnya diikuti begitu saja oleh Sekolah Frankfurt. Mazhab Frankfurt juga mengkritisi Kant dalam beberapa hal, terutama pada keterbatasannya yang

[89] *Ibid*., hal. 133. Filsafat Kant menjelaskan pengetahuan sebagai sintesis antara unsur-unsur *a priori* dan *a posteriori*.
[90] *Ibid*., hal. 133.
[91] Sindhunata, *op.cit.*, hal. 31.

masih dirasa kurang untuk dapat mendukung proyek kritisisme yang mereka usung. Sekali lagi untuk memperkuat akar kritisisme, mereka tetap membutuhkan kritik atas pemikiran tokoh yang dijadikan acuan.

Sekolah Frankfurt memandang bahwa Kant tidak memandang pengetahuan manusia sebagai terbentuk secara historis, yang terikat juga oleh situasi tertentu. Kant bisa jadi berusaha mensintesiskan antara pengetahuan *a priori* dengan pengetahuan yang bersifat *a posteriori* yang berkenaan dengan persentuhan dari luar diri. Tetapi hal itu, setidaknya dalam tulisan Sindhunata,[92] dikatakan kurang berani menerobos ke dalam hal-hal di luar akal budi manusia, padahal penerobosan itulah yang bisa memperkaya isi pengetahuan manusia. Dan selanjutnya dikatakan bahwa, jika dengan model Kant yang demikian maka semua penilaian terhadap pengetahuan akan bersifat formal, karena dalam kritisisme Kant syarat-syarat kebenaran bersifat subjektif.

Namun pemikiran Kant merupakan upaya memurnikan pengetahuan dari akarnya, dan serta-merta mengajak kita untuk menguji kesahihan pengetahuan. Kemungkinan untuk menerobos ke dalam hal-hal di luar akal budi manusia dalam konsep Kant, rasanya tetap bisa terjadi jika persentuhan subjek dan penilaiannya terhadap objek di luar dirinya terjadi dengan cepat dan untuk merespon kejadian secara keseluruhan. Tetapi demi mendapatkan keutuhan kritisisme, lantas dilanjutkan kepada Hegel yang mengatakan kebenaran adalah keseluruhan (*the truth is the whole*), yang dinilai mampu menutupi kekurangan Kant.

#### 2.5.2.2 Kritisisme Hegel

[92] *Ibid*.

Berbeda dengan kritisisme Kant, Hegel mengembangkan kritik dengan caranya sendiri dan bahkan juga mengkritisi epistemologi Kant. Di atas telah dijelaskan bahwa kritik Kant bersifat transendental demi mendapatkan kebenaran yang kokoh. Kant menemui kritik bahwa rasio atau akal budi dalam kritiknya subjek bersifat ahistoris, hal ini berarti tidak menghiraukan bagaimana rasio juga sesungguhnya dipengaruhi oleh situasi sejarah tertentu.

Dengan istilah Hegel, rasio ditempatkan di dalam rangka proses pembentukan-diri (*Bildungsprozess*) dari rasio. Dalam *Bildungsprozess* atau *Self-formative process* adalah proses sejarah kebudayaan atau proses pembudayaan manusia. Kata *Bildung* berarti pendidikan kepribadian. Dalam pandangan Hegel, rasio bersifat kritis tidak dengan cara transendental dan ahistoris seakan-akan rasio itu sudah sempurna pada dirinya. Rasio menjadi kritis justru kalau ia menyadari asal-usul pembentukannya sendiri. Rasio semakin sadar saat ia menghadapi rintangan-rintangan dalam sejarah, untuk menjadi semakin rasional dan semakin sadar, dan rasio melangkah ke kualitas rasionalitas yang lebih tinggi.[93] Hegel menjelaskan epistemologi kritisnya dengan cara yang berbeda, ia berusaha menyusun narasi dengan memanfaatkan alur peradaban manusia, bagaimana rasio dipengaruhi oleh keadaan dan lingkungan sekitarnya yang historis.

Dengan memanfaatkan alur sejarah dan beberapa pertentangan peradaban dalam sejarah dunia, Hegel menjelaskan maksudnya bahwa rasio mencapai kesadarannya yang lebih tinggi dengan menghadapi rintangan dan berusaha menyelesaikan

[93] Fransiskus Budi Hardiman, *Kritik Ideologi*, (Yogyakarta: Buku Baik, 2004), hal. 44.

pertentangan-pertentangan di dalamnya.[94] Hegel memberikan contoh, salah satunya adalah Revolusi Perancis. Meskipun revolusi ini menghasilkan korban-korban, berkat pertentangan inilah warga negara memperoleh kebebasannya dari kekuasaan monarkhi absolut. Kesadaran yang diperoleh dalam revolusi Perancis tak lain dari hasil refleksi dan perjuangan rasio sendiri untuk menyadari adanya rintangan-rintangan untuk menjadi semakin bebas dan sadar. Proses sejarah manusia memahami siapa dirinya, apa itu masyarakat, kebudayaan, dan alam semesta adalah proses pembentukan-diri Rasio.[95]

Bagi Hegelian, kritik berarti negasi atau dialektika, karena bagi Hegel kesadaran timbul melalui rintangan-rintangan, yaitu dengan cara menegasi atau mengingkari rintangan-rintangan itu.[96] Maka proses untuk mengatasi dan menyelesaikan tantangan sejarah adalah proses kritis yang niscaya akan memberikan kesadaran baru bagi rasio untuk melangkah ke tingkatan rasionalitas yang lebih tinggi.

#### 2.5.2.3 Kritisisme Marx

Filsafat Marx secara khusus menjadi kritik terhadap filsafat Hegel. Dalam pandangan Marx, Hegel menjelaskan proses kritisisme adalah dalam wilayah rasio saja, bukan dalam bentuk kritisisme fisik. Menurut Marx dialektika kritis Hegel hanya sebatas pada pemahaman semata dan tidak mampu melakukan perubahan yang lebih nyata. Oleh karena itu dengan kritiknya kemudian Marx, dengan tetap berpegang pada dialektika Hegel,

[94] Lihat sebagaimana Hegel memberikan beberapa peradaban dunia sebagai bukti perkembangan kesadaran rasio manusia (G.W.F. Hegel, Filsafat Sejarah, Pustaka Pelajar: Yogyakarta, 2001).

[95] Budi Hardiman, *op.cit.*, hal. 45.

[96] *Ibid*., hal. 46.

berusaha menarik ide kritis Hegel ke dalam wilayah fisik yang lebih praktis.

Oleh karena itu kemudian Marx menjelaskan filsafatnya dalam materialisme dengan mengamati tentang manusia dan ekonomi. Filsafat Marx memang ditujukan untuk mengatasi serangan kapitalisme yang menghisap perekonomian rakyat di kelas bawah, sebagaimana teori kelas Marx tentang kelas atas dan kelas bawah yang menjelaskan bahwa perubahan dalam masyarakat bukanlah oleh individu-individu melainkan oleh kelas-kelas dalam masyarakat.

Marx pada awalnya memandang bahwa filsafat Hegel adalah akhir dari filsafat, karena konsepnya yang totalitas dialektika sejarah dalam menjelaskan kesadaran rasio ke tingkatnya yang lebih tinggi, tetapi Marx merasa perlu untuk menjadikan dialektika Hegel ke dalam ranah praktis. Filsafat Hegel sendiri baru merupakan salah satu tahap dalam perkembangan Roh, yaitu tahap teoritis. Maka tahap ini berarti: filsafat Hegel perlu disangkal secara dialektis. Tesis Hegel bahwa filsafatnya adalah pengetahuan absolut harus disangkal oleh tindakan praktis. Filsafat Hegel belum absolut karena keabsolutannya hanya dalam teori, sedangkan realitas sosial-politik masih belum tersentuh filsafat.[97]

Dalam pemikiran Hegel ia memandang bahwa kepentingan manusia adalah pemenuhan hasratnya sendiri, dan ini bisa menjadikan keadaan kacau-balau, hal ini menurut Hegel tidak dapat dibiarkan saja, melainkan harus ditampung dalam oleh negara. Negara kemudian diasumsikan sebagai bentuk kesejahteraan universal yang merupakan hakikat realitas yang

[97] Franz Magnis-Suseno, *Pemikiran Karl Marx: Dari Sosialisme Utopis ke Perselisihan Revisionisme*, (Jakarta: Gramedia, 2001), hal. 64.

benar dan umum, oleh karenanya negara adalah tujuan yang sebenarnya bagi masyarakat sedangakan keluarga dan masyarakat luas adalah unsur-unsurnya. Hal inilah yang mendapat kritik dari Marx, Marx menilai Hegel memutarbalikkan subjek dan objek. Dalam filsafat Hegel masyarakat sebagai objek, tetapi sebenarnya masyarakatlah yang berperan sebagai subjek. Kemudian di dalamnya Marx menemukan kekurangan lain Hegel, yaitu Hegel berusaha menertibkan egoisme masyarakat modern dengan negara, hal ini berarti kesosialan (anti-egoisme) tidak masuk kembali ke dalam manusia, melainkan hanya dipaksakan dari luar kepadanya oleh negara; padahal yang perlu adalah mengembalikan kesosialan manusia itu sendiri.[98]

Demikianlah kritik Marx yang khas dialektis materialistik. Namun kelemahan Marx selalu pada konsep utopianya yang membuat tidak nyata analisis dan jalan keluar yang ditawarkan. Kelelahan dalam mengejar konsep Marx tentang kelas dan produksi yang mampu menjadikan manusia menemukan dirinya dengan bayangan besar utopianya justru mengesankan Marx terlalu memandang bahwa perubahan dan pembebasan manusia dapat dilakukan dengan kesederhanaan struktur dasar pemikirannya.

#### 2.5.2.4 Kritisisme Freud

Psikoanalisa sudah sejak awal adalah temuan khas Freud terhadap dunia kejiwaan, sehingga psikoanalisa bisa juga dikatakan sebagai ‘Psikoanalisa Freud’. Freud memaparkan promosinya kepada berbagai kalangan tentang kajian ilmu baru,

[98] Lihat penjelasan Franz Magnis dalam pola dasar kritik Marx terutama terhadap hukum negara Hegel, dalam: Franz Magnis-Suseno, *Filsafat Sebagai Ilmu Kritis*, (Yogyakarta : Kanisius, 2001), hal. 120-122.

psikoanalisa, dalam kumpulan lima ceramahnya.[99] Di dalam penjelasan dan promosinya Freud menyampaikan tentang metode yang ia pakai dan kritik keras dari berbagai pihak terhadap cara pandangnya. Metode psikoanalisa ini adalah kritik Freud terhadap psikologi yang telah mapan. Kritik atasnya yang paling umum adalah tentang pandangan Freud bahwa tekanan seseorang adalah pengaruh dari tekanan seksual yang dibawa sejak usia anak-anak. Sanggahannya adalah bahwa anak-anak tidak memiliki tekanan bersifat seksual, itu hanya dimiliki orang dewasa. Namun bukti-bukti kemudian bermunculan dari rekan-rekan Freud sendiri, misalnya tentang bagaimana ikatan bersifat seksual di masa kanak-kanak bisa mempengaruhi tekanan psikis di kemudian hari. Oleh karena itulah Freud menyampaikan dalam kelima ceramahnya itu bahwa meneliti kejiwaan itu seperti menyelediki atau mencari penyakit secara hati-hati dengan pisau bedah terhadap pasien, dengan ingatan masa lalunya yang berlapis-lapis.

Dalam Mazhab Kritis, konsep kritik Freud mampu memberikan pengertian yang lebih lengkap, meskipun Freud tidak secara eksplisit menyebut konsep kritiknya. Dengan ini Teori Kritis berupaya mengintegrasikan konsep-konsep kritis dari Freud mengenai gangguan-gangguan psikis dan naluri-naluri ke dalam kritik-ideologi Marx. Dengan cara ini suatu kritik yang bersifat kemasyarakatan mendapat pendasaran psikologisnya.[100]

Dalam psikoanalisa Freud menjelaskan bahwa dalam berbagai bentuk psikopatologi yang dialami oleh manusia adalah karena adanya berbagai tekanan psikis yang tertahan dan kemudian menjadi gangguan-gangguan kejiwaan, tekanan yang menumpuk itu terjadi karena seseorang berusaha menutupi, atau

[99] Sigmund Freud, *Memperkenalkan Psikoanalisa: lima ceramah (Ueber Psychoanalyse, Funf Vorlesungen)*, diterjemahkan oleh K. Bertens, (Jakarta: Gramedia, cet. Keenam, 1987).

[100] Fransiskus Budi Hardiman, *Kritik Ideologi*, (Yogyakarta: Buku Baik, 2004), hal. 49.

secara tak sadar karena tekanan bawah sadar memaksanya menyimpan tekanan-tekanan itu. Maka dengan menciptakan gambaran-gambaran palsu, ilusi-ilusi, delusi-delusi dan melakukan mekanisme pertahanan diri, subyek merasa seolah-olah memperdamaikan konflik-konfliknya, tetapi sesungguhnya semua ini hanyalah penipuan diri oleh diri dan penindasan diri oleh dirinya sendiri. Dengan demikian subyek psikoanalisis Freud, seperti juga kaum proletariat pada teori Marx, berada dalam situasi ketidakbebasan. Hanya pada pasien Freud, ketidakbebasannya adalah ketidakbebasan psikis.[101]

Walaupun telah dijelaskan bahwa pembahasan soal represi dalam Freud melulu bersifat psikis yang kemudian berusaha diterapkan secara adaptif ke dalam bentuk tekanan yang dialami kaum proletar dalam teori Marx untuk mengungkap ketertindasan dan tipuan di dalamnya, sebenarnya dalam salah satu ceramahnya Freud juga menjelaskan tentang bagaimana simbol-simbol represi itu dengan menggeneralisir pada bentuk-bentuk fisik di luar diri,

> Di tempat lain dalam kota yang sama, tidak jauh dari "London Bridge", terdapat sebuah tiang tinggi dan lebih modern yang dikenal sebagai "The Monument". Ini memperingati terjadinya kebakaran besar yang telah melanda tempat di sekitar itu pada tahun 1666 dan memusnahkan sebagian besar kota. Maka monumen-monumen ini merupakan simbol-simbol ingatan sama seperti gejala-gejala histeria.[102]

Dengan pertimbangan generalisasi yang disampaikan oleh Freud dalam dunia nyata, yang mengingatkan orang kepada memori negatif di masa lalu, kiranya hal itulah yang bisa dijadikan analogi bagi penerapannya dalam pemikiran kritis secara praktis. Menarik kajian psikologi personal ke dalam bentuk psikologi

[101] *Ibid*., hal. 50.
[102] Freud, *op.cit.*, hal. 10-11.

masyarakat, meliputi manipulasi dan berbagai hal yang membenarkan represi.

### 2.5.3 Diskursus dan Demokrasi Deliberatif Habermas

Untuk membahas publik mayantara (*cyber society*) kiranya gagasan-gagasan Jurgen Habermas untuk mengkaji masyarakat modern bertalian erat dan memiliki kompetensi untuk itu, juga dari sisi hukumnya. Dalam membahas bab tentang peran politis ruang publik di "*The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*," Habermas telah mengulas perihal kepublikan dan posisi otoritas di dalamnya dalam pembentukan hukum serta dialektika di dalamnya dengan mencontohkan perkembangan akses peran publik sebagai kritik terhadap parlemen dan segala bentuk kebijakan serta pemantauan atasnya dengan memanfaatkan fungsi investigatif dari media massa, dalam hal ini koran. Dengan contoh historis dari Inggris Habermas memberikan perihal perkembangan hukum publik dan privat di Inggris.

Franz Magnis-Suseno meringkas perkembangan pemikiran Habermas. Pemikiran Habermas bertolak dari Marx, Pengetahuan dan Kepentingan, Rasionalitas dan Kebebasan. Setelah itu kajiannya terhadap patologi modernitas yang menjadi hasil perjalanannya itu, yang digariskannya tahun 1982 dalam dua jilid karya sentralnya *A Theory of Communicative Action* (TCA). Kemudian diakhiri dengan dua konsepsi yang disampaikan oleh—Franz Magnis menyebutnya—, Habermas "matang" yang ia anggap paling penting, etika diskursus dan paham demokrasi deliberatif. Franz Magnis menjelaskan hasrat paling dasar Habermas sebagai: "menyelamatkan warisan Pencerahan melawan mereka yang menggerogotinya."[103]

#### 2.5.3.1 Berangkat dari Marx

[103] Franz Magnis-Suseno, 75 Tahun Jurgen Habermas, dalam Majalah Basis, Nomor 11-12, Tahun ke-53, November-Desember 2004, Basis : Yogyakarta, 2004, hal. 4-5.

Sebagaimana akar pemikiran kritis Mazhab Frankfurt, Habermas juga berangkat dari kritisisme Marx dari karya Marx maupun karya-karya para pendukung pemikiran Marx. Sebagaimana pendahulunya, ia ingin menyesuaikan pemikiran Marx dengan tuntunan-tuntunan zaman. Habermas menilai bahwa teori-teori Marxis yang berkembang sebelumnya sudah kadaluwarsa dan tidak lagi sesuai dengan perkembangan zaman, Habermas ingin menegaskan kembali agar akar teori-teori itu dapat terus mendorong adanya *praxis*.

Dari Goerg Lukacs, Habermas mengambil paham "reifikasi", tetapi bersama Horkheimer dan Adorno ia menyadari bahwa harapan Lukacs tentang reifikasi yang akan didobrak oleh revolusi proletariat tidak didukung oleh kenyataan. Dalam analisanya terhadap teori revolusi Marx, Habermas lalu untuk pertama kali mengajukan sebuah kritik yang akan terus dikembangkannya: Bahwa Marx mengabaikan satu dari dua tindakan dasar manusia, komunikasi.[104] Hal inilah yang kemudian terus menjadi ide besar Habermas tentang teori tindakan komunikatif.

Dalam era yang disebut sebagai Spätkapitalismus atau "kapitalisme-lanjut", Habermas melihat bahwa Marxisme klasik tidak lagi mampu menghadapi lawannya, kapitalisme sudah tidak seperti pada masa lalu. Untuk itu Habermas mengajukan empat alasan. Pertama, berbeda dari zaman kapitalis liberal saat ekonomi menentukan kebijakan politik, dewasa ini, karena intervensi negara terhadap pasar, politik bukan lagi merupakan

[104] *Ibid*., hal. 5-6. Dalam penjelasan ini, lebih lanjut Franz menerangkan, bahwa sebenarnya 'komunikasi' sudah dibahas Marx dalam *dialektika antara teori dan praxis*. Tetapi kemudian Marx mengalami 'salah pahan saintistik', sehingga ia tidak bisa mengintegrasikan lagi komunikasi ke dalam teorinya, karena analisa perkembangan masyarakat Marx semata-mata berfokus pada bidang produksi, analisa ini tidak memadai.

"superstruktur". Pengandaian dasar Marx bahwa basis ekonomi menentukan superstruktur kesadaran menjadi tidak relevan. Kedua, perkembangan standar hidup dewasa ini sudah bagitu jauh, sehingga revolusi tidak lagi dapat dikobarkan melalui istilah ekonomi. Dewasa ini juga telah terjadi kompromi kelas sosial, sehingga antagonisme kaum buruh dan kapitalis ala Marxisme itu juga menjadi tidak relevan, karena kecemburuan sosial tidak lagi hanya dirasakan oleh kaum buruh, tetapi juga kelas sosial lain. Ketiga, karena itu, kaum proletar tidak dapat lagi dijadikan tumpuan harapan agen perubahan. Perjuangan kelas pada taraf nasional sudah distabilkan, tetapi sebagai gantinya, terjadi ketegangan global antar negara-negara kapitalis dan komunis. Keempat, berdirinya raksasa Uni Soviet memadamkan diskusi kritis mengenai Marxisme sehingga Marxisme lambat laun kehilangan daya tariknya sebagai ilmu.[105]

#### 2.5.3.2 Pengetahuan dan Kepentingan

Perdebatan populer pada tahun 1961 di Universitas Tubingen antara dua tokoh berlawanan dalam satu seminar, Theodor Wiesengrund Adorno dan Karl Popper,[106] bisa menjadi

[105] F. Budi Hardiman, *Menuju Masyarakat Komunikatif*, (Yogyakarta: Kanisius, 2009), hal. 79. Lihat juga pada: Fransiskus Budi Hardiman, *Kritik Ideologi*, (Yogyakarta: Buku Baik, 2004), hal. 90-91.

[106] Popper terkenal dengan konsep falsifikasi dan falsibilitasnya dalam upaya pemecahan masalah rasional-empiris, pemikiran Popper tidak searang dengan Sekolah Frankfurt karena ia sudah anti Marxis sejak muda, dan latar belakang ilmu pastinya mendorong kepada pemikiran positivisme logis yang jelas bertentangan dengan Mazhab Frankfurt yang menolak saintisme. Terlebih pemikiran Popper menyatakan bahwa teori sama dengan logika dan itu dapat dipisahkan dari praxis, sedangkan Mazhab Frankfurt yang terkenal dengan Sosiologi Kritisnya senantiasa berupaya mendorong bagaimana teori dapat menjadi praxis. Berbeda dengan Filsafat Lingkungan Wina yang populer dengan asas verifikasinya, Popper mengkritiknya, baginya, hipotesis-hipotesis justru harus dibuktikan kesalahannya dan hipotesis yang tidak gugur kemudian diperkuat (Lihat: Fransiskus Budi Hardiman, *Kritik Ideologi*, (Yogyakarta: Buku Baik, 2004), hal. 16-17). Nampaknya pemikiran Popper dan perlawanannya terhadap Mazhab Frankfurt ini seiring dengan pandangannya bahwa Frankfuters cenderung ideologis atau menurut dia dogmatis dan dia lebih bersifat kritis. Namun para pendukung teori Popper bagaimanapun adalah para ahli dalam ilmu-ilmu pasti, kenyataannya grand designnya adalah sebuah solusi dalam upaya pemecahan masalah logika, maka dikatakan ia adalah seorang

satu contoh perdebatan pemikiran tentang adanya akar kepentingan/orientasi dalam sejarah dan perkembangan pengetahuan.

Popper menyusun tuduhan bahwa filsafat sejarah sebagaimana diuraikan oleh Marx dan Hegel, yang di dalamnya dijelaskan tentang hukum perkembangan dan tujuan objektif. Popper menyatakan semestinya sejarah bersifat faktual semata jangan ditata dengan *grand design*, menurutnya filsafat dengan yang memandang adanya grand design justru menjadikannya semacam ideologi. Popper menyatakan sebaiknya masyarakat ditata dengan menangani permasalahan secara *piecemeal*, dengan menangani masalah-masalah yang muncul langkah kecil demi langkah kecil. Sebaliknya, pihak Adorno dan Horkheimer menyanggah, bahwa justru penanganan yang "bebas nilai" itulah yang ideologis karena tidak menyadari bahwa "objektivitas" itu justru layar asap kepentingan-kepentingan terselubung. Pemikiran Popper yang demikian ini dianggap contoh pendekatan yang menghasilkan "*rasionalitas dalam detil, irrasionalitas dalam keseluruhan.*"[107]

Kant telah menjadi tonggak pemikiran kritis terhadap kepentingan dalam pengetahuan, melepaskan pengetahuan dari kepentingan-kepentingan di luar pengetahuan itu sendiri, kita kenal dengan kritisisme Kant. Hegel, Marx dan Freud juga memberikan modal kritis dalam pemikiran Habermas dalam filsafat ilmu pengetahuan. Lebih lanjur, Habermas mencoba untuk merumuskan dua arti *Kritik*.

---

penganut rasionalisme kritis (Lihat: Alfons Taryadi, *Epistemologi Pemecahan Masalah: Menurut Karl R. Popper*, (Jakarta: Gramedia, 1991)).

[107] Franz Magnis-Suseno, 75 Tahun Jurgen Habermas, dalam Majalah Basis, Nomor 11-12, Tahun ke-53, November-Desember 2004, Basis : Yogyakarta, 2004, hal. 6.

Arti Kritik yang pertama diambil dari transendentalisme Kant. Kritik dalam arti ini adalah suatu refleksi atas syarat-syarat kemungkinan dari pengetahuan, perkataan dan tindakan kita sebagai subyek yang mengetahui, berbicara dan bertindak. Kritik dalam arti ini disebut Habermas sebagai "*rekonstruksi rasional*". Arti kritik yang kedua diambil dari idealisme Hegel dan materialisme Marx. Kritik dalam arti ini adalah suatu refleksi atas hambatan-hambatan yang dihasilkan secara tak sadar yang menyebabkan subyek (pribadi maupun kelompok sosial tertentu) menundukkan diri kepadanya dalam proses pembentukan-dirinya. Habermas menyebut kritik dalam arti kedua ini sebagai 'Refleksi-diri'. Jika Hegel dan Marx melakukan kritik dalam arti ini terhadap bentuk-bentuk kesadaran sosial (secara idealis atau materialistis), Habermas melakukannya terhadap filsafat ilmu pengetahuan yang berkembang di dalam masa-masa awal positivisme modern. Dengan kata lain, kritik adalah refleksi atas kesadaran palsu.[108]

#### 2.5.3.3 Etika Diskursus

Diskursus adalah bentuk komunikasi reflektif dengan *niveau* yang tinggi dengan menggunakan argumentasi rasional untuk mencapai suatu konsensus tanpa paksaan. Berbeda dari komunikasi naif sehari-hari yang mengandaikan kebenarannya begitu saja, diskursus adalah bentuk komunikasi yang muncul pada saat sesuatu diproblematisasikan. Problematisasi itulah yang merangsang para peserta komunikasi untuk mengeluarkan klaim-klaim kesahihan, seperti: klaim kebenaran, ketepatan, atau kejujuran dari pernyataan-pernyataannya.[109]

---

[108] Budi Hardiman, *op.cit.*, hal. 234-235.
[109] F. Budi Hardiman, *Filsafat Fragmentaris*, (Yogyakarta: Kanisius, 2007), hal. 119.

Dalam sebuah masyarakat demokratis, praksis diskursus itu akan membangun suatu sikap yang menghargai kekuatan argumentasi yang lebih baik sehingga berbagai manipulasi "ideologis" itu sendiri pada gilirannya akan diperiksa secara publik dalam arena diskursus rasional yang bersifat publik. Klaim-klaim kesahihan yang dimunculkan dalam diskursus berfungsi kritis terhadap pernyataan-pernyataan yang dikeluarkan oleh para peserta diskursus.[110]

Franz Magnis-Suseno menambahkan pembahasan mengenai etika di dalam konteks diskursus. Etika diskursus berusaha menjawab pertanyaan "apa yang adil?" jika di dalam masyarakat yang homogen bisa jadi jawabannya akan bersumber dari tradisi moral atau mengacu pada ajaran agama. Tetapi masyarakat-masyarakat sekarang makin pluralis, mereka terdiri atas komunitas-komunitas dengan pandangan berbeda. Bahkan di komunitas yang sama pertanyaan moral sering sudah dijawab secara berbeda. Itulah situasi etika diskursus. Menurut Habermas, apakah sebuah normadapat diberlakukan secara universal hanya dapat dipastikan dalam sebuah diskursus di mana semua yang bersangkutan terlibat. Itulah inti etika diskursus.[111]

#### 2.5.3.4 Demokrasi Deliberatif

Demokrasi dan kekuatannya dalam menentukan keputusan politis bagi pusat kekuasaan masih tetap terikat oleh adanya diskursus praktis yang dapat menjadi legitimasi publik terhadap kebijakan penguasa.

Untuk mewujudkan himbauan teori klasik tentang demokrasi itu, Habermas mencoba menghubungkan pendiriannya dengan keadaan-keadaan empiris masyarakat-masyarakat dewasa

[110] *Ibid*.
[111] Magnis-Suseno, *op.cit.*, hal. 10-11.

ini. Struktur-struktur komunikasi yang terkandung di dalam konstitusi negara hukum demokratis dimengerti oleh Habermas sebagai sebuah proyek yang belum selesai namun dapat diwujudkan. Akan tetapi agar keadaan-keadaan empiris masyarakat-masyarakat kompleks itu dapat didekatkan pada tujuan proyek itu haruslah ada sebuah model yang sesuai untuk demokrasi, sebuah model yang secara sosiologis dapat menjelaskan dinamika komunikasi politis di dalam negara hukum demokratis yang ada. Model yang sesuai dengan konsep proseduralistis tentang negara hukum itu adalah model demokrasi deliberatif (deliberative demokratie). Model deliberatif ini menekankan pentingnya prosedur komunikasi untuk meraih legitimasi hukum di dalam sebuah proses pertukaran yang dinamis antara sistem politik dan ruang publik yang dimobilisasi secara kultural. Dalam model demokrasi deliberatif ini Habermas mencoba untuk menghubungkan tesis hukumnya, yakni tesis tentang fungsi hukum sebagai medium integrasi sosial, dengan sebuah teori sosiologis tentang demokrasi. Hasilnya menarik: konsep-konsep dasarnya seperti konsep tindakan komunikatif, *Lebenswelt* (dunia-kehidupan) dan diskursus praktis sekarang beroperasi di dalam kerangka sebuah teori demokrasi.[112]

### 2.5.4 Konsep Opini Publik Jurgen Habermas

Pembahasan tentang 'Konsep Ruang Publik' ini dibahas secara khusus di dalam satu bab terakhir dari *Ruang Publik,*[113] "Bab VII: Perihal Konsep Ruang Publik". Habermas dalam pembukaan bab ini langsung mendistingsikan pembahasan dengan fokus pada peran "Opini Publik sebagai Fiksi Hukum Konstitusional –dan Likuidasi Sosial-Psikologis

[112] F. Budi Hardiman, *Demokrasi Deliberatif: Menimbang 'Negara Hukum' dan 'Ruang Publik' dalam Teori Diskursus Jurgen Habermas*, (Yogyakarta: Kanisius, 2009), hal. 126-127.

[113] Jurgen Habermas, Ruang Publik, Sebuah Kajian Tentang Kategori Masyarakat Borjuis, Kreasi Wacana: Yogyakarta, 2010.

Konsep Opini Publik". Pembahasan yang memperlihatkan sisi kritis sosial dan sekaligus upayanya untuk menunjukkan bahwa konsep kritis sosial semestinya dibawa menuju ke dalam bentuk *praxis*. Dan menurut Habermas, adalah hukum.

Sepanjang kajiannya tentang kategori masyarakat borjuis dalam bukunya 'Ruang Publik' tersebut, Habermas berusaha menjelaskan konstinuitas semangat pencerahan selepas Revolusi Perancis dalam konsistensinya tentang kajian masyarakat modern. Dan yang terlihat jelas adalah bagaimana ia menceritakan tentang proses pembauran kelas borjuis dengan warga terdidik yang memiliki sikap kritis terhadap kerajaan (Inggris) melalui kafe-kafe atau salon-salon. Melalui para kritikus sosial dengan latar belakang pendidikan yang baik inilah mereka yang proletar mendapatkan pembelaan haknya untuk bersuara melalui para terdidik ini, yang oleh Habermas lebih didefinisikan sebagai kelas menengah terdidik.

Habermas membedakan publisitas berkaitan dengan opini publik, atau dengan kata lain 'publisitas manipulatif' dengan 'publisitas kritis'. Ia menjelaskan bahwa masing-masing memiliki tempatnya sendiri-sendiri di dalam konfigurasi sosial, walaupun konsekuensi fungsionalnya bersilangan satu sama lain. Kendati demikian, keduanya mengharapkan publik untuk bertindak dengan cara yang berbeda satu sama lain. Dengan menggunakan distingsi seperti telah diuraikan sebelumnya, bisa dikatakan bahwa salah satunya berpijak pada premis opini publik, sementara yang lain pada premis nonpublik.[114]

Meskipun di dalam kerangka hukum konstitusional dan ilmu politik, analisis mengenai norma-norma konstitusional yang berkenaan dangan realitas konstitusional mayoritas negara demokratis yang menjalankan hak-hak sosial secara terpaksa. Akan tetapi bagi sebagian negara-kesejahteraan sosial yang demokratis masih membutuhkan opini publik secara

[114] Jurgen Habermas, *Ruang Publik: Sebuah Kajian tentang Kategori Masyarakat Borjuis* (*Public Sphere: An Inquiry into a Category of Borgeois Society*), diterjemahkan oleh Yudi Santoso, (Yogyakarta: Kreasi Wacana, 2010), hal. 328.

menyeluruh dengan pertimbangan, karena opini publik masih merupakan satu-satunya basis yang bisa diterima bagi legitimasi dominasi politis. Opini publik secara menyeluruh kemudian menjadi kebutuhan sebuah negara demokrasi modern untuk menerapkan konstitusi yang mengikat secara menyeluruh.[115]

> *"The modern state resupposes as the principle of its own truth the sovereignty of the people, and this in turn is supposed to be public opinion. Without this attribution, without the substitution of public opinion as the origin of all authority for decisions binding the whole, modern democracy lacks the substance of its own truth."*[116]

Habermas memberikan gambaran situasi saat keadaan ruang publik yang ambruk dan kepercayaan naif terhadap ide nasionalisasi kekuasaan tidak dapat terlepas dari fakta itu. Maka Habermas menjelaskan bahwa, pada saat itulah jalan menuju pendefinisian konsep opini publik jadi terbentang jelas. Yang dijelaskan dalam dua jalan pendefinisian:

*Jalan pertama*, membawa kepada posisi liberalisme, yang di tengah-tengah ruang publik yang terpecah belah, ingin menyelamatkan komunikasi internal lingkaran para wakil rakyat yang mengkonstitusikan sebuah publik dan membentuk opini, yaitu kepada publik yang berdebat kritis di tengah-tengah publik yang hanya memberikan persetujuan. Di dalam proses ini kualifikasi yang dulunya milik masyarakat privat di ruang perniagaan dan kerja sosial sebagai kriteria sosial bagi keanggotaan di dalam publik, telah berubah menjadi kualitas perwakilan yang hirarkis dan otonom sehingga basis lama publisitas tidak lagi terpahami.[117] Habermas hendak menjelaskan, bahwa saat ada kekacauan opini di dalam publik, yang tidak lagi berbentuk opini-opini besar yang berdebat di ruang keterwakilan tidak

---

[115] Jurgen Habermas, *Ruang Publik: Sebuah Kajian tentang Kategori Masyarakat Borjuis* (*Public Sphere: An Inquiry into a Category of Borgeois Society*), diterjemahkan oleh Yudi Santoso, (Yogyakarta: Kreasi Wacana, 2010), hal. 328-329.

[116] Jurgen Habermas, *The Structural Transformation of The Public Sphere: An Inquiry into a Category of Bourgeois Society*, (Cambridge: MIT Press, 1993), hal. 237-238.

[117] Jurgen Habermas, *Ruang Publik: Sebuah Kajian tentang Kategori Masyarakat Borjuis* (*Public Sphere: An Inquiry into a Category of Borgeois Society*), diterjemahkan oleh Yudi Santoso, (Yogyakarta: Kreasi Wacana, 2010), hal. 330.

lagi mudah dipahami dengan pengamatan. Kemudian dengan cara mengembalikan perdebatan itu kepada masyarakat dan memberikan kesempatan bagi opini publik untuk berjuang lebih keras dalam memulihkan kesadaran komunikatif. Sehingga hasil pasca-liberalisasi ini akan menjadi penyelamatan tindakan komunikasi dalam lingkaran wakil rakyat.

Akan tetapi liberalisasi ini tidak dapat mengembalikan keadaan atau pola publisitas sebagaimana bentuk awalnya dalam ruang publik. Karena liberalisasi ini pastilah akan mengambil langkahnya yang lebih efektif, yaitu untuk memperoleh otoritas kepatuhan lewat pandangan yang diadopsi hanya dari mereka yang "relatif cukup informatif, cerdas dan bermoral" [kutipan dari W.Hennis oleh Habermas]. Dan Habermas juga melihat indikasi tidak dapat dikajinya keterwakilan yang semacam ini pada kondisi-kondisi yang ada sekarang.

Selanjutnya *jalan kedua*. Jalan kedua mengarahkan kita kepada konsep opini publik yang mencabut kriteria material seperti rasionalitas dan perwakilan penuh dari pertimbangan yang matang dan membatasinya hanya kepada kriteria institusional saja. Opini publik semacam ini bisa eksis menjadi 'publik' hanya ketika diproses melalui partai. Habermas sependapat bahwa opini publik memang berkuasa tetapi tidak memerintah dan parlemen sebagai corongnya tidak secara tepat menjadi corongnya karena aktor-aktor yang bertikai adalah selalu partai, baik partai pemerintah maupun oposisi. Partai yang merangkul mayoritas dianggap mewakili opini publik.[118] Habermas menyimpulkan dari dua model tersebut, semakin organisasi independen dari pemobilisasian dan pengintegrasian opini masyarakat, semakin jauh dia dari peran politis dalam pembentukan konsensus opini publik dalam ruang demokrasi.

Dengan demikian, sebagai fiksi hukum konstitusional, opini publik tidak lagi diidentikkan dengan tingkah laku aktual publik. Namun begitu,

[118] *Ibid*., hal. 331.

kendati opini dilekatkan kepada lembaga-lembaga politik pun (yang diabstraksikan bersama-sama dengan tingkah laku publik) tidak juga menghilangkan karakter fiktifnya. Penelitian sosial empiris akan menemui jalan buntunya kaum positivis ketika hendak menyusun definisi 'opini publik' yang tepat. Mengapa? Karena penelitian tersebut akan mengabstraksikan definisi 'opini publik' dari aspek-aspek institusionalnya, padahal tindakan yang demikian akan segera melikuidasi karakter sosio-psikologisnya.[119] Optimisme Habermas dalam upayanya membawa modernisme dan semangat pencerahan pasca-revolusi perancis, salah satunya dengan mengembangkan kerangka kritisnya yang berkembang dari Kant, Hegel, Marx, dan Freud sebagai basis pemikiran kritis Frankfurtnya. Yang kemudian ia pertemukan dengan pemikiran-pemikiran politik serta sosial terkini terutama dalam membahas secara khusus mengenai opini publik.

Mula-mula 'publik', memang subjek opini publik, dipersamakan dengan 'massa', lalu dengan 'kelompok', kemudian sebagai substratum sosial-psikologis bagi proses komunikasi dan interaksi antara dua individu atau lebih. 'kelompok' diabstraksikan dari serangkaian kondisi sosial dan historis, serta alat-alat institusional, dan tentunya dari jaringan-jaringan fungsi sosial yang dulu pernah jadi penentu strata masyarakat privat yang bergabung membentuk publik yang berdebat kritis di wilayah politis. Opini bukan hanya mencakup kebiasaan yang terekspresikan di dalam konsep-konsep tertentu –misalnya opini yang berbentuk agama, kebiasaan, adat istiadat, atau hanya sekadar 'prasangka', yang untuk menentang hal-hal inilah, opini publik dimunculkan sebagai standar kritik abad ke-18—namun juga segala mode tingkah laku.[120]

Sementara itu, Lazarsfeld sudah menegaskan bahwa terlalu tinggi harga yang harus dibayar bagi konsep sosio-psikologis opini publik apabila

[119] *Ibid*., hal. 332.
[120] *Ibid*., hal. 334.

semua elemen sosiologis dan kesipilannya (*politological*) yang esensial harus dihilangkan. Namun tahapan yang lebih signifikan menuju sintesis antara konsep opini publik klasik dengan representasi sosial-psikologisnya hanya bisa tercapai dengan menyorot lagi soal relasi penuh-paksaan dengan lembaga-lembaga politik berkuasa. Sama seperti konsep opini publik yang berorientasi pada lembaga pemegang kekuasaan politis yang tidak pernah sampai menyentuh dimensi proses komunikasi informal, demikian pula konsep opini publik yang basis sosiopsikologisnya telah direduksi menjadi hubungan-kelompok tidak akan lagi berkaitan dengan dimensi tersebut, walaupun dulu pernah menjadi kategori untuk mengembangkan fungsi strateginya. Pereduksian ini terus bertahan sampai sekarang, membuat kehidupan yang terasingkan (*recluse*) tidak lagi dianggap serius bagi para sosiolog: persisnya dia telah berlaku sebagai fiksi hukum konstitusional.[121]

Dengan demikian hubungannya dengan kekuasaan hanyalah tambahan bagi latar belakangnya saja. Keinginan-keinginan 'privat' untuk memiliki mobil dan pendingin ruangan, misalnya, dimasukkan ke bawah kategori 'opini publik' karena banyak berkaitan dengan tingkah laku kelompok tertentu, seolah-olah keinginan ini relevan dengan fungsi pemerintahan dan administratif negara-kesejahteraan sosial.[122]

#### 2.5.4.1 Klarifikasi Sosiologis Opini Publik *a la* Habermas

> Bahan-bahan material penelitian opini –yaitu semua jenis opini yang digunakan oleh segala jenis kelompok populasi— belum dapat dikukuhkan sebagai opini publik lantaran masih menjadi objek pertimbangan, putusan dan tindakan-tindakan politis. Kriteria untuk mengukur opini secara empiris menurut tingkat kepublikannya dikembangkan berdasarkan evolusi negara dan masyarakat sendiri. Sesungguhnya, spesifikasi empiris opini publik semacam itu dewasa ini telah menjadi pengertian yang

[121] *Ibid*., hal. 335-336.
[122] *Ibid*., hal. 337.

paling terpercaya untuk memperoleh pertanyaan yang valid dan adil mengenai tingkatan integrasi demokratis yang menjadi ciri realitas konstitusional.[123]

Opini-opini informal berbeda dalam tingkatan-tingkatan kewajiban mereka. Pada tingkatan pertama, semakin rendah tataran wilayah komunikasi direpresentasikan oleh verbalisasi hal-hal yang secara kultural diterima begitu saja (*taken for granted*) tanpa didiskusikan, semakin tinggi perlawanan yang dihasilkan oleh proses akulturasi tersebut, yang biasa tidak dikontrol bahkan oleh refleksi individu itu sendiri –seperti contoh, tingkah laku terhadap hukuman mati atau moralitas seksual. Pada tingkatan kedua, pengalaman-pengalaman biografis mendasar yang jarang didiskusikan mulai diverbalisasikan, sehingga akibat-akibat tak tertahankan dari kejutan sosialisasi sekali lagi menjadi subreflektif –seperti contohnya, sikap-sikap terhadap perang dan damai atau hasrat-hasrat tertentu akan rasa aman. Dan akhirnya, pada tataran ketiga, kita menemukan bahwa hal-hal yang sering didiskusikan muncul sebagai sesuatu yang jelas dengan sendirinya bagi industri budaya, yang hasilnya adalah serbuan pemberitaan dan manipulasi propaganda tanpa henti oleh media terhadap konsumen, dan yang jadi target utamanya adalah waktu luang mereka.[124]

> *Over and against the communicative domain of nonpublic opinion stands the sphere of circulation of quasi-public opinion. These formal opinions can be traced back to specific institutions; they are officially or semiofficially authorized as announcements, proclamations, declarations, and speeches*.[125]

Kendati opini-opini kuasi-resmi ini bisa ditunjukkan kepada publik luas, tetap saja mereka tidak memenuhi persyaratan proses

[123] *Ibid*., hal. 337-338.
[124] *Ibid*., hal. 338-339.
[125] Jurgen Habermas, The Structural Transformation of The Public Sphere: An Inquiry into a Category of Bourgeois Society, MIT Press: Cambridge, 1993, hal. 237-238.

publik bagi perdebatan rasional kritis menurut model liberal. Karena sahih secara institusional, opini kuasi-resmi selalu diistimewakan sehingga sama sekali tidak berimbang dengan masa 'publik- tak-terorganisasi. Kita juga dapat melihat bahwa wahana pewartaan ini, bila dikelola dengan baik, bisa memengaruhi opini-opini formal yang ada –namun sebagai sesuatu yang 'termanifestasikan secara publik', publisitas yang ini harus dibedakan dari opini 'kuasi-publik'.[126]

Lantaran terperangkan di dalam pusaran *publisitas yang dipanggungkan bagi tontonan atau manipulasi*, maka klaim yang dilontarkan publik masyarakat privat tak-terorganisasi sesungguhnya dibentuk bukan melalui komunikasi publik melainkan lewat komunikasi opini-opini yang termanifestasikan secara publik. Akan tetapi, opini baru bisa menjadi publik dalam maknanya yang ketat apabila dilahirkan di suatu tataran di mana dua wilayah komunikasi di atas dijembatani oleh pihak ketiga, yaitu *publisitas kritis*.[127]

> *For a sociological theory of public opinion this tendency is nevertheless of decisive importance, for it provides the criteria for a dimension in which alone public opinion can be constituted under the conditions of a large democratic state commited to social rights.*[128]

Derajat bagi sebuah opini boleh disebut sebagai publik juga bisa diukur lewat standar berikut: seberapa besar dia muncul dari ruang publik intraorganisasional yang dibentuk oleh publik anggota-anggota organisasi dan seberapa banyak rung publik intraorganisasional berkomunikasi dengan ruang publik eksternal

---

[126] Jurgen Habermas, *Ruang Publik: Sebuah Kajian tentang Kategori Masyarakat Borjuis* (*Public Sphere: An Inquiry into a Category of Borgeois Society*), diterjemahkan oleh Yudi Santoso, (Yogyakarta: Kreasi Wacana, 2010), hal. 341.

[127] *Ibid*., hal. 342.

[128] Jurgen Habermas, The Structural Transformation of The Public Sphere: An Inquiry into a Category of Bourgeois Society, MIT Press: Cambridge, 1993, hal. 248.

yang terbentuk lewat pertukaran pewartaan, yaitu via media massa, antara organisasi kemasyarakatan dan institusi-institusi negara.[129]

C.W. Mills mendefinisikan opini publik: "Di dalam sebuah *publik*, seperti yang kita pahami dengan istilah ini, (1) 'opini publik' adalah opini yang banyak diungkapkan oleh masyarakat sekaligus yang banyak diterima oleh masyarakat sendiri. (2) Komunikasi publik begitu tertata, sampai-sampai jawaban-balik terhadap opini apa pun yang diungkapkan di dalam publik bisa dilakukan dengan cepat dan efektif. Opini yang dibentuk oleh diskusi semacam itu (3) sudah memiliki landasannya di dalam tindakan efektif, yang bila diperlukan dapat menentang sistem otoritas yang ada. Dan akhirnya, (4) institusi-institusi otoritatif tidak menginfiltrasi publik, sehingga publik kurang lebih menjadi otonom dalam mengoperasikan opini mereka. Empat kriteria komunikasi *massa* ini baru terpenuhi ketika wilayah informal kemunikasi dikaitkan dengan wilayah formalnya melalui saluran-saluran publisitas yang dipentaskan demi tujuan manipulasi atau tontonan semata. Kalau begitu, dengan "penyebaran budaya industri yang tak terelakkan" ini, opini nonpublik diintegrasikan lewat opini yang "termanifestasikan secara publik" menjadi sistem seperti yang kita miliki sekarang. Di dalam sistem yang seperti ini, opini nonpublik tidak memiliki otonomi apa pun.[130]

#### 2.5.4.2 Peran Opini Publik dalam Negara Demokratis

Demokrasi dan kekuatannya dalam menentukan keputusan politis bagi pusat kekuasaan masih tetap terikat oleh adanya

---

[129] Jurgen Habermas, *Ruang Publik: Sebuah Kajian tentang Kategori Masyarakat Borjuis* (*Public Sphere: An Inquiry into a Category of Borgeois Society*), diterjemahkan oleh Yudi Santoso, (Yogyakarta: Kreasi Wacana, 2010), hal. 343.

[130] *Ibid*., hal. 344.

diskursus praktis yang dapat menjadi legitimasi publik terhadap kebijakan penguasa.

Untuk mewujudkan himbauan teori klasik tentang demokrasi itu, Habermas mencoba menghubungkan pendiriannya dengan keadaan-keadaan empiris masyarakat-masyarakat dewasa ini. Struktur-struktur komunikasi yang terkandung di dalam konstitusi negara hukum demokratis dimengerti oleh Habermas sebagai sebuah proyek yang belum selesai namun dapat diwujudkan. Akan tetapi agar keadaan-keadaan empiris masyarakat-masyarakat kompleks itu dapat didekatkan pada tujuan proyek itu haruslah ada sebuah model yang sesuai untuk demokrasi, sebuah model yang secara sosiologis dapat menjelaskan dinamika komunikasi politis di dalam negara hukum demokratis yang ada. Model yang sesuai dengan konsep proseduralistis tentang negara hukum itu adalah model demokrasi deliberatif (*deliberative Demokratie*). Model deliberatif ini menekankan pentingnya prosedur komunikasi untuk meraih legitimasi hukum di dalam sebuah proses pertukaran yang dinamis antara sistem politik dan ruang publik yang dimobilisasi secara kultural. Dalam model demokrasi deliberatif ini Habermas mencoba untuk menghubungkan tesis hukumnya, yakni tesis tentang fungsi hukum sebagai medium integrasi sosial, dengan sebuah teori sosiologis tentang demokrasi. Hasilnya menarik: konsep-konsep dasarnya seperti konsep tindakan komunikatif, *Lebenswelt* (dunia-kehidupan) dan diskursus praktis sekarang beroperasi di dalam kerangka sebuah teori demokrasi.[131]

Sebagai konsep dalam teori diskursus, istilah ‘demokrasi deliberatif’ sudah tersirat di dalam apa yang telah kita bicarakan di

[131] F. Budi Hardiman, *Demokrasi Deliberatif: Menimbang ‘Negara Hukum’ dan ‘Ruang Publik’ dalam Teori Diskursus Jurgen Habermas*, (Yogyakarta: Kanisius, 2009), hal. 127.

atas sebagai diskursus praktis, formasi opini dan aspirasi politis (*politische Meinungs-und Willenbildung*), proseduralisme atau kedaulatan rakyat terhadap prosedur (*Volksouveränität als Verfahren*). Akan tetapi kali ini kita mengarahkan pandangan kita tidak lagi pada ide negara hukum, melainkan lebih pada proses legitimasi itu sendiri. Teori demokrasi deliberatif tidak memusatkan diri pada penyusunan daftar aturan-aturan tertentu yang menunjukkan apa yang harus dilakukan oleh warganegara, melainkan pada prosedur untuk menghasilkan peraturan-peraturan itu.[132]

Dengan kata lain model demokrasi deliberatif meminati persoalan kesahihan keputusan-keputusan kolektif itu. Pada hemat saya model ini dapat secara memadai menjelaskan arti kontrol demokratis melalui opini publik. Opini-opini publik bisa jadi merupakan opini-opini mayoritas yang mengklaim legitimasi mereka. Opini-opini itu juga dapat memiliki suatu bentuk yang logis dan koheren yang dianggap sahih secara universal dan rasional. Akan tetapi opini-opini mayoritas tidak niscaya secara identik dengan opini-opini yang benar. Bagi model demokrasi deliberatif adalah jauh lebih penting memastikan *dengan cara manakah* opini-opini mayoritas itu terbentuk sedemikian rupa sehingga seluruh warganegara dapat mematuhi opini-opini itu.[133]

#### 2.5.4.3 Peran Opini Publik dalam Pembentukan Hukum

Ada beberapa aspek yang menajamkan pendirian politik deliberatif Habermas:

*Pertama*, seperti pemulis-penulis lainnya, Habermas juga mementingkan aturan-aturan main demokratis, jaminan hak-hak kebebasan, adanya partai-partai yang berkompetisi, pemilihan

[132] *Ibid*., hal. 128.
[133] *Ibid*., hal. 129.

umum yang *fair*, asas mayoritas, debat publik dst. Menurutnya bila demokrasi deliberatif juga menekankan pentingnya dan arti normatif prosedur demokratis, ia tidak boleh merasa cukup dengan aturan-aturan empiris seperti itu. Hal ini berarti bahwa kondisi-kondisi komunikasi yang memungkinkan konsensus intersubjektif di antara para warganegara selalu saja tetap bersifat kontrafaktual di harapan jalannya komunikasi faktual. Akibatnya sebuah tatanan kekuasaan tidak dapat dilegitimasikan atas dasar berjalannya komunikasi faktual.[134]

*Kedua*, seperti para penulis lain, Habermas mencoba mengembangkan sebuah model demokrasi yang peka terhadap konteks, sebuah model yang memperhitungkan perubahan-perubahan yang telah terjadi di dalam masyarakat-masyarakat kompleks yang terglobalisasi dewasa ini. Habermas justru berupaya untuk menunjukkan bahwa demokratisasi tidak dapat ditanamkan dari luar ke dalam masyarakat-masyarakat kompleks. Demokratisasi berkembang dari dalam masyarakat-masyarakat itu sendiri dan didorong oleh sistem politik yang sudah ada di sana. Ia yakin bahwa rasio komunikatif yang menggerakkan proses-proses demokrasi sudah tersedia di dalam praktik-praktik negara hukum dan institusi-institusi ruang publik yang telah ada. Menurut pendapat saya hal yang sangat penting bagi model demokrasi deliberatif adalah bagaimana potensi-potensi rasionalisasi praktik-praktik negara hukum modern dapat diaktualisasikan.[135]

*Ketiga*, seperti model-model deliberatif lain, model Habermas juga beroperasi dengan ciri-ciri ideal deliberasi, seperti pentingnya bentuk argumentasi, inklusivitas para peserta, kebebasan dari paksaan, pencapaian konsensus dst. Model

[134] *Ibid*., hal. 130-131.
[135] *Ibid*., hal. 131.

Habermas menekankan apa yang disebut "proses deliberasi politik jalur ganda" yang di dalamnya terjadi pembagian kerja antara sistem politik dan ruang publik.[136]

#### 2.5.4.4 Fungsi Kritis Opini Publik Terhadap Sistem Sosial

Dalam kesimpulan sementaranya: "Tindakan Sosial, Tindakan-Bertujuan, dan Komunikasi" dalam buku "Teori Tindakan Komunikatif" pertamanya,[137] Habermas ingin menjawab pertanyaan Weber dalam kajian sosiologi agama yang memunculkan pertanyaan empiris yang cukup panjang. "Mengapa diferensiasi tiga kompleks rasionalitas setelah terjadinya disintegrasi pandangan dunia tradisional belum juga menubuh dalam bentuk institusi dalam tatanan kehidupan masyarakat modern, mengapa ketiganya tidak menentukan praktik komunikatif dalam kehidupan sehari-hari pada tingkat yang sama."[138]

Namun, melalui asumsi tindakan-teoretis dasar ini, Weber mencurigai pertanyaan ini sedemikian rupa sehingga proses rasionalisasi masyarakat hanya dapat dilihat dari sudut pandang rasionalitas bertujuan. Oleh karena itulah saya ingin mendiskusikan kendala-kendala konseptual dalam teori tindakan dan menggunakan kritik ini sebagai pijakan awal untuk analisis lebih lanjut atas konsep tindakan komunikatif.[139]

Karena Weber berangkat dari model tindakan yang dikonsepsikan secara monologis, maka konsep "tindakan sosial" tidak dapat diperkenalkan dengan cara menjelaskan konsep

---

[136] *Ibid*., hal. 132.

[137] Jurgen Habermas, Teori Tindakan Komunikatif (buku satu): Rasio dan Rasionalisasi Masyarakat (*Theorie des Kommunikativen Handeln, Band I: Handlungsrationalitat und gesellschaftliche Rationalisierung*), diterjemahkan oleh Nurhadi, (Yogyakarta: Kreasi Wacana, 2009).

[138] *Ibid*., hal. 335. Akan tetapi dalam pertanyaan panjang tersebut, Habermas tidak memberikan tanda tanya di akhir kalimat tanyanya.

[139] *Ibid*., hal. 335.

makna. Oleh karena itu dia harus memperluas model tindakan bertujuan dengan dua spesifikasi sehingga syarat bagi interaksi sosial dapat terpenuhi: (a) suatu orientasi ke arah perilaku subjek lain yang bertindak, dan (b) suatu relasi refleksi orientasi tindakan resiprokal dari beberapa subjek yang bertindak.[140]

Untuk membangun sebuah teori tindakan, ada hal lain yang lebih penting. Haruskah Weber memperkenalkan aspek rasionalitas tindakan berdasarkan model tindakan teleologis, ataukah justru konsep tindakan sosial yang harus dijadikan dasar rasionalitas tersebut? Untuk kasus yang pertama, Weber harus membatasi dirinya pada aspek rasionalitas yang terikat dengan model aktivitas-aktivitas, yaitu dengan rasionalitas makna dan tujuan. Sedangkan untuk kasus kedua, pertanyaan yang muncul adalah apakah relasi-relasi refleksi orientasi tindakan itu berbeda-beda dan oleh karena itu menjadi aspek tambahan bagi dasar tindakan agar bisa dirasionalisasikan.[141]

Weber tidak mampu membuat tipologi tindakan yang tidak resmi yang dikemukakannya ini bisa bermanfaat bagi problematika rasionalisasi masyarakat. Versi yang resmi, bagaimanapun, dipahami secara sempit sehingga di dalam kerangka kerja tindakan sosialnya hanya dapat dijajagi berdasarkan aspek rasionalitas-bertujuan. Dari perspektif konseptual ini rasionalitas sistem tindakan harus dibatasi pada pembentukan dan perseberan tipe-tipe tindakan rasional-bertujuan yang spesifik bagi berbagai subsistem. Jika rasionalisasi masyarakat akan diteliti secara menyeluruh, maka sangat diperlukan landasan tindakan teoretis.[142]

[140] *Ibid*., hal. 334.
[141] *Ibid*., hal. 345.
[142] *Ibid*., hal. 349.

Dalam kerangka teori rasionalisasi, proses pembentukan diri masyarakat berarti proses menuju "rasionalitas", atau proses menuju otonomi dan kedewasaan (*Mundigkeit*). Oleh karena itu, di samping teori materialisme-sejarah Marxis, teori Rasionalisasi Weber juga mendapat kedudukan penting dalam proyek Teori Kritis untuk menyusun sebuah teori perkembangan masyarakat. Habermas lebih rinci lagi mengkritik modernisasi kapitalis yang memutlakkan rasionalitas kognitif instrumental dalam bentuk kekuasaan politis dan kemakmuran ekonomis yang berpadu dengan hedonisme dan konsumerisme yang menyebabkan erosi makna, karena modernisasi tersebut menindas bentuk rasionalitas lain, yaitu rasionalitas praktis-moral. Masalahnya adalah, dalam masyarakat kapitalis, ketiga bentuk rasionalitas itu tidak dikembangkan secara seimbang.[143]

Di sini kita melihat bahwa Habermas mengambil sikap yang berbeda dari rekan-rekannya dari Mazhab Frankfurt. Bahkan ia juga tidak sepenuhnya setuju dengan Weber. Ilmu dan teknologi yang dicurigai sebagai bentuk penindasan oleh para pendahulunya justru dilihat sebagai faktor penting yang mengemansipasikan masyarakat dari kendala alamiah dan proses obyektif, bahkan teknologi sosial sekalipun dipandang sebagai sebuah kemungkinan untuk perkembangan masyarakat. Tapi Habermas memberi peringatan bahwa semua ini harus dilancarkan secara seimbang dan utuh dengan pengembangan di bidang hukum, moralitas, erotisme, dan seni.[144]

#### 2.5.4.5 Peran Publik dalam Penegakan Hukum Pidana Mayantara: Perspektif Habermas

[143] F. Budi Hardiman, *Menuju Masyarakat Komunikatif: Ilmu, Masyarakat, Politik dan Postmodernisme Menurut Jurgen Habermas*, (Yogyakarta: Kanisius, 2009), hal. 118.

[144] *Ibid*., hal. 118-119.

Pemikiran Jurgen Habermas yang dapat kita gunakan membedah karakter modernitas dalam dunia mayantara dan bagaimana peran ruang publik dalam pembentukan kebijakan hukum dan dalam penegakan hukumnya. Dengan perangkat analisis sosialnya yang kritis kepada realitas masyarakat modern, gagasan masyarakat komunikatif, dan bagaimana Habermas berusaha menciptakan demokrasi mendialogkan hukum dengan konsep diskursusnya. Sebuah ruang bagaimana hukum kolektif yang diciptakan dari kesatuan pengertian tentang keadilan dan bagaimana mengupayakannya dengan komunikasi baik ruang publik maupun ruang privat. Dalam peta pemikiran Habermas, tanpa komunikasi yang intens, atau dengan kata lain, tanpa adanya kepedulian sosial tentang hukum dalam solidaritas yang mengoptimalkan komunikasi sebagai bentuk intimitas, maka masyarakat akan hancur karena fungsi hukum tidak berjalan dengan baik.

Berbeda dengan hukum sipil/keperdataan yang untuk bagian terbesar dipraktikan dalam kehidupan nyata di luar ketelibatan hakim (hal yang sama berlaku pula berkenaan dengan hukum administrasi), *jus puniendi*, dalam hal pengejawantahan, pengakuan dan pengungkapannya dalam realita sangat tergantung pada peradilan. Aturan-aturan yang terkait dengan hal di atas, yaitu yang menunjukkan bagaimana hukum pidana demikian harus direalisasikan (dalam proses peradilan), kita namakan hukum acara pidana (*strafverderingsrecht*), atau juga hukum pidana formil untuk membedakannya dari hukum pidana materiil.[145] Hukum pidana selalu berupaya menyelaraskan

[145] Jan Remmelink, *Hukum Pidana* (*Inleiding tot de Studie van het Nederlanse Strafrecht*), diterjemahkan oleh Tristam Pascal Moeliono, (Jakarta: Gramedia, 2003), hal. 3.

pandangannya dengan kemasyarakatan, segala ketentuan di dalamnya memiliki implikasi sosial.

Jelas bahwa sosiologi, ilmu (tentang) masyarakat, telah menyumbangkan banyak hal yang bagi ahli hukum pidana amat bermanfaat untuk memperkaya wawasan serta pemahaman tentang pelbagai gejala hukum. Terpikirkan adalah 'perbuatan' (tindakan) dan 'culpa', kemampuan mempertanggungjawabkan perbuatan di hadapan hukum (*toerekeningsvatbaarheid*) dari orang-orang yang menderita gangguan jiwa (yang memang harus dinilai dalam konteks sosial). Bahkan juga hukum pidana ekonomi dan hukum pidana lalulintas (*verkeersstrafrecht*) mendapatkan banyak manfaat dari temuan-temuan yang diangkat ke permukaan oleh sosiolog. Akhirnya, dapat dikatakan bahwa sosiologi juga memainkan peran penting dalam menguji dan menilai pengaruh dari pidana (*straffen*) dan tindakan (*maatregelen*).[146]

Lebih lanjut Remellink juga mengkritisi tentang kontrol penuh terhadap masyarakat sebagaimana digagas dalam ajaran psikologi-sosial, *behaviorisme* (pada tahun 1950-an dikembangkan oleh Burrhus Frederic Skinner yang meninggal tahun 1990 di Amerika Serikat) yang tidak lagi mementingkan kebebasan manusia. Meski demikian Remellink tetap menolak kebebasan total terhadap manusia, karena harus diakui bahwa di dalam hukum pidana kita tidak dapat mengabaikan sama sekali dampak peran atau fungsi yang harus dimainkan seseorang dalam pergaulan masyarakat, sekalipun peran itu sangat sederhana. Secara ringkas, Remellink ingin menunjukkan bahwa "kontrol sosial" tidak hanya memanfaatkan mekanisme yang bekerja secara negatif (ke dalamnya sebagai eksponen ekstrem harus dicakupkan sanksi yang dijatuhkan peradilan pidana), melainkan juga yang

[146] *Ibid*., hal. 18-19.

bernuansa positif, seperti: pendidikan, pengajaran dan penerangan (dengan cara ini anggota kelompok menerima nilai-nilai yang bersangkutan sebagai bagian dari dirinya, menyatukan diri dengannya, atau yang dikenal dengan konsep: internalisasi), pelbagai manfaat/pujian dan lain sebagainya.[147]

Diskursus dan prinsip demokrasi deliberatif dalam sosiologi kritis Jurgen Habermas yang menekankan pada prinsip kritik sosial, komunikasi yang berangkat dari intimitas klektif, juga menjelaskan tentang fungsi sosial tiap individu dalam wilayah publik dalam konsensus atas nilai-nilai keadilan. Terdapat beberapa wawasan yang disampaikan dalam pengalaman Habermas sendiri saat bertentangan dengan musuh-musuh pemikirannya.

Saat menghadapi Hans Albert yang mewakili kubu K.R. Popper, Habermas menyanggah pemikiran ala falsifikasi Popper yang tidak mementingkan *grand design* masyarakat tetapi lebih mengutamakan untuk menangani masalah-masalah kecil, karena penolakannya bahwa seakan dengan demikian justru akan membawa pada tujuan ideologis yang mengorbankan manusia. Menurut Habermas, justru dengan cara hanya mengamati hal-hal kecil, maka masyarakat akan tidak menyadari selubung objektifitas yang diam-diam menggiringnya.

Habermas bagaimanapun sadar bahwa ada kekuasaan di dalam pengetahuan manusia/masyarakat yang tidak bebas kepentingan. Bukan pengetahuan yang bebas kepentingan, melainkan pencerahan tentang kepentingan yang mendorong pengetahuan itulah yang membongkar selubung ideologis.[148]

---

[147] *Ibid*., hal. 20.

[148] Franz Magnis-Suseno, 75 Tahun Jurgen Habermas, dalam Majalah Basis, Nomor 11-12, Tahun ke-53, November-Desember 2004, Basis : Yogyakarta, 2004, hal. 6.

Dengan salah satu ‘musuh besarnya’, Niklas Luhmann, yang populer dalam teori sistem dan disebutkan masuk dalam salah satu tokoh sosiologi hukum di dalam *A Primer in the Sociology of Law* karya Dragan Milovanovic, Habermas memberi kritik, bahwa apa yang dilihat Luhman sebagai keniscayaan perkembangan evolusioner sesungguhnya adalah bersifat regresif dan tidak mesti (*unnecessary*). Masyarakat dalam kenyatannya mungkin berkembang menjadi sistem dunia yang terdiferensiasi secara fungsional dan tertutup yang tak mampu bertindak atas nama dunia sosial secara keseluruhan, tetapi ini adalah sesuatu yang harus dilawan. Teori seharusnya dikembangkan untuk membantu mengatasi kecenderungan ini, bukan membuatnya tak terhindarkan, seperti yang dilakukan Luhmann.[149]

Bagaimanapun, meski ada bentuk kolektif untuk dapat menyatakan pendapat masing-masing individu, namun masyarakat tetaplah mesti diatur. Luhmann dengan *autopoiesis*-nya, yang memperlihatkan bahwa masyarakat semisal organ biologis yang dapat memenuhi kebutuhannya untuk mereorganisasi diri dan membentuk kelompoknya, melengkapi diri dengan organ-organ yang diperlukan dengan *auto-reference* pada dirinya sendiri, tetaplah harus diatur. Tidak hanya diamati, didefinisikan secara karakteristik, namun malah terlihat menjadi tidak menentu. Konsistensi Habermas pada pesan pencerahan sejak revolusi Perancis tetap ia pegang teguh, demi membawa visi masyarakat modern yang memiliki kecenderungan lebih baik. Optimisme Habermas pada modernitas menjadikannya demikian realistis terhadap modernisasi, dimana komunikasi dan informasi adalah modal.

[149] George Ritzer dan Douglas J. Goodman, *Teori Sosiologi Modern* (*Modern Sociological Theory*), diterjemahkan oleh Alimandan, (Jakarta: Kencana, cet. Keenam, 2010), hal. 261.

# BAB III

# DINAMIKA SOSIAL MAYANTARA DAN *CYBERCRIME*

## 3.1 Struktur Masyarakat Mayantara

Pengenalan dan pemahaman terhadap bentuk serta karakteristik lingkungan sosial mayantara akan menjadi pendekatan yang baik dalam manyiapkan media untuk melakukan kontrol dan menerapkan peraturan di dalamnya. Dengan memahaminya akan memberikan gambaran fungsional, ruang lingkup, serta laju perkembangan berbagai unsur-unsurnya. Sehingga arah pikir tentang *cyberspace* yang tidak bisa diatur akan dibimbing menuju ke arah optimisme penegakan hukum secara efektif.

Dalam suatu lingkungan sosial, perkembangan akan terjadi saat semakin meningkatnya interaksi di dalamnya yang menghasilkan kesepakatan-kesepakatan baru antar tiap-tiap anggota masyarakat. Dalam *cyberspace* yang terus berkembang, jaringan komunikasi juga akan terus berkembang sesuai dengan meningkatnya kebutuhan yang dibangun di dalamnya, yang memudahkan kerja kita di dunia nyata, yang kini kian diwakilkan menjadi simulasi-simulasi.[150]

Terkadang ketakutan tentang internet dan modernisme membawa kita kepada pemikiran postmodernisme,[151] yang melihat akhir dari modernisme. Semestinya ketakutan tersebut tidak dibahas terlalu jauh ke arah pemikiran yang cenderung bersikap pasif terhadap arus modernisme dengan memandangnya

---

[150] Dalam berbagai kajian tentang *cultural studies* sering dipakai istilah '*simulacrum'* (bentuk jamak dari *simulacra*). Simulasi adalah keserupaan, dalam hal ini adalah kerja nyata telah digeser ke ranah mayantara menjadi simulasi dari bentuk klasiknya, misalkan: transaksi dengan teller bank untuk cek saldo, penarikan dan setoran tabungan, atau pun transfer, dapat disimulasikan dalam ruang internet.

[151] Anthony Giddens mengutip kepada Jean-Francois Lyotard, "Seperti dikatakannya, pascamodernitas mengacu kepada pergeseran dari usaha untuk membumikan epistemologi dan dari keyakinan akan kemajuan yang direkayasa manusia. Kondisi pascamodernitas berbeda dengan menguapnya "narasi agung" –suatu "alur kisah" yang mencakup semua hal yang dengannya kita ditempatkan dalam sejarah sebagai makhluk yang memiliki masa lalu pasti dan masa depan yang dapat diprediksikan. Sudut pandang pascamodern melihat adanya pluralitas klaim pengetahuan yang heterogen, di mana ilmu pengetahuan tidak menduduki posisi istimewa. Lihat Anthony Giddens, *Konsekuensi-Konsekuensi Modernitas (The Consequences of Modernity),* diterjemahkan oleh Nurhadi, (Yogyakarta: Kreasi Wacana, 2009), hal. 2.

seakan tidak terbendung, tidak karuan, di luar kontrol manusia, dan mereduksi peran-peran ilmu pengetahuan. Di sisi lain, semangat modernisme dalam pemikiran Habermas menyokong gagasan, bahwa semestinya modernisme itu memiliki tujuan dan dapat diatur. Dan dengan itulah kita menautkannya kepada hukum, dari semangat penegakan hukum dengan kesadaran hukum yang baiklah ketertiban dalam masyarakat dapat diciptakan.

Teror dari berbagai kejahatan yang berkembang di ruang *cyber* menjadi hal keseharian saat masyarakat menemukan ketergantungannya terhadap *cyberspace* semakin jamak. Kepentingan tentang bagaimana ruang *cyber* itu dibentuk untuk kemaslahatan bersama, dan bagaimana wawasan mengenainya, terus bergerak maju. Modernisme yang membawa arus budaya internet memberikan banyak kemudahan untuk memperoleh pengetahuan.

Setidaknya dari pemahaman sederhana tersebut kita tahu bahwa modernisme dan pengetahuan yang tersebar luas bersamanya adalah bertujuan dan diarahkan, bukan melulu menuju kepada *chaos* dan absurditas masa depan yang semakin tidak jelas. Pada posisi tersebutlah etika internet memberikan andil, mengelola kepada arah dan nilai-nilai bersama yang terus dikembangkan. Kemudian masyarakat yang semakin sadar akan kebutuhannya di dalam internet akan menuntut keterlibatan hukum secara lebih aktual menghadapi permasalahan.

### 3.1.1 Sekilas tentang Sejarah Internet

> *The most pressing question for the future of the Internet is not how the technology will change, but how the process of change and evolution itself will be managed… the architecture of the Internet has always been driven by a core group of designers, but the form of that group has changed as the number of interested parties has grown.* _www.isoc.org.[152]

Komputer tidak diragukan lagi berperan besar dalam menciptakan aktifitas manusia yang lebih cepat, lebih aman, dan lebih menarik. Komputer menciptakan bentuk-bentuk baru dari bekerja dan bermain.

[152] Barry M. Leiner, et.al, "History of The Internet" <http://www.isoc.org/internet/history/brief.shtml#Commercialization>, Diakses pada 16 Desember 2010, pukul 05.00 Wib.

Secara terus-menerus menciptakan ide-ide baru dan menawarkan berbagai keuntungan sosial, meskipun pada saat yang bersamaan komputer juga memberikan peningkatan peluang bagi bahaya sosial.[153] Teknologi komputer terus-menerus berkembang dan terus menciptakan hal-hal baru, dan bersamaan dengan itu kejahatan terus mengiringi secara ketat perkembangan yang diciptakan oleh teknologi komputer.

Menurut data Facebook, pada Desember 2010 pengguna situs jejaring sosial tersebut di tanah air mencapai 25 juta pengguna. Terbesar ketiga di bawah Amerika Serikat dan Inggris. Di situs media sosial lainnya seperti Twitter, pengguna asal Indonesia mencapai 5 sampai 6 juta user. Indonesia juga ada di peringkat ketiga sebagai negara dengan pengguna Twitter terbanyak setelah Amerika Serikat dan Jepang. Pertumbuhan pengguna Internet di Indonesia 49 persen per tahunnya. Sekitar 70 persen di antaranya adalah usia 35 tahun ke bawah.[154] Dari data yang disampaikan tersebut, perkembangan pemanfaatan jaringan sosial internet di Indonesia mengalami peningkatan terus menerus. Kita akan melihat bagaimana perkembangan teknologi komputer mendukung ketat perkembangan internet yang memudahkan orang untuk bersosialisasi tanpa batas negara dan waktu. Dan perkembangan kejahatan yang dibentuk dari kemudahan komunikasi di dalamnya.

Sejarah dari teknologi internet dapat dirunut sejak tahun 1962, sebelum istilah 'internet' ditemukan. Pada masa itu komputer masih dalam bentuknya yang primitif, dan harganya masih ratusan ribu dolar per unitnya, sangat mahal untuk ukuran masa itu. Komputer baru memiliki beberapa ribu kata yang terekam dalam *magnetic core memory*, dan memprogramnya sangat jauh dari kata mudah. Di Amerika Serikat, saat itu

---

[153] George M. Mohay, *Computer and Intrusion Forensics*, (Norwood, MA: Artech, 2003), hal. 1.

[154] Muhammad Firman dan Muhammad Candra Taruna, "2009 Jadi Tonggak Sejarah Internet Indonesia," http://teknologi.vivanews.com/news/read/168958-2009-jadi-tonggak-sejarah-internet-indonesia. diakses pada 15 Desember 2010, Pukul 14.00 Wib. Informasi terbaru dari jejaring sosial Facebook (Februari 2011) telah mencapai 35.000 akun dari Indonesia.

komunikasi data dikelola secara monopolis oleh AT&T begitu juga dalam komukasi secara global. Namun penelitian proyek *Advanced Reseach Project Agency* (ARPA) milik Departemen Pertahanan Amerika Serikat kemudian menjadi sebuah investasi berharga untuk masa depan, penelitian ini mendanai untuk proyek penelitian '*high-risk, high-gain*', yang menjadi tonggak lahirnya ARPANET, dan lebih jauh lagi, inilah awal dari internet.[155] Dari uraian yang lebih panjang dapat disederhanakan bahwa pada era 1960-an adalah era ketika ARPA berkembang menjadi ARPANET dan terus berusaha meluaskan jaringannya.

Semenjak awal 1970-an bermunculan berbagai penemuan di dunia internet, seperti perangkat surat elektronik (*electronic mail*) atau yang biasa disingkat *email,* yang semakin memperluas kemungkinan berkomunikasi. Muncul juga berbagai jaringan yang diparalelkan dengan ARPANET, yang diluncurkan dengan nama seperti JANET (Joint *Academic Network*) milik Inggris dan NSFNET (milik *American National Science Network*) dengan memanfaatkan protokol-protokol komunikasi tertentu, jaringan ini bisa terhubung bersamaan, membentuk sebuah internet, sebuah jaringan dari banyak jaringan.[156]

Seiring dengan pertumbuhan pada sektor-sektor komersial ikut serta membawa peningkatan pada standar pelayanan. Dimulai pada awal 1980-an dan terus berlanjut semenjak itu, internet kian tumbuh melampaui akar-akar dasar penelitiannya dengan melibatkan lebih banyak komunitas pemakai dan juga meningkatkan lebih banyak aktifitas komersial.[157] Perhatian yang lebih meningkat tersebut digunakan bersamaan untuk menciptakan proses yang lebih terbuka dan juga pelayanan kepada

---

[155] "Internet History" <http://www.computerhistory.org/internet_history/>, Diakses pada 15 Desember 2010, pukul 16.00 WIB.

[156] Majid Yar, *Cybercrime and Society*, (London: Sage Publication, 2006), hal. 8.

[157] Barry M. Leiner, et.al, "History of The Internet" <http://www.isoc.org/internet/history/brief.shtml#Community>, Diakses pada 16 Desember 2010, pukul 02.00 WIB.

masyarakat yang haus akan informasi secara lebih baik lagi. Dengan ini, kebutuhan telah dibentuk dan terus ditingkatkan.

Dikarenakan adanya pemikiran tentang perlunya kebutuhan akan internet, pada 1990 otoritas Amerika Serikat melepaskan ARPANET untuk dikontrol oleh sipil, dengan pengawasan dari *National Science Foundation*. Pada tahun yang sama, pengembangan *web browser* dilakukan para peneliti di laboratorium fisika CERN di Swiss. Mendapatkan julukan '*world wide web*', piranti lunak ini kemudian terus diteliti oleh para programmer, dengan kemampuan lebih baik lagi mampu melakukan lebih banyak pertukaran informasi.[158] Penciptaan antar-muka (*interface*) berupa *web browser* ini semakin memudahkan setiap pengguna internet melihat dan mengelola informasi secara jarak jauh, dan menjadi tahap lanjut untuk mengembangkan berbagai fasilitas komunikasi dalam jaringan internet.

Browser komersial pertama bernama Netscape diluncurkan pada 1994, dan kemudian diikuti oleh Internet Explorer milik Microsoft di tahun selanjutnya. Browser-browser tersebut menjadikan lebih mudahnya pertukaran informasi antara komputer pribadi (*personal computer*). Pada pertengahan 1990-an, sejumlah *Internet Service Provider* (ISP) komersial mulai memasuki pasar informasi, menawarkan layanan sambungan internet kepada siapa pun yang menggunakan komputer dan memanfaatkan akses terhadap sambungan layanan telepon pada umumnya saat itu.[159] Perkembangan signifikan dari ISP dan browser kepada masyarakat inilah yang menjadikan jaminan pertukaran informasi (internet) dengan memanfaatkan sambungan telepon lebih mudah, dan benar-benar dapat dirasakan oleh masyarakat umum. Seluruh layanan yang semula dilepas begitu saja kepada publik, pada akhirnya memunculkan banyak layanan komersial yang mendukungnya.

---

[158] Majid Yar, *Cybercrime and Society*, (London: Sage Publication, 2006), hal. 8.
[159] *Ibid*.

Internet kini telah menjadi sebuah komoditas komersial, dan terlebih lagi telah menjadi sebuah infrastruktur informasi dalam era global untuk mendukung berbagai bentuk komersialisasi. Hal ini sangat dimungkinkan dengan semakin meningkatnya pemanfaatan browser dan teknologi *world wide web*, yang memudahkan setiap orang untuk mengakses dengan **lebih** mudah semua bentuk informasi yang saling terhubung dengan internet dalam jaringan global.[160] Dengan demikian pemasaran berbagai produk komersial telah mendapatkan demikian banyak peningkatan dalam berbagai layanan informasi yang mungkin diberikan oleh internet, dan seiring dengan bertambahnya waktu kemudahan komersialisasi pun semakin bertambah.

Hampir dalam tiga dekade terakhir teknologi internet semakin menunjukkan eksistensi dan peranannya secara global. Perkembangan dari era *personal computer*, *client-server computing*, *peer-to-peer computing*, dan kini memasuki era *cloud computing*, kian memudahkan setiap orang berbagi informasi, lebih banyak informasi. Bukan hanya hal-hal yang bersifat 'berbagi' secara umum, teknologi yang sama juga dimanfaatkan untuk mengakses data-data penting yang bersifat rahasia, dan sekaligus kemudahan untuk mengaksesnya, seperti halnya melakukan *log-in* ke **dalam** jaringan internet untuk mengakses informasi ATM. Tidak dapat dipungkiri, internet telah memasukkan berbagai bentuk layanan dan menciptakan ruang-ruang publik dan juga privat dalam ruang besar yang sama, yang dipilah-pilah secara maya.

Menyaksikan perkembangannya, kita tidak bisa mengatakan bahwa perkembangan teknologi internet akan cepat berakhir dan menemukan titik jenuhnya. Internet adalah ciptaan dari teknologi komputer dan bukan sebuah jaringan tradisional seperti televisi dan telepon. Internet akan terus melakukan peningkatan kemampuannya sesuai dengan kebutuhan dan

[160] Barry M. Leiner, et.al, "History of The Internet" <http://www.isoc.org/internet/history/brief.shtml#Commercialization>, Diakses pada 16 Desember 2010, pukul 02.00 WIB.

perkembangan jaman. Sebagaimana kita saksikan semakin meningkatnya kebutuhan dan kemampuan mengakses jaringan internet melalui berbagai piranti yang semakin *portable* (misalkan: telepon genggam, laptop, PDA), semakin mudah diakses ke dalam piranti-piranti yang berhubungan erat dengan keseharian manusia. Bagaimanapun berbicara tentang teknologi dan internet secara umum adalah bagaimana menjadikan segalanya lebih mudah, sederhana, dan jauh lebih murah, untuk menjangkau dan menggunakannya dalam membantu rutinitas.

### 3.1.2 Ilmu Pengetahuan di Dalam *Cyberspace*

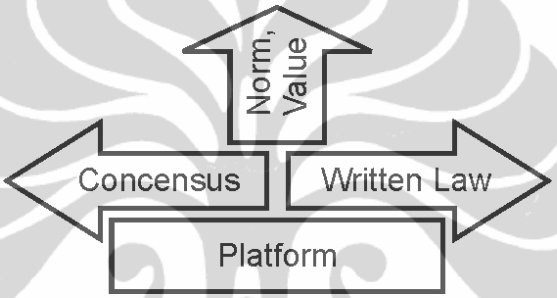
*Knowledge is power, share it and it will multiply*. Di era informasi ini internet memberikan akses yang luas dan kemudahan bagi berkembangnya ilmu pengetahuan, terutama dalam bidang teknologi. Onno W. Purbo dalam "Filosofi Naif Kehidupan Dunia *Cyber*" membahas tentang "Konsekuensi Infrastruktur *Cyber* dalam Proses Pendidikan dan Pemandaian", dalam bab tersebut Onno menjelaskan tentang bagaimana mudahnya pengetahuan diciptakan di dalam era *cyber* ini. Dengan semangat: "Nilai (*value*) seseorang, tergantung manfaat seseorang kepada ummat manusia".[161] Maka bertebaranlah berbagai forum berbagi pengetahuan, dan bentuk riil masyarakat yang terfokus dan saling terintegrasi dapat kita temui dalam bentuknya sebagai *cybercommunity*.

Pembahasan mengenai ilmu pengetahuan di dalam *cyberspace* bukanlah tanpa tujuan dalam kajian hukum, karena dari sinilah kita mulai merunut bagaimana peran komunitas-komunitas *cyber* dalam membina para anggotanya untuk sadar terhadap apa yang mereka hadapi di dalam *cyberspace*, dan bagaimana pengetahuan yang datang secara acak dari berbagai sumbernya mengalami pemurnian untuk diserap sebagai sebuah pengetahuan oleh tiap anggota komunitas. Dan sekali lagi alasan terkuat adalah, bahwa pengetahuan menjadi bentuk ketertarikan sebagian besar

[161] Onno W. Purbo, *Filosofi Naif Kehidupan Dunia Cyber*, (Jakarta: Republika, 2003), hal. 87.

masyarakat untuk masuk ke dalam *cyberspace* dan menjelajahinya. Baik untuk mencari atau untuk berbagi.

Onno W. Purbo memberikan memberikan pendapat, bahwa secara naif, filosofi arsitektur sosial, budaya, dan hukum di dunia maya tampaknya dapat digambarkan secara sederhana dalam bentuk tiga pilar utama yang membangun di atas sebuah infrastruktur atau platform.[162] Onno W. Purbo memberikan subjudul "Aliran Kanan vs Aliran Kiri & Aliran Tuhan", subjudul ini mengesankan bahwa ada kompetisi antara aliran kanan (*written law*) dengan aliran kiri (*concencus*).




*Gambar 3.1. Filosofi arsitektur sosial, budaya, dan hukum di dunia maya.*

Penjelasan yang diberikan pada bagan tersebut adalah:

- Norma (*norm*), nilai (*value*), Iman, Taqwa – yang sifatnya vertikal antara manusia dengan penciptanya.
- Hukum tertulis (*written law*), undang-undang, PP, Kepmen, Kepdirjen – yang sifatnya horizontal dan bertumpu pada aparat penegak hukum dan pengadilan sebagai lembaga yang menjamin tegaknya kebenaran.
- Hukum tidak tertulis, konsensus, hukum adat – yang sifatnya juga horizontal akan tetapi tidak mengandalkan pengadilan dan aparat untuk menegakkan kebenaran dan keadilan, melainkan menggunakan *"People's Power"*.[163]

Onno W. Purbo lantas menambahkan bahwa perubahan dinamika platform tersebut ternyata akan mempengaruhi dominasi di antara ketiga

[162] *Ibid*., hal. 89.
[163] *Ibid*.

pilar di atas, yang akan menimbulkan banyak pertentangan filosofis yang sangat nyata dalam dunia pendidikan, beberapa pertentangan tersebut adalah:

- Apakah kita akan menganut pola pengajaran *teaching based* yang berpusat pada guru? Atau *learning based* dimana guru hanya berfungsi fasilitator?
- Apakah kita akan membentuk siswa dan mahasiswa sebagai konsumen informasi dan pengetahuan? Atau aktif sebagai produsen pengetahuan?
- Apakah kita akan menjaga pengetahuan yang kita miliki menggunakan *copyright,* HAKI, dan hak paten? Atau menggunakan konsensus masyarakat berbasis *copyleft*, *copywrong*, dan *public domain*?
- Apakah kita percayakan penilaian institusi pendidikan kepada Badan Akreditasi Nasional (BAN)? Atau langsung kepada pengakuan masyarakat?
- Apakah kita mengejar ijazah, sertifikat, KUM? Atau bertumpu langsung pada pengakuan masyarakat?
- Apakah kita yakin dengan pendidikan formal yang standar, *rigid*, terstruktur, diseragamkan berbasis pada kurikulum nasional untuk membentuk karakter manusia yang berbeda-beda? Atau bertumpu pada pendidikan informal, nyantri, tanpa kurikulum?[164]

Perubahan platform jelas akan mengubah cara berpikir. Perubahan dari pendidikan dengan cara klasikal yang disekat-sekat dalam dinding sekolah jelas akan berbeda dengan cara seseorang belajar di dalam internet, dimana informasi seperti arus yang tidak terbendung. Demikianlah pada kenyataannya, internet telah menghasilkan para jagoan IT lebih besar daripada sekedar jumlah mereka yang ada di bangku perkuliahan fakultas tehnik jurusan tehnik informatika.[165]

---

[164] *Ibid*., hal. 90-91.

[165] Beberapa narasumber (*hacktivists*) dalam wawancara, dalam penelitian ini menyampaikan bahwa ada beberapa jagoan tehnik informatika yang mereka kenal bahkan tidak datang

Habermas memberikan kritik yang jelas dalam kepentingan ilmu pengetahuan. F. Budi Hardiman menegaskan bahwa Habermas jelas berpendirian bahwa proses untuk memperoleh pengetahuan diarahkan oleh kepentingan. Dalam kehidupan sehari-hari saja kita sudah dapat menyadari kaitan itu: gagasan kita sering kali berfungsi untuk membenarkan perbuatan kita. Psikoanalisa menyebut kecenderungan ini "rasionalisasi" yang pada taraf sosial disebut "ideologi". Menurut Habermas, ilmu pengetahuan sudah terlatih dalam menyingkirkan kepentingan macam itu untuk mencegah opini subjektif dan untuk mencapai apa yang disebut "objektivitas". Habermas tidak menyangkal pentingnya usaha macam itu, tetapi dia melihat bahwa ilmu pengetahuan menutupi kepentingan yang lebih fundamental lagi, yang tidak hanya mendorong tetapi juga menjadi syarat kemungkinan untuk mencapai objektivitas itu. Usaha-usaha untuk menyingkirkan opini subjektif, tendensi, penilaian moral, dan kepentingan lainnya didorong oleh kepentingan yang lebih dalam lagi, yaitu untuk mencapai teori murni.[166]


*Gambar 3.2. Siklus pemurnian pengetahuan.*

Dengan adanya teknologi informasi seperti internet, proses siklus perputaran *knowledge* menjadi sangat cepat sekali. Platform kolaborasi

dari jurusan tehnik informatika. Mereka mempelajarinya secara otodidak. Dan hal serupa dapat kita temukan dalam banyak bidang lain, tidak hanya tehnik informatika.

[166] F. Budi Hardiman, *Menuju Masyarakat Komunikatif: Ilmu, Masyarakat, Politik dan Posmodernisme Menurut Jurgen Habermas*, cet. Kelima, (Yogyakarta: Kanisius, 2009), hal. 34.

untuk *transfer tacit knowledge, digital* library untuk management *explicit knowledge*, dan kemampuan analisis dalam mengolah data mentah menjadi *knowledge* menjadi terasa sebagai sebuah kesatuan terpadu, dibantu pula dengan teknologi informasi yang berfokus pada konsep *knowledge management*.[167]

### 3.1.3 Memahami Struktur Sosial Masyarakat Mayantara

Struktur sosial masyarakat terikat dengan fungsi tiap-tiap agen sosial yang ada di dalamnya, dan di dalam dunia maya fungsi tersebut erat dengan kemampuan tiap individu dalam suatu strata. *Pertama*, kemampuan yang dimiliki seseorang, terutama berkaitan dengan berbagai hal teknis di dunia maya, seperti kemampuan dalam berbagai bahasa pemrograman komputer ataupun yang berbasis internet dan penerapannya dalam *browser*. *Kedua*, kemampuan untuk mengeksploitasi serta mencari celah kelemahannya, bahkan memanfaatkannya. Kemampuan pertama dan kedua tersebut semestinya dimiliki secara bersamaan oleh seseorang yang benar-benar memahami internet, walaupun dalam konotasi yang berlawanan tetapi keduanya sama-sama bermanfaat untuk mengembangkan keamanan di dalam internet. Yaitu kemampuan untuk menciptakan dan mencari kelemahannya, agar kelemahan yang masih ada bisa ditutupi dengan perbaikan program, yang semisal berupa *patch*.[168] Dengan empati, kemampuannya dapat terus terasah untuk membantu para pemakai (publik) mayantara lainnya. Demi kebaikan dan kenyamanan bersama.

Dari memahami suatu kemampuan seseorang dan perannya di dunia maya kita dapat berusaha untuk lebih mengenali bagaimana posisinya

---

[167] Purbo, *Op.cit.*, hal. 95-96.

[168] Istilah '*patch*' dalam program komputer berarti 'tambalan' secara harfiah. Seperti halnya Microsoft yang melepas *operating system* baru ke pasaran, pihak Microsoft sesungguhnya tidak melepas program yang bisa dikatakan sempurna, karena Microsoft sendiri secara rutin tetap melakukan update terhadap temuan *hole* di dalam OS (*operating system*) mereka, baik dengan cara menemukannya sendiri ataupun merespon laporan para pemakai aplikasinya. Baru setelah ada laporan mengenai *bug* (lubang/ celah program) mereka berusaha memperbaikinya dengan mempublikasikan tambalannya. Tambalan ini dipublikasikan dalam bentuk *update* (*update windows xp*, misal). Oleh karenanya para pelanggan harus terus menambal kelemahan dalam program komputernya dengan *patch-patch* yang diterbitkan Microsoft, demi keamanan mereka sendiri.

dalam strata kemampuan yang tersebar luas di dunia maya, yang secara umum menjadi penentu tingkatannya dalam suatu masyarakat maya secara luas dan secara khusus di dalam komunitasnya.

Pertimbangan tentang kemampuan dan peranan seorang pakar *cyber* cenderung dalam ukuran utilitarian, melihat orang perorang dari fungsinya terhadap ruang sosial. Begitu pulalah bagaimana kajian hukum yang berkembang selama ini dalam memandang ruang mayantara itu sendiri. Kejahatan mayantara dimasukkan dalam kejahatan yang dilakukan oleh orang-orang yang memiliki keahlian tertentu (kerah putih/ *white collar crime*) dengan landasan berpikir bahwa untuk melanggar sistem di dalam ruang mayantara memerlukan keahlian khusus dalam bidang teknik *cyber*, dan itu memperlihatkan bahwa pengusaan teknologi merupakan hal utama untuk melakukan tindak kejahatan. Begitu pula bagi mereka yang berada dalam tingkatan-tingkatan strata sosial mayantara pada umumnya menguasai teknologi internet untuk dapat mengelola dan menjalankan perannya dengan baik. Pengertian-pengertian yang demikian berawal dari pemahaman bahwa penguasaan informasi adalah pembentuk 'kekuasaan' dalam arti sesungguhnya dalam era informasi ini.

Dengan demikian inti dari penguasaan suatu masyarakat maya ada pada penguasaan seseorang atas informasi. Dan di masa kini, informasi yang semula dibagikan secara terbuka, kini mulai muncul pembatas-pembatas ruang-ruang privat.[169] Sedangkan di sisi lain ada pihak-pihak yang merasa perlu untuk mengakses segala bentuk data (informasi) yang ada di dunia maya, demi penguasaan informasi dan demi keinginan (mempertahankan haknya) untuk tetap *well informed*.

[169] Seorang narasumber dalam penelitian ini (DM) menyampaikan uraian singkat tentang hal ini. Pada mulanya internet adalah bersifat publik, kemudian muncul pengaturan-pengaturan mengenai batasan-batasan *bandwidth* (besaran dalam perhitungan kapasitas koneksi internet), ruang privasi, dan sebagainya. Kemudian karena itulah beberapa orang kemudian merasa perlu melakukan revolusi terhadap batasan-batasan yang dibentuk, yang dinilai membatasi gerak dan memanipulasi informasi dari ruang publik. Dari sanalah (menurut narasumber tersebut) bermulanya semangat munculnya komunitas-komunitas *hacker* dan semacamnya.

Struktur sosial mayantara berlaku kepada mereka yang memiliki kemampuan untuk melakukan interaksi di dalamnya (ruang maya tentu saja didefinisikan kepada mereka yang berinteraksi di dalamnya, baik individu maupun yang mengatasnamakan suatu negara). Dengan penjelasan *a la* Habermas tentang ruang publik dalam kajiannya terhadap kategori masyarakat borjuis, setidaknya kemampuan yang dimiliki para pakar *cyber* adalah bentuk borjuasi yang berbeda dalam era informasi, penguasaan informasi sama berharganya dengan kekuasaan para borjuis dalam wilayah-wilayah dunia nyata.

Dengan mengkaji tentang masyarakat borjuis dalam "Ruang Publik" karya Habermas, keserupaan dalam penguasaan sektor-sektor publik ditemukan dalam penguasaan akan sumber-sumber informasi dan bagaimana kemampuan meretasnya agar informasi itu dapat diperoleh atau terkadang kemudian dimanipulasi. Namun perbedaannya adalah, di dalam kajian terhadap borjuasi tidak memberikan pemahaman tentang wilayah yang bersifat publik secara bersamaan dengan saat kita membahas ruang borjuis itu sendiri. Tetapi di dalam masyarakat *cyber* mereka yang memiliki kemampuan lebih dalam penguasaan teknologi *cyber* dapat mengelola ruang-ruang bagi publik (selain mereka) yang menggunakannya, sekaligus secara bersamaan. Dan memahami betul permasalahan yang dihadapi oleh publik secara umum dan mendasar.

Perbedaan antara penguasaan atas wilayah sosial di dunia nyata dengan penguasaan atas wilayah sosial di dunia maya berbeda, karena kemampuan untuk menangani secara umum dalam ruang publiknya maupun dalam sekat-sekat keamanan privat, pada mulanya berangkat dari kemampuan awam (dalam ruang publik bersama dengan yang lainnya) yang sekedar ia gunakan untuk menjelajahi secara sederhana (awam), kemudian interaksinya dengan dunia maya memberikan ketertarikan sendiri untuk lebih memahami bagaimana mekanismenya, bagaimana sistem itu diatur dan dikelola, bagaimana keamanan mampu menjaga tiap

privasi yang diciptakan. Maka perbedaannya adalah: intimitas dengan masa lalu sebagai pengalaman yang dimiliki oleh seorang penguasa dalam ruang mayantara memberikannya pemahaman lebih baik terhadap ruang publiknya secara umum, sedangkan bentuk penguasaan dalam ruang nyata tidak dapat sepenuhnya dijelaskan secara bersamaan sebagai pemahaman secara baik terhadap publik yang ada di strata di bawahnya. Karena kekuasaan di dunia nyata dapat berupa karena keturunan atau pun bentuk keberuntungan politis dan kemungkinan lain dari keberuntungan yang tak jauh berbeda, dan diskontinuitas seseorang dalam menapaki tingkatan-tingkatan yang ada dalam setiap strata dapat diterima secara logis dibandingkan dengan di dunia nyata.[170]

Habermas dalam *The Structural Transformation of The Public Sphere: An Inquiry into a Category of Borgeois Society*,[171] memberikan penjelasan yang luas tentang perubahan peran masyarakat borjuis dan perubahan posisinya dalam masyarakat Inggris pada khususnya, di era awal pasca revolusi Perancis. Di dalamnya ia menarasikan bagaimana peran kekuasaan feodal yang dimiliki oleh kaum borjuis memberikan sekat yang teramat jauh dengan golongan bawah (proletar), beruntung adanya peran golongan menengah yang berpendidikan kemudian menjadi jembatan bagi kaum borjuis untuk menemukan posisinya dalam ruang publik masyarakat proletar melalui politik, dan golongan menengah-terpelajar itulah yang mempertemukan kekuatan politik dengan kaum borjuis yang tidak

[170] Beberapa narasumber dalam *interview* penelitian ini mendukung penjelasan, saat seseorang menyatakan dirinya sebagai *whitehat hacker*, maka dia tidak bisa melepaskan kenyataan bahwa untuk mencapai afirmasi sebagai *whitehat* ia pasti pernah melakukan cara-cara sebagaimana seorang *blackhat hacker*. Dengan kata lain, untuk mencapai pengetahuan sebagai seseorang yang mampu membenahi sistem yang rusak dengan paripurna (dan hanya memperbaikinya tidak bertujuan memanfaatkan celah kelemahan untuk tujuan merusak), seseorang itu tentulah pernah menjalani masa ketika ia belajar bagaimana mencari kelemahan dan mencari tahu sejauh mana kelemahan itu dapat memunculkan kerusakan, dari yang sederhana sampai tingkat fatal, dengan melakukan perusakan itu sendiri. Dengan cara seperti itulah pengetahuan terbaik dapat dicapai dan mendapatkan afirmasi dari yang lain.

[171] Lihat, Jurgen Habermas, *Ruang Publik: Sebuah Kajian tentang Kategori Masyarakat Borjuis* (*Public Sphere: An Inquiry into a Category of Borgeois Society*), diterjemahkan oleh Yudi Santoso, (Yogyakarta: Kreasi Wacana, 2010).

memiliki kekuatan politik. Di sisi lain, dengan adanya golongan menengah-terpelajar inilah golongan proletar dapat menyampaikan aspirasinya kepada golongan di atas mereka.

Penguasaan politik dan pengetahuan yang kemudian dimiliki oleh kaum borjuis ini dapat menjadi gambaran, bagaimana kekuasaan atas politik atau bahkan ilmu pengetahuan, tidak sepenuhnya memiliki intimitas yang riil dengan publik proletar yang menjadi obyek kajiannya baik dalam politik maupun pengetahuan secara lebih luas. Pembelajaran tidak selamanya menjadikan kita bagian utuh dari apa yang kita pelajari, karena pendidikan tentang sesuatu tidak berarti kita harus mengalaminya secara langsung, melainkan kita cukup mengalaminya dalam simulasi-simulasi yang terus disederhanakan oleh berbagai bentuk metode yang berkembang. Kemudian kita meyakini, bahwa narasi yang teruji dan dengan adanya penelitian yang diakui di luar sana, apa yang kita ketahui dan pelajari di sini adalah benar. Tetapi dalam *cyberspace*, untuk mempelajari bagaimana sesuatu itu terjadi dan mungkin serta bagaimana mengatasinya, adalah dengan cara mengalaminya.[172]

Dengan uraian di atas, tujuan utamanya adalah bahwa kekuasaan yang menjadi bagian utama struktur masyarakat mayantara adalah

---

[172] Saya lebih menyukai untuk membahasnya dalam gagasan Erich Fromm tentang dua modus mengada, yaitu 'memiliki' dan 'menjadi'. Seseorang dalam gambaran tingkat borjuasinya akan mendapatkan pengalaman-pengalaman pengetahuan dan kemudian menjadi seorang pemimpin, namun pengalaman-pengalaman tersebut adalah sebatas informasi yang masuk dan dia mengada dengan cara memiliki-nya. Tetapi gambaran dari para kelas menengah yang memobilisasi gerakan proletar yang sadar akan kebutuhannya di dalam ruang publik, dengan menyadari adanya kekuasaan negara dan adanya borjuasi di atas mereka, mereka terdidik dan mengalami sendiri bagaimana menjadi rakyat merasakan bagaimana menjadi tertindas. Pada intelektual yang demikian ini adalah mengalami modus mengada dengan menjadi, atau ia hadir sepenuhnya mewakili suara rakyat. Lihat, Erich Fromm, *Memilik dan Menjadi: Tentang Dua Modus Eksistensi* (*To Have or To Be*), diterjemahkan oleh Susilohardo, cetakan kedua, (Jakarta: LP3ES, 1988).

Demikian juga pengetahuan tentang *cyberspace* dapat dicapai dengan cara menjalani tahap-tahap bagaimana pengertian-pengertian yang ada di dalam pengetahuan tersebut hadir dan diserap dengan baik dengan cara mengalaminya. Sebagaimana pencurian itu mungkin, maka seseorang setidaknya memahami bagaimana menjebol sistem keamanan dan mencuri sesuatu yang berharga yang disimpan di dalamnya dengan mengalaminya sendiri. Yang kemudian untuk memperkuat sistem keamanan kemudian dia menghindari dan memperbaiki hal-hal yang memungkinkan orang lain melakukan pencurian. Dengan cara memperbaiki sistem keamanannya.

penguasaan teknologi di dalamnya. Mereka yang memiliki kekuasaan lebih dalam dunia maya adalah mereka yang memiliki pengetahuan lebih menyeluruh dari yang mendasar hingga tahapan dimana ia berada, dan dengan bertolak dari tingkat pengetahuan serta afirmasi publik atas kemampuannya seseorang berada dalam suatu strata tertentu.

Sebagian orang berusaha memahami suatu struktur sosial hanya sebagai struktur saja, sedangkan sebagian yang lain memahami dan berusaha mengenalinya dengan memahami fungsionalisasi di dalamnya

**3.1.3.1 Internet: Komunitas Dunia *Cyber***

> Internet sering diasosiasikan dengan Web, yang merupakan situs di dunia *cyber* tempat informasi diletakkan dan dapat diakses oleh pengguna internet. Sifat web biasanya pasif dan menunggu pengunjung mendatangi situs Web untuk mengambil informasi yang dibutuhkan. Pada saat akses Web, pengunjung berinteraksi dengan server Web dan basis data di belakangnya. Terus terang, pola interaksi demikian sangat tidak manusiawi bagi sebagian besar pengguna internet.[173]
>
> Mengamati lingkungan sosial di dunia *cyber* akan sangat strategis dengan mengamati profil dan karakteristik komunitas di dunia *cyber*. Sebagai gambaran, dari analisis konten komunitas dunia maya, kita dapat dengan mudah mengidentifikasi konsentrasi massa, pemimpin massa, pergerakan massa, sampai teknik terbaik untuk melakukan penetrasi ke dalam massa, serta mengetahui selera masyarakat Indonesia khususnya pengguna internet.[174]
>
> Menurut pengamatan Onno W. Purbo, meskipun konten komunitas di media cetak dan di dunia maya sama-sama terbentuk karena selera masyarakat tentang sesuatu, seperti tentang sepak bola, masak-memasak, otomotif, politik, hukum, dan sebagainya.

[173] Purbo, *op.cit.*, hal. 27.
[174] *Ibid*., hal. 15.

Tetapi, ada beberapa kelebihan konten komunitas dunia cyber dari konten media cetak. Pada komunitas dunia cyber, konten dibangun dan dihasilkan langsung oleh masyarakat atau pembaca sendiri. Pada media cetak, konten lebih banyak dibuat oleh dewan redaksi melalui berbagai cara untuk memperoleh kontennya, sehingga belum tentu 100 persen merepresentasikan kesukaan masyarakat pembacanya.[175]

Komunitas-komunitas *cyber* memang erat dengan tema-tema tertentu yang diusung oleh tiap komunitas, dan pembentukannya tidaklah karena otoritas satu orang, melainkan karena adanya kesamaan selera. Tiap komunitas bisa memiliki selera yang berbeda dari komunitas lainnya, dari hal sederhana seperti kegemaran akan hal-hal yang berkaitan dengan sepeda *onthel* dan pernak-perniknya, hingga hal-hal yang terlarang seperti pembahasan kerumitan sistem informasi dan diskusi tentang teknik melakukan kejahatan di dalamnya, seperti teknik *hacking, carding,* dan sebagainya.

Kajian tentang *cybercrime* akan lebih spesifik jika fokus pada komunitas-komunitas yang menyatakan diri sebagai komunitas *hacker,* terutama di Indonesia. Karena di komunitas-komunitas dengan pembahasan tentang keamanan dan berbagai bentuk antisipasi terhadap kelemahannya merupakan pembahasan umum inilah tempat bertemu berbagai kalangan dari sisi hitam maupun putih, bersama-sama berbagi ilmu dan belajar dengan melakukannya (*learning by doing*).

### 3.1.3.2 *Hacker*: Sub-Kultur Dunia *Cyber*

Robin Hood di era komputer atau jagoan dengan tehnik tinggi yang beraksi di belakang layar dalam dunia digital? Masyarakat membangun berbagai cerita dan pemahaman tentang kehebatan para *hacker* atau bahkan mengutuk mereka sebagai bagian tidak

[175] *Ibid*., hal. 16.

terpisahkan dari kejahatan dunia maya. Berbagai pemahaman berkembang tergantung dengan cerita-cerita yang datang dan membangun pandangan mereka tersebut. Akan tetapi berbagai persepsi yang ada sering kali tidak membuat kita memahami dengan baik bagaimana dunia mereka yang sesungguhnya, cenderung mendorong lebih dalam kepada satu pemahaman yang belum tentu kebenarannya.

Terminologi peretas muncul pada awal tahun 1960-an diantara para anggota organisasi mahasiswa Tech Model Railroad Club di Laboratorium Kecerdasan Artifisial Massachusetts Institute of Technology (MIT). Kelompok mahasiswa tersebut merupakan salah satu perintis perkembangan teknologi komputer dan mereka berkutat dengan sejumlah komputer *mainframe*. Kata bahasa Inggris "*hacker*" pertama kalinya muncul dengan arti positif untuk menyebut seorang anggota yang memiliki keahlian dalam bidang komputer dan mampu membuat program komputer yang lebih baik daripada yang telah dirancang bersama. Kemudian pada tahun 1983, istilah *hacker* mulai berkonotasi negatif. Pasalnya, pada tahun tersebut untuk pertama kalinya FBI menangkap kelompok kriminal komputer The 414s yang berbasis di Milwaukee, Amerika Serikat. 414 merupakan kode area lokal mereka. Kelompok yang kemudian disebut *hacker* tersebut dinyatakan bersalah atas pembobolan 60 buah komputer, dari komputer milik Pusat Kanker Memorial Sloan-Kettering hingga komputer milik Laboratorium Nasional Los Alamos.[176]

Pada kenyataannya, secara sederhana *hacker* adalah orang-orang yang menyukai mainan. Setiap ada permainan baru dalam telekomunikasi di eranya, mereka tertarik untuk segera melakukan

[176] "Hacker" <http://opensource.telkomspeedy.com/wiki/index.php/*Hacker*>, diakses pada 5 Juni 2011, 13.00 WIB.

sesuatu kepada ‘mainan’ baru tersebut. Pada dekade 80-an saat muncul berbagai peralatan telekomunikasi. Di dalam beberapa tahun itu, segala sesuatu meledak. Segera muncul segala bentuk perusahaan telepon baru untuk dijelajahi dan dimainkan. Menjadikan sebuah panggilan telepon sederhana sebagai sebuah tantangan dan petualangan. Berbagai sistem bermunculan sebagai leluhur dari voicemail dewasa ini. Kita bahkan menemukan beberapa sistem pendeteksi suara masa awal. Fax, pager, teleconference, telepon selular, di dekade ini segalanya mendatangi kita dengan begitu cepatnya. Dan dengan setiap penemuan yang dilakukan seorang *hacker* atau yang dilakukan peretas telepon, muncul para penyimak yang selalu menanti pemahaman baru dari semua itu.[177]

Emmanuel Goldstein menarasikan berbagai latar sejarah telekomunikasi modern Amerika Serikat dengan peran para *hacker* dalam memeriksa berbagai kelemahan telekomunikasi dalam memainkan permainannya. Dimanapun ada perkembangan teknologi—dan di sana ada kegiatan praktis harian dalam telekomunikasi pada tahun 1980-an—Anda dapat menyaksikan para *hacker* hadir sebagai yang pertama dalam upaya menemukan cara memainkan permainan itu, sebagian besar dengan cara-cara yang tidak ditujukkan oleh pembuat pertama kali. Dewasa ini, banyak para pembuat kerusakan yang telah mengacaukan jalur telepon, mencari tau cara memonitor panggilan melalui gelombang radio, atau dengan sederhana membiarkan dunia tahu apa yang tidak berfungsi dan servis apa saja yang dibuang—orang-orang tersebut kini adalah orang-orang yang membuat sistem-sistem baru dan

[177] Emmanuel Goldstein, *The Best of 2600: A Hacker Oddyssey*, (Indianapolis: Willey Publishing, 2008), hal. 65. “2600” adalah sebuah jurnal terkenal di Amerika Serikat, penerbitan ini merilis secara rutin berbagai hal tentang *hacker* dan hacking, atau dengan kata lain sebagai media *hacker* populer di Amerika Serikat.

menciptakan permainan-permainan baru bagi generasi kemudian dalam dunia *hacker*.[178]

Gerakan *underground* mayantara dijelaskan dalam banyak bagian dari jurnal-jurnal semacam *Phrack* dan *2600*. Bagaimanapun, tidak mungkin untuk memisahkan pengertian tentang *hacker* dari pencitraan identitas *hacker*. Sebagai sebuah subkultur, *hacker* telah membangun sebuah gaya hidup yang berubah dari berbagai masa dan telah terstruktur seperti luapan dan bentuk yang kuat dari perlawanan. Sebagai sebuah kultur generasi muda, *hacker* secara terus-menerus mencari cara untuk menggelisahkan atau mengacaukan otoritas dan menantang segala pemahaman atau penggambaran tentang siapa mereka.[179] Dalam melacak kebiasaan seperti apa yang dibangun oleh para *hacker*, bermutasi, dan berkembang, Douglas Thomas dalam bukunya *"Hacker Culture"* (2002) mencoba memeriksa bagaimana dimulainya dalam budaya komputer, perubahannya sebagai tempat melekatnya identitas *subculture*, dan, puncaknya, saat berbenturannya antara kekuatan identitas *subculture* mereka dengan identitas yang dimunculkan secara paksa terhadap mereka dalam film-film dan media massa.

> *Understanding hackers of today necessitates a basic understanding of the history of the subculture that preceded them and of how, traditionally, subcultures have functioned to resist dominant cultural interpretations of them.*[180]

Memahami suatu masyarakat memerlukan ketelitian, terlebih lagi kelompok subkultur seperti *hacker*, *biker*, *punk subculture*, dan sebagainya, perlu pendekatan khusus menyentuh sisi sensitif mereka. Kemampuan dan tehnik hacking yang memerlukan seni

---

[178] *Ibid*., hal. 66.

[179] Douglas Thomas, *Hacker* Culture, (Minneapolis: University of Minnesota Press, 2002), hal. 141.

[180] *Ibid*.

tinggi dalam dunia *cyber* terkadang menjadikan mereka benar-benar seniman yang tidak selalu mudah dimengerti.

Douglas Thomas menjelaskan bahwa *hacker* lebih tepat jika disebut sebagai sebuah *subculture*, sebuah kultur yang terikat oleh dua sisi, parental culture, dan sekaligus bersifat melawan terhadapnya. *Subculture* ditandai dengan ketidakstabilan mereka, perubahan konstan baik dalam makna dan dalam proses dimana makna dibentuk. Dick Hebdige menjelaskan, makna dari subculture selalu dalam perselisihan, dan coraknya adalah wilayah dimana mempertentangkan definis-definisi perselisihan dengan kekuatan yang paling dramatis. Tekanan ini adalah tempat dimana ketertarikan umum atau kepentingan umum dilampaui, dimana sebuah elemen subculture menguasai kontrol atas pemaknaan atas sesuatu yang memiliki arti penting bagi kebudayaan yang lebih luas. pengertian dari style, kemudian, digerakkan dari sumbangan subculture atas sebuah simbol dari budaya mainstream. Sumbangan atau pemberian itu juga melibatkan reinterpretasi. Dengan cara ini, subculture mengambil bagian dari culture (budaya) yang lebih luas dan merekontekstualisasikannya dengan maksud untuk memberikan perbedaan, seringkali pertentangan makna.[181]

Corak (*style*) *subculture*, kemudian, adalah tentang mengidentifikasikan objek-objek penting dari semiotika kultural dan memposisikannya kembali dengan cara yang berkebalikan untuk menunjukkan penolakan dari diskursus *mainstream* dan untuk mengkonstruksikan sebuah diskursus baru seputar pemosisian-kembali dan melakukan artikulasi ulang atas objek-objek. Maka tidak mengherankan, lokasi utama dari identitas *subculture* adalah kultur anak muda. Identifikasi *subculture* juga tentang resistensi kepada pemilik otoritas, dan sebagian merupakan resistensi

[181] *Ibid*., hal. 142.

terhadap metode-metode, corak mode, cara-cara bersikap atas kultur yang lebih luas, kultur kekuasaan orang tua. Bagi para pemuda ini merupakan masa transisi dari sebuah dunia dalam otoritas orang tua, dimana orang tua mendikte bagaimana berbagai hal mesti dilakukan, menuju pada sebuah dunia tanggungjawab, dimana pemuda membuat keputusan-keputusannya sendiri. Transisi ini ditandai dengan pemberontakan, pembangkangan, dan berfokus dalam satu pikiran dalam memandang perbedaan.[182]

Pengertian *subculture* adalah, kemudian, selalu dalam pertentangan, dan coraknya adalah wilayah dimana definisi-definisi yang berlawanan berbenturan dengan kekuatan paling dramatis. Seperti dalam novel Genet,[183] sebuah novel pertama Genet *"Our Lady of The Flowers" (Notre-Dame-des-Fleurs)*[184] bisa sebagai contoh, proses tersebut akan dimulai dengan sebuah kejahatan melawan aturan alam, meskipun dalam hal ini tindakan menyimpang pada kenyataannya tampak remeh—memelihara jambul, keahlian tentang skuter atau sebuah rekaman atau pakaian dengan corak tertentu. Tetapi pada akhirnya dalam konstruksi

[182] *Ibid*., hal. 142-143.

[183] Jean Genet (19 Desember 1910 – 15 April 1986), adalah seorang terkemuka, terkadang dicemooh, seorang penulis berkebangsaan Perancis dan kemudian menjadi seorang aktifis politik. Pada awal hidupnya dia adalah seorang gelandangan dan kriminal kelas teri; kemudian dalam hidupnya, Genet menulis novel, drama, syair, dan berbagai essay. Dalam kelima novel awalnya, karya-karya Genet bertujuan untuk menumbangkan setting tradisional atas nilai-nilai moral atas apa yang telah ia dapatkan dari berbagai bacaan. Dia merayakan kecantikan dalam kejahatan, menekankan keganjilannya dengan cara ia ciptakan posisi para pelaku kejahatan kriminal sebagai icon-icon, menikmati keteguhan sikap seorang gay dan mengkodekan serta melukiskan gambaran-gambaran pengkhianatan. (http://www.newworldencyclopedia.org/entry/Jean_Genet, diakses pada 20 Mei 2011, pukul 07.00 WIB).

[184] Jean Genet, *Our Lady of The Flowers*, (Paris: Olympia Press, 2004). Diterjemahkan oleh Bernard Frechtman dan dengan kata pengantar oleh Jean-Paul Sartre, novel ini ditulis dalam sebuah penjara Perancis dalam sebuah kertas coklat yang biasa digunakan sebagai tas kertas. Publikasinya secara serta merta menjadikan Genet berada dalam baris depan para penulis Perancis yang mengekspresikan pemikiran jenius mereka melalui pemahaman mereka akan keadaan manusia pada derajat terendahnya. Our Lady of the Flowers adalah tentang pembunuh berusia 16 tahun yang telah memenuhi takdirnya dengan mencekik seorang lelaki tua. Dalam dunianya, para germo, pencuri, pelacur, moralitas dalam keseharian tidaklah memiliki arti. Fantasi Genet dari ruang penjaranya memberikan sosok pahlawan-pahlawan kriminal, menunjukkan kekuatannya sebagai seorang moralis dalam menciptakan karya tentang kejahatan di luar dari suatu masyarakat yang diatur oleh hukum.

corak, dalam sebuah bentuk penyimpangan atau penghinaan, dalam satu senyuman atau sebuah seringai. Hal itu menjadi sinyal-sinyal penolakan. Saya lebih suka memikirkan bahwa penolakan ini adalah cara menciptakan arti, bahwa sikap-sikap demikian memiliki suatu arti, bahwa senyuman-senyuman dan sikap-sikap mencemooh memiliki beberapa nilai subversif, meskipun jika, dalam analisis akhir, mereka, seperti gantungan dinding gangster dalam novel Genet, hanyalah sisi lebih gelap dari seperangkat peraturan, hanya begitu banyaknya grafiti pada sebuah dinding penjara (Dick Hebdige, 1979: 3).[185]

Uraian Hebdige sebagaimana tokoh yang ia kutip, Genet, terhadap konsep *subculture* tampaknya juga ia peroleh dari berbagai bahan bacaan yang ia dapatkan. Searah dengan Hebdige yang telah secara umum menjelaskan tentang *subculture,* Onno W. Purbo dalam menjawab salah satu pertanyaan penelitian ini menyampaikan, bahwa untuk mendekati sub-kultur masyarakat *cyber*, yang biasa dikenal sebagai komunitas *hacker*, tidaklah mudah, karena dibutuhkan ketelatenan dan kesabaran. "*hacker* adalah "seniman," *gak* gampang bergaul dengan seniman," ungkap Onno W. Purbo.[186]

Dick Hebdige dengan analisisnya atas konstruksi subculture sebagian caranya melalui pendekatan psikologis cukup menarik. Hebdige menyatakan bahwa *culture* yang demikian muncul secara dominan pada masa transisi dari wilayah otoritas orang tua kepada wilayah tanggungjawab pribadi yang membutuhkan keputusan-keputusan mandiri dari usia muda, mencuat dalam bentuk yang penuh kesan berontak dan terkadang melawan hukum alam, dan bukan tidak mungkin terkesan sebagai kriminalitas.

[185] Dick Hebdige, *Subculture: The Meaning of Style*, (London: Routledge, 1979), hal. 3.
[186] Wawancara dengan Onno W. Purbo, 20 Mei 2011.

> *If men cannot refer to common values, which they all separately recognize, then man is incomprehensible to man. The rebel demands that these values should be clearly recognized as part of himself because he knows or suspects that, without them, crime and disorder would reign in the world. An act of rebellion seems to him like a demand for clarity and unity. The most elementary rebellion, paradoxically, expresses an aspiration to order* (Camus, 1974: 29).[187]

Pemberontakan atas otoritas sebagaimana dijelaskan Hebdige, perlu didukung oleh pemahaman metafisika dari Camus. Sebagaimana dalam dunia *hacker*, dengan menyimak sejarah *hacker* dalam jurnal *2600: A Hacker Odyssey* yang ditulis oleh Emmanuel Goldstein di atas, pemberontakan yang dilakukan adalah dalam rangka untuk membuka ruang informasi yang lebih layak dan transparan bagi setiap orang, sehingga menghindarkan setiap orang yang mengkonsumsi alat-alat tersebut dari manipulasi teknologi. Tujuan untuk meningkatkan kemudahan komunikasi dan mendapatkan jaringan internet murah atau gratis sekalipun bisa dilihat sebagai pelanggaran bagi penegak hukum, tetapi bagi mereka ini adalah sebuah pemberontakan atas bentuk-bentuk muslihat yang ada dalam budaya yang lebih luas, yang berpotensi bagi setiap orang untuk termanipulasi dengan kelemahan servis yang ada. Pengembaran dunia *hacker* selalu berusaha memberi kritik terhadap sistem dan menunjukkan kelemahannya untuk perbaikan bagi semua.[188]

Sementara itu penelitian yang merunut dengan telaten seperti Emmanuel Goldstein (2008: 66) yang menjadi penulis dalam jurnal *hacker* populer, "2600", yang memiliki kedekatan tersendiri dengan

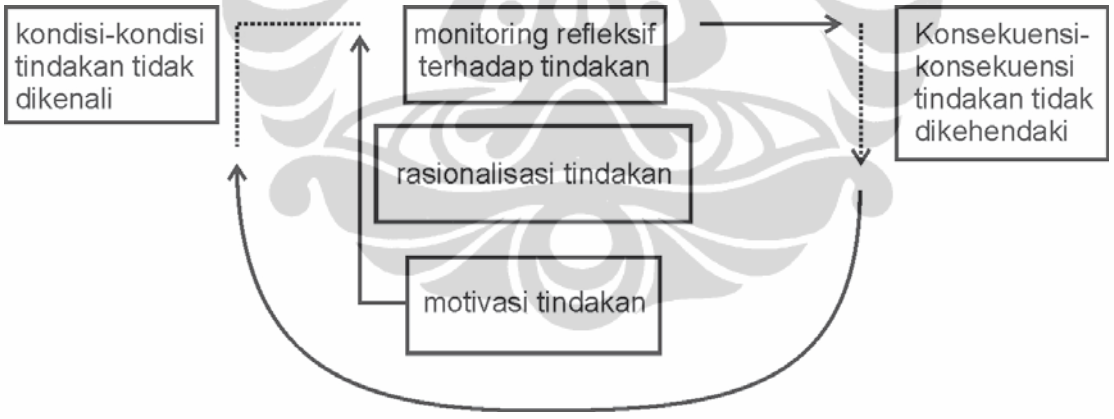
[187] Albert Camus, *The Rebel*, (Middlesex, England: Penguin Books, 1974), hal. 29.

[188] *Hacking* memiliki pengertian yang luas. Sebuah situs populer "Hackaday" (http://hackaday.com/) menunjukkan bagaimana 'mengakali' benda-benda di sekitar kita agar menjadikannya sesuatu yang lebih bermanfaat bahkan melampaui kemampuan benda tersebut sendiri dalam makna teknisnya, untuk keperluan dan kegiatan keseharian. Kira-kira dalam pengertian yang demikianlah apa yang disampaikan oleh Goldstein dalam "A *Hacker* Odyssey"-nya.

dunia *hacker*—mungkin juga secara intense dengan dunia *hacker*, tentu berbeda dengan pengamatan melalui media. Seperti yang diungkapkan oleh Douglas Thomas (2002: 141) di atas, bahwa seringkali pemahaman tentang dunia *hacker* itu sendiri terdistorsi dengan kesan-kesan yang disampaikan oleh media yang terus berkembang.

**1) *Hacker* Sebagai Agen Sosial**

Sementara itu akan merujuk kepada konsep struktur sosial Anthony Giddens. Aktor atau agen sosial, dalam penjelasannya tentang bagian-bagian struktur sosial, tidak hanya memonitor secara terus-menerus arus aktivitas mereka dan berharap orang lain melakukan hal sama terhadap aktifitas mereka sendiri; para aktor ini juga secara rutin memonitor aspek-aspek, baik sosial maupun fisik, dari konteks-konteks tempat di mana mereka bergerak.




*Gambar 3.3. Monitor refleksif atas tindakan (Giddens, 1984)*

Dalam bagan tersebut terdapat bagian yang disebut dengan ‘rasionalisasi tindakan’. Giddens menjelaskan, bahwa yang ia maksud dengan rasionalisasi tindakan adalah bahwa aktor mempertahankan suatu ‘pemahaman teoretis’ yang terus-menerus tentang landasan aktifitas mereka. Menurut Giddens memiliki pemahaman semacam itu tidak boleh disamakan

dengan pengungkapan alasan-alasan bagi unsur-unsur tindakan tertentu, tidak juga dengan kemampuan menspesifikasi alasan-alasan itu secara diskursif. Namun demikian, harapan para agen kompeten tindakan-tindakan yang lain—dan inilah kriteria kompetensi yang diterapkan dalam perilaku sehari-hari—adalah bahwa para aktor biasanya akan mampu menjelaskan sebagian besar tindakan mereka, jika memang diminta.[189]

Mengamati dari peran *founder*, *hacker*, dan para *security professionals* lainnya terhadap lingkungannya, serta kemampuan mereka mendefinisikan alur dan arus mekanis di dalam ruang-ruangnya dan kompetensi yang mereka tunjukkan dalam menjelaskan dan mengatasi permasalahan merupakan bentuk rasionalisasi tindakan. Dalam grafis terlihat bahwa Giddens berusaha menjelaskan bahwa seorang aktor/agen adalah mereka yang mengalami sendiri pengamatan dan mampu menjelaskannya dengan baik. Oleh karena itulah ia mengatakan "'pemahaman teoretis' yang terus-menerus tentang landasan-landasan aktifitas mereka." hal ini menunjukkan adanya aspek teleologis dan naratif terhadap pengamatan yang ia lakukan.

Seorang *hacker* dalam menapaki tahapan untuk kemudian mendapatkan afirmasi akan kemampuan dan penguasaannya akan ruang tempat ia berada dan hal ini terus-menerus diperkuat secara rutin dalam keseharian. Dan terlihat dalam gambaran sederhana, dalam wawancara dengan para *cyberactivists*, bahwa setiap mereka mampu menjelaskan secara baik dengan pemahaman serius atas *cyberspace* dan pertimbangan berbagai kemungkinan logis tentang *cybercrime*. *Hacker* jelas memilih peran dan posisinya sendiri, dan mereka adalah pihak yang dapat

[189] Anthony Giddens, *Teori Strukturasi: Dasar-Dasar Pembentukan Struktur Sosial Masyarakat* (*The Constitution of Society: Outline of the Theory of Structuration*), diterjemahkan oleh Maufur dan Daryatno, (Yogyakarta: Pustaka Pelajar, 2010), hal. 7-8.

dijelaskan secara definitif sebagai agen/aktor ruang publik mayantara. Begitu juga karakter dan moralitas kembali kepada para *hacker* masing-masing.

"Istilahnya, senioritas dengan skill-nya harus balance. Kondisi sekarang, malingnya sendiri tahu cara kerja polisi bagaimana. Sekarang *hacker* itu kembali kepada diri sendiri-sendiri." (BD, 11 April 2011)

**2) *Hacker Ethics***

Steven Levy, seorang penulis seputar *cyberlife* dan segala perkembangannya memberikan beberapa pokok *hacker ethics*, dalam bukunya yang populer tentang wacana *hacker*, "*Hacker*s: Heroes of The Computer Revolution":

- *Access to computers and anything which might teach you something about the way the world works should be unlimited and total. Always yield to the Hands-On Imperative!*
- *All information should be free.*
- *Mistrust Authority Promote Decentralization.*
- *Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.*
- *You can create art and beauty on a computer.*
- *Computers can change your life for the better.*
- *Like Aladdin's lamp, you could get it to do your bidding.*[190]

Etika di atas sebetulnya cukup berbeda dengan dunia nyata, salah satu konsekuensi yang paling mendasar yang di anut oleh banyak *hacker* adalah, *"hacker tidak percaya pada otoritas*

[190] Steven Levy, *Hacker*s: *Heroes of The Computer Revolution*, (New York: Delta Publishing, 1994), 32-41. Dalam pembahasan tentang *hacker* secara khusus, pembahasan yang diusung oleh Steven Levy ini juga dapat disimak dalam: "Etika Hacker", <http://opensource.telkomspeedy.com/wiki/index.php/Filosofy:_Etika_*Hacker*>, diakses pada 6 Juni 2011, jam 22.00 WIB.

*(penguasa), dan mereka hanya menghormati seseorang karena keahliannya."*[191]

Yang dijabarkan oleh Levy bisa jadi merupakan dorongan kepada seluruh komunitas *hacker* agar berusaha memegang sederet etika tersebut, untuk juga menanamkan prinsip-prinsip positif yang bisa dibangun sejak awal seseorang tertarik memasuki dunia tersebut, disamping kepercayaan pada prinsip untuk *well informed* secara total, tetapi tetap berprinsip bahwa komputer dapat memberikan kehidupan yang lebih baik bagi siapa saja.

**3) Kemampuan Teknis *Hacker***

Dalam mengukur kemampuan umum para *hacker* tidak ada standar khusus mengenai hal tersebut. Meskipun saat seseorang telah diterima dalam suatu komunitas *hacker* sebagai seorang *hacker* belum tentu ia memiliki kemampuan/ keterampilan yang sebanding dengan, *hacker* yang lainnya.

Sejak munculnya masalah *cyber-control* atas jaringan digital manajemen penerbangan Amerika Serikat pada 11 September 2001, memunculkan pertanyaan penting dalam benak *founder* EC Council –Jay Bavisi dan Haja Mohideen, tentang bagaimana menemukan formula untuk menghindari terjadinya *cyberwar*. Mereka melakukan riset, mereka berusaha mencari pada situs-situs berbagai program untuk "Internet Security" yang

[191] "Etika Hacker" <http://opensource.telkomspeedy.com/wiki/index.php/Filosofy:_Etika_*Hacker*>, diakses pada 6 Juni 2011, jam 22.00 WIB. Dalam halaman situs tersebut, pandangan Levy mendapat beberapa penjabaran: 1) **Akses ke komputer** – dan apapaun yang akan mengajarkan kepada anda bagaimana dunia ini berjalan / bekerja – harus dilakukan tanpa batas & total. Selalu mengutamakan pengalaman lapangan! ; 2) **Semua informasi harus bebas**, tidak di sembunyikan. Etika ini yang menjadi dasar berbagai lisensi yang sifatnya terbuka, open source, seperti GNU, GPL, Apache License dll; 3) **Tidak pernah percaya autoritas** – percaya pada desentralisasi; 4) **Seorang *hacker* hanya di nilai dari kemampuan hackingnya**, bukan kriteria buatan seperti gelar, umur, posisi, kekayaan atau suku bangsa; 5) Seorang ***hacker* membuat seni** & keindahan di komputer; 6) Seorang *hacker* percaya bahwa **komputer dapat mengubah hidup kita menjadi lebih baik**.

bisa menjamin para profesional *Information Security* dengan berbagai perlengkapannya dan pendidikan yang bisa membantu mereka mencegah terjadinya *cyberwar*, menurut mereka hal ini semestinya diadakan.

Hasil dari riset tersebut mengecewakan mereka dan hal itu memotivasi mereka untuk membentuk *International Council of Electronic Commerce Consultants*, yang dikenal dengan sebutan EC-Council. Dengan segera mereka mendapatkan dukungan berbagai hal yang diperlukan para ahli dari berbagai belahan dunia yang secara serta-merta mengarahkan kepada penciptaan berbagai standar dan sertifikasi yang keduanya dalam lingkup *electronic commerce* dan *information security*.[192]

Ketakutan akan terjadinya cyberwar ini juga terus dikembangkan oleh negara-negara maju dengan membentengi sistem keamanan mereka. Inggris, sebagaimana disampaikan dalam Guardian.co.uk, tengah membangun program *cyber-weapons* untuk menangkis berbagai tantangan *cyberwar*. Sampai menteri angkatan bersenjata Inggris, Nick Harvey, mengatakan kepada Guardian bahwa *"action in cyberspace will form part of the future battlefield,"*[193] Antisipasi mereka sungguh mengejutkan, memberikan gambaran tentang apa yang akan terjadi jika sistem suatu negara diserang, hingga diperlukan pembentukan program kokoh dengan analogi sebuah persenjataan untuk menghadapi perang *cyber*.

Lepas dari ketakutan akan terjadinya perang dalam benak negara-negara maju, di pihak EC-Council hingga kini terus

[192] EC-Council, "*History of The Company*", <http://www.eccouncil.org/about_us.aspx>, diakses pada 6 Juni 2011, pukul 22.00 WIB.

[193] Nick Hopkins, "UK Developing Cyber-Weapons Programme to Counter Cyber war Threat," <http://www.guardian.co.uk/uk/2011/may/30/military-cyberwar-offensive>, diakses pada 6 Juni 2011, pukul 00.00 WIB.

berusaha memberikan pendidikan dan sertifikasi untuk menciptakan ahli-ahli keamanan informasi yang beretika. Di dalamnya terdapat beraneka ragam jenis sertifikasi. Di antara yang populer adalah sertifikasi CEH (*Certified Ethical Hacker*), dan CHFI (*Computer Hacking Forensics Investigator*). Keduanya populer untuk para tenaga keamanan *cyber*. Dan dengan melihat materi yang ada di dalam sertifikasi dan pendidikan keduanya, sekiranya kita dapat mengetahui seperti apa kemampuan umum para *hacker*.

Pertama, *certified ethical hacker*, dalam pendidikan dan kelulusan sertifikasinya seseorang harus memahami dan mampu mengaplikasikan beberapa bagian pengajaran: *1) introduction to Ethical Hacking; 2) Footprinting and Reconnaisance; 3) Scanning Networks; 4) Enumeration; 5) System Hacking; 6) Trojans and Backdoors; 7) Viruses and Worms; 8) Sniffers; 9) Social Engineering; 10) Denial of Service; 11) Session Hijacking; 12) Hijacking Webservers; 13) Hacking Web Applications; 14) SQL Injection; 15) Hacking Wireless Networks; 16) Evading IDS, Firewalls, and Honeypots; 17) Buffer Overflow; 18) Cryptography; 19) Penetration Testing.*[194]

Disana dijelaskan bahwa CEH ini diperuntukkan bagi pegawai *security, auditors, security professionals, site administrators,* dan siapa saja yang berada dalam bidang berkaitan dengan integritas infrastruktur jaringan. Seorang lulusan CEH adalah seorang profesional terlatih yang memahami dan mengerti bagaimana mencari kelemahan dalam sistem milik target dan menggunakan pengetahuan yang sama dan peralatan yang sama seperti seorang *hacker* yang berbahaya.

[194] EC-Council, "*CEH Course Outline*," <http://www.eccouncil.org/training/professional_series/ceh_course_outline.aspx>, diakses pada 7 Juni 2011, pukul 01.30 WIB.

Kedua, *computer hacking forensics investigator*. CHFI adalah proses dalam mendeteksi serangan hacking dan secara teratur menjabarkan bukti untuk laporan kejahatan dan melakukan audit dengan maksud mencegah terjadinya serangan di masa yang akan datang. *Computer forensics* merupakan perangkat untuk *computer investigation* dan menganalisis tehnik-tehnik dalam maksud menentukan bukti-bukti hukum yang potensial. Bukti bisa dicari dalam jangkauan luas *computer crime* atau penyalahgunaan, termasuk tetapi tidak dibatasi pada pencurian dan rahasia dagang, pencurian atau perusakan intellectual property, dan penipuan.[195]

Dalam pendidikan dan sertifikasi CHFI, seseorang harus melewati 65 modul kajian mengenai *digital investigation: 1) Computer Forensics Today's World; 2) Computer Forensics Investigation Process; 3) Searching and Seizing of Computers; 4) Digital Evidence; 5) First Responder Procedures; 6) Incident Handling; 7) Computer Forensics Lab; 8) Understanding Hard Disk and File Systems; 9) Digital Media Devices; 10) CD/DVD Forensics; 11) Windows Linux Macintosh Boot Process; 12) Windows Forensics I; 13) Windows Forensics II; 14) Linux Forensics; 15) Mac Forensics; 16) Data Acquisition and Duplication; 17) Recovering Deleted Files and Deleted Partitions; 18) Forensics Investigations Using Access Data FTK; 19) Forensics investigations Using Encase; 20) Steganography; 21) Image Files Forensics; 22) Audio Files Forensics; 23) Video Files Forensics 24) Application Password Crackers; 25) Log Capturing and Event Correlation; 26) Network Forensics and Investigating Logs; 27) Investigating*

[195] EC-Council, "*CHFI Course Outline*," http://www.eccouncil.org/training/professional_series/chfi_course_outline.aspx, diakses pada 6 Juni 2011, pukul 01.30 WIB.

*Network Traffic; 28) Router Forensics; 29) Investigating Wireless Attacks; 30) Investigating Web Attacks; 31) Investigating DoS Attacks; 32) Investigating Virus, Trojan, Spyware and Rootkit Attacks; 33) Investigating Internet Crimes; 34) Tracking Emails and INvestigating Email Crimes; 35) PDA Forensics; 36) Blackberry Forensics; 37) iPod and iPhone Forensics 38) Cell Phone Forensics; 39) USB Forensics; 40) Printer Forensics; 41) Investigating Corporate Espionage; 42) Investigating Computer Data Breaches; 43) Investigating Trademark and Copyright Infringement; 44) Investigating Sexual Harassment Incidents; 45) Investigating Child Pornography Cases; 46) Investigating Identity Theft Cases; 47) Investigating Defamation over Websites and Blog Postings; 48) Investigating Social Network Websites for Evedences; 49) Investigation Search Keywords; 50) Investigative Reports; 51) Becoming an Expert Witness; 52) How to Become a Digital Detective; 53) Computer Forensics for Lawyers; 54) Law and Computer Forensics; 55) Computer Forensics and Legal Compliance; 56) Security Policies; 57) Risk Assessment; 58) Evaluation and Certification of Systems; 59) Ethics in Computer Forensics; 60) Computer Forensics Tools; 61) Windows Based Command Line Tools; 62) WIndows Based GUI Tools; 63) Forensics Frameworks; 64) Forensics Investigation Templates; 65) Computer Forensics Consulting Companies.*[196]

Dalam situs EC-Council tersebut dijelaskan bahwa, CHFI merupakan pendidikan dan sertifikasi yang didesain secara spesifik terutama bagi: a) Anggota kepolisian dan penegak hukum lain; b) Anggota militer dan pertahanan; c) *e-Business*

[196] EC-Council, "*CHFI Course Outline*," <http://www.eccouncil.org/training/professional_series/chfi_course_outline.aspx>, diakses pada 6 Juni 2011, pukul 01.30 WIB.

*Security professionals*; d) *Systems administrators*; e) Para profesional hukum; f) Para profesional perbankan dan asuransi; g) Agen-agen pemerintah; h) Manager-manager IT.[197]

Kemampuan-kemampuan teknis tersebut dapat berlaku sebagai wawasan umum dalam komunitas *hacker*, tidak setiap orang memiliki bekal kemampuan teknis yang lengkap. Yang jelas adalah selalu terdapat pembelajaran tentang kemampuan teknis dari yang sudah mahir kepada yang membutuhkan secara *peer-to-peer*, atau melepas tutorial secara bebas di dalam *forum* atau *group.*[198]

**4) Komunitas *Underground* Indonesia**

Tidak banyak yang mengetahui tentang aktifitas komunitas *underground* di Indonesia, padahal sebetulnya cukup transparan di Internet dan dapat di lihat aktifitas nyatanya. Sebagian aktifitas rekan-rekan *underground* ini kadang tergolong unlegal, seperti, carding dan deface web. Akan tetapi sebetulnya banyak sekali aktifitas mereka yang sangat positif terutama dalam pengembangkan sumber daya manusia dan *programmer*/*hacker* IT yang handal.[199]

Dulu para *underground* banyak melakukan chatting mengunakan IRC di DALNET dll. Pada masa lalu di IRC, proses arsip dan keanggotaan diskusi tidak terlalu terstruktur sebagian besar ilmu yang berkembang dari chatting akan hilang karena

---

[197] EC-Council, "*CHFI Course Outline*," <http://www.eccouncil.org/training/professional_series/chfi_course_outline.aspx>, diakses pada 6 Juni 2011, pukul 01.30 WIB.

[198] Dalam komunitas penggemar hacking yang terbuka untuk umum dan sudah populer, seperti Jasakom-Perjuangan dan Yogyafree-Perjuangan, di dalam forum dan *group* (group.yahoo) dapat dengan mudah ditemukan berbagai pelajaran (tutorial) tentang berbagai hal yang ditanyakan yang merupakan balasan (jawaban) dari yang mengetahui permasalahan, dan terus mengamati forum/group tersebut.

[199] Onno W. Purbo, "Komunitas *Underground* Indonesia 2006," <http://opensource.telkomspeedy.com/wiki/index.php/Komunitas_*Underground*_Indonesia_2006>, diakses pada 6 Juni 2011, pukul 02.00 WIB.

tidak terarsip. Pada saat ini, satu media komunikasi yang lumayan banyak digunakan untuk diskusi para *hacker* adalah mailing list terutama di yahoogroups.com yang dapat di akses melalui Web di http://groups.yahoo.com. Dengan melakukan search sederhana di http://groups.yahoo.com, kita akan menemukan beberapa komunitas *hacker* Indonesia yang lumayan aktif. Di samping komunitas *hacker* maupun programmer yang sifatnya lebih ke software, ada beberapa komunitas para geek lainnya yang lebih ke elektronik maupun system administrator. Di sisi yang membosankan, kita juga akan melihat beberapa komunitas diskusi yang lebih ke politik kadangkala terlalu mengawang tentang teknologi informasi di Indonesia.[200]

| **Nama** | **Jumlah Anggota** | **Berdiri** |
|---|---|---|
| **Komunitas IT & Politik** | | |
| genetika | 2205 | 6 Januari 2001 |
| telematika | 1750 | 14 Juli 1999 |
| mastel-anggota | 337 | 13 September 2000 |
| **Komunitas Sistem Administrator** | | |
| asosiasi-warnet | 6241 | 14 April 2000 |
| Ilmukomputer-networking | 5636 | 6 Desember 2003 |
| It-center | 4889 | 22 April 2000 |
| Indowli | 4766 | 3 Februari 2000 |
| **Komunitas Geek Elektronik** | | |
| orari-news | 1242 | 1 Februari 2001 |
| pcrakitan | 829 | 12 Februari 2005 |
| elpop | 583 | 12 Maret 2001 |
| **Komunitas Programmer** | | |
| IlmuKomputer-programming | 5226 | 6 Desember 2003 |
| Indoprog-vb | 5215 | 8 Maret 2001 |
| Delphindo | 2844 | 21 Februari 2001 |
| Jug-indonesia | 1783 | 12 April 2003 |
| Csharp-indo | 699 | 21 Januari 2002 |
| **Komunitas *Hacker* & Virus** | | |
| Jasakom-perjuangan | 12278 | 28 Februari 2003 |
| Newbie-*hacker* | 5636 | 11 Juli 2003 |

[200] *Ibid*.

| | | |
|---|---|---|
| Majalahneotek | 5633 | 19 Juli 2000 |
| Vaksin | 3388 | 1 Desember 2000 |
| Yogyafree | 2251 | 25 April 2005 |
| Indocrack | 1175 | 12 Februari 2005 |
| bandunghack | 1046 | 9 Agustus 2004 |

*Tabel 3.1 Komunitas underground di Indonesia (2006).*[201]

Data tahun 2006 telah banyak berubah, dan mengalami perkembangan pesat, baik dalam jumlah anggotanya, maupun jumlah komunitas-komunitas baru yang terus bermunculan. Sebagaimana dijelaskan tentang subculture yang cenderung tumbuh pada masa remaja, pembelajaran para remaja dan kesadaran mereka terhadap teknologi yang terus meningkat dari generasi ke generasi memberikan potensi kian besarnya kuantitas dan kualitas per-individu dalam komunitas dan juga dalam menumbuhkan komunitas-komunitas *underground* baru.

Tetapi tak hanya *underground-hacker* yang bertumbuh, akan tetapi komunitas *underground* lain juga memiliki potensi yang sama, yang masih tetap berkaitan dengan *cyber technology*. Berikut adalah revisi dari beberapa komunitas di atas dan beberapa komunitas *underground* baru:

| **Nama Komunitas** | **Jumlah Anggota** |
|---|---|
| Yogyafree (yogyafree-perjuangan)<br>(xcode.or.id/) | 5491 (yahoo.groups)<br>8502 (facebook/group) |
| Jasakom (jasakom-perjuangan)<br>(jasakom.com/) | 82481 (jasakom/forum, aktif: 3842)<br>2552 (facebook/group) |
| *Hacker* Cisadane<br>(*hacker*-cisadane.org/)<br>(berdiri: Februari 2010) | 2341 (forum.*hacker*-cisadane.org)<br>1743 (facebook/page) |
| Indonesian*hacker*<br>Indonesian*hacker*.or.id/) | 226207<br>(indonesian*hacker*.or.id/forum, aktif: 79631) |

[201] *Ibid*.

| | |
|---|---|
| Echo<br>(wiz.echo.or.id) | 38138 (echo.or.id/forum)<br>711 (facebook/group) |
| Malangcyber Crew<br>(mc-crew.info/) | 907 (facebook/group) |
| Magelangcyber Team<br>(magelangcyber.web.id/) | 256<br>(magelangcyber.web.id/defacer) |
| Devilzc0de<br>(devilzc0de.org/) | 10836 (devilzc0de.org/forum) |

*Tabel 3.2 Komunitas underground-hacker di Indonesia (2011).*[202]

Terlihat bahwa komunitas-komunitas *underground* tersebut di atas adalah beberapa yang bisa diamati aktifitasnya dengan cara menjadi anggota atau menjadi pengunjung untuk mencari informasi dan berbagai tutorial mengenai *cyber-technologies* dan berbagai permasalahannya. Terkadang untuk menjadi anggota komunitas *hacker-underground* tertentu, yang sifatnya tertutup tidak bisa dengan mudah mendaftar masuk dengan sekedar kemampuan teknis, tetapi lebih cenderung karena adanya *referral*.[203]

Tidak semua komunitas yang populer bisa terdata dengan baik, sebagian mereka menggunakan halaman facebook (facebook/page), yang tidak bisa menjadi patokan aktifitas komunitas. Terdapat pula komunitas yang cukup populer dan hanya diikuti oleh banyak *hacker* yang bersifat umum, tetapi tidak dapat didata jumlah anggotanya, yaitu "*Indonesiancoder Team.*" Dan terdapat beberapa komunitas lama yang disebutkan oleh Onno W. Purbo yang sudah tidak aktif lagi, atau juga yang

[202] Data ini didapatkan dengan menjelajahi situs masing-masing komunitas dan mengamati kegiatannya. Akses secara terus-menerus dari hari ke hari terus bertambah jumlahnya dan terus memodifikasi layanannya kepada para anggota. Diakses pada masing-masing situs dan jejaring tiap-tiap komunitas, pada 8 Juni 2011.

[203] Wawancara dengan BD, 11 April 2011. Referral, cara menjadi anggota dengan satu anggota menyarankan kepada leader komunitas tentang seorang calon anggota team. BD mencontohkan "Indonesian Coder Team".

dahulunya memiliki publikasi berupa majalah *hacker*, seperti Neotek, yang sudah tidak menerbitkan. Cukup menarik perhatian adalah beberapa komunitas yang sudah cukup senior, seperti Yogyafree, Jasakom, devilzc0de, ataupun echo, memiliki ruang yang leluasa bagi para anggota untuk berkomunikasi secara online dengan menciptakan forum dan berbagai jejaring sosial (khususnya devilzc0de, yang memiliki 'facebook'nya sendiri), yang memudahkan dan menciptakan kenyamanan bagi para pengunjung yang terregistrasi dalam komunitas untuk mencari informasi dan menanyakan tentang berbagai permasalahan seputar spesialisasi komunitas dan mengajukan pertanyaan untuk saling berbagi pengetahuan.

Dalam komunitas *underground*-lah kita dapat melihat bagaimana proses pemurnian informasi dijalankan, dan bagaimana pengetahuan diciptakan dan dibagikan, kemudian mengalami beberapa revisi sesuai dengan pengalaman yang diterapkan terhadap pengetahuan tersebut secara terus-menerus. Demikianlah manfaat dari komunitas secara umum dalam *cyberspace*, akan tetapi kekhasan *underground community* adalah mereka membahas hal-hal yang pada mulanya dianggap tabu dalam masyarakat teknologi saat usianya muda. Akan tetapi kini kebutuhan akan *cybersecurity* dan berbagai keahlian dan pengetahuan yang melingkupinya merupakan hal umum bagi setiap mereka yang sering berlalu-lalang dalam ruang maya.

Onno W. Purbo memberikan beberapa contoh *founder* komunitas *cyber* beserta karya mereka dalam situs mereka:

| | |
|---|---|
| S'to | http://jasakom.com/sto/ |
| Xnuxer | http://xnuxer.or.id/ |
| Jim Geovedi | http://jim.geovedi.com/ |
| Irvan | http://irvan.or.id/ |
| Y3dips | http://y3dips.echo.or.id/ |

Ciri khas *hacker-hacker* kelas elit adalah publikasinya yang bukan main banyaknya, sebagian dalam bentuk buku, sebagian dalam bentuk e-Zine sebagian lagi dalam bentuk presentasi-presentasi bahkan di forum-forum internasional seperti yang dilakukan oleh Jim Geovedi.[204] Namun kini seiring berkembangnya jumlah komunitas *hacker* dan masyarakat yang dengan inisiatifnya sendiri berusaha menjadi bagiannya, baik mereka dengan tujuan untuk menjadi pintar mengenai hacking, atau untuk mencari solusi, maka kemudian juga terus bermunculan tokoh-tokoh baru *cyberworld* yang pakar dalam bidang IT dan permasalahannya. Para *founder* dan keahliannya adalah layaknya CEO perusahaan dan kelihaiannya dalam meningkatkan produktifitas, bukan hanya dirinya, tetapi juga ruang komunitas dan para anggotanya.

Komunitas *underground* juga memiliki berbagai varian karakter dan bentuk keakrabannya, tidak semua komunitas bisa bertemu di darat. BD menjelaskan bahwa, kebanyakan komunitas *underground* seringkali menjadikannya sekedar komunitas dan organisasi yang wujudnya maya, tetapi hanya sedikit yang mampu bertemu secara langsung satu sama lain dan mengenal anggotanya satu sama lain.[205] Berbeda dengan Magelangcyber yang satu sama lain benar-benar saling mengenal dan akrab di dunia nyata, PZ menjelaskan tentang kenyataan komunitas Jasakom dan *Hacker* Cisadane,

> "Jangan tanya di daratnya ya. Jangankan HC (*Hacker* Cisadane) yang baru-baru ini hidup, Jasakom saja yang sudah lama. Kalau di darat pasti sedikit orangnya. Ini

[204] Onno W. Purbo, "Komunitas *Underground* Indonesia 2006," <http://opensource.telkomspeedy.com/wiki/index.php/Komunitas_*Underground*_Indonesia_2006>, diakses pada 6 Juni 2011, pukul 02.00 WIB.

[205] Wawancara dengan BD, 11 April 2011. BD memberikan contoh adalah komunitas Magelangcyber yang satu sama lain sudah saling mengenal. Mereka memiliki agenda diskusi dan pertemuan (Kopi-darat) untuk mempertemukan satu anggota dengan seluruh anggota komunitas.

> umumnya berlaku di semua komunitas *online*. Hampir pasti itu. Makanya terkenal dengan istilah L4, *lo lagi lo lagi*."[206]

Biasanya, hal ini terpaut dengan permasalahan geografis dan jumlah anggota. Komunitas *hacker* yang memiliki jumlah anggota relatif sedikit (masih dalam hitungan ratusan, tidak sampai ribuan), dan dalam lingkup satu kota atau antar-kota yang bersebelahan, tentunya akan lebih sering bertemu dan memiliki ikatan emosional yang lebih tinggi antara tiap individunya.

Di lain komunitas bisa memiliki karakteristik yang berbeda lagi, PZ mencontohkan komunitas *Hacker* Cisadane yang ia pimpin bahkan memiliki berbagai aktifitas sosial memberi pendidikan kepada masyarakat berupa seminar amal yang oleh Detikinet.com diberitakan dengan judul "Forum *Hacker* Cisadane: Nama 'Seram' dengan Kegiatan Positif."[207] Pada akhirnya memang seperti yang diisyaratkan oleh Onno W. Purbo, BD, dan PZ, bahwa semua tergantung moralitas dan baik-buruknya pencitraan *hacker* akan kembali kepada pribadi masing-masing.

> "Menurut saya orang yang gabung kan banyak "alirannya". Ada yang *white, black*, dan *grey*, sepertinya saya masuk dalam kategori ini, karena saya bukan malaikat, bukan juga setan. Tapi di antaranya."[208]

Pada kenyataannya tidak selamanya bisa ditegaskan bahwa secara konsisten seseorang, baik itu *hacker* atau tidak, akan selalu berada dalam garis lurus, terlebih lagi saat masih dalam tahap pencarian identitas. Ada yang sedang mencari peran dalam komunitas dan ada pula yang hanya sekedar ini mengetahui hal-hal yang membuat seseorang tertarik. Berada dalam komunitas

---

[206] Wawancara dengan PZ, 19 April 2011.

[207] http://www.detikinet.com/read/2010/10/14/163749/1465203/404/forum-*hacker*-cisadane-nama-seram-dengan-kegiatan-positif, diakses pada 19 April 2011.

[208] Wawancara dengan PZ, 19 April 2011

dan mempelajari hacking butuh stamina dan konsistensi untuk belajar tanpa henti, bisa jadi seseorang berhenti belajar dalam suatu komunitas dan keadaan itu masih tetap dihargai bagi komunitas.

> "… anggota forum kan tidak semua terjun langsung, ada yang cuma sekedar ingin tahu ada yang cuma belajar. Adapun member aktif, cuma dia *non-deface*, *non-hacking*, untuk itu ya cuma belajar *aja*, banyak *kaya* gitu."[209]

Mayoritas komunitas *hacker* di Indonesia mungkin masih tergolong terbuka untuk umum dalam menerima keanggotaan, baik aktif maupun tidak aktif. Karena mereka memiliki organisasi dan komunikasi yang general serta tidak membebani administrasi seperti di dunia maya berapa pun jumlah anggotanya.

> "Orang kan ada yang merasa bosan dengan itu, "ah paling cuma segitu", padahal yang namanya *security kaya gitu* kan setiap saat *update*."[210]

BD menjelaskan bahwa terkadang ada anggota, dalam komunitas *hacker* yang seluruh anggotanya serius untuk terus belajar, yang berhenti belajar hal-hal baru. Padahal teknologi dan muslihat yang ada di dunia maya terus berkembang dan mengalami perubahan dari waktu ke waktu, dan secara konsisten harus senantiasa diasah dan direvisi ulang tehnik-tehniknya. Sebagaimana uji kemampuan yang disertifikasi oleh EC-Council terhadap *Certified Ethical Hacker* (CEH) selalu mengalami perkembangan dari tahun ke tahun.

### *3.2 Cybercrime*

Luasnya ruang *cyber* yang tidak terbatas ini menjadikan tidak mudahnya menjangkau pelaku kejahatan di dalamnya, namun tidak berarti aktivitas ruang

[209] Wawancara dengan BD, 11 April 2011.
[210] *ibid*.

*cyber* dibiarkan tanpa hukum. Di Indonesia suatu perbuatan dapat dijatuhi pidana apabila telah memenuhi rumusan delik. Namun hal ini tidak selalu suatu perbuatan dapat dijatuhi pidana jika memenuhi rumusan delik saja, di samping itu terdapat ketentuan, yaitu perbuatan tersebut: (a) merupakan perbuatan manusia; (b) bersifat melawan hukum; (c) perbuatan tersebut dapat dicela.[211]

Penjelasan singkat tentang perluasan pengertian tentang dapat dipidananya suatu perbuatan tersebut kiranya dapat membantu dalam menangani permasalahan pidana dalam ruang mayantara. Di Indonesia dalam permasalahan perundang-undangan yang terkait erat dengan tindak pidana di ruang *cyber* masih terbatas jumlahnya. Satu peraturan perundang-undangan yang secara khusus menjurus kepada aktifitas dalam teknologi informasi dan memuat beberapa larangan terkait *cybercrime* adalah Undang-undang Nomor 11 Tahun 2008 tentang ITE (Informasi dan Transaksi Elektronik). Akan tetapi pendefinisiannya sebagai undang-undang khusus tentang tindak pidana mayantara (*cybercrime*) belum dapat dijelaskan dengan baik.

Perlunya perbaikan filosofis masih terbuka bagi UU ITE. Hukum sebagai keseluruhan aturan tingkah laku yang bertujuan mencapai ketertiban dalam masyarakat mengharuskan adanya ketegasan, kejelasan, dan ketepatan dalam penyusunan kalimat. Di samping itu, dituntut pula adanya konsistensi. Semua itu dimaksudkan untuk mencegah agar perumusan norma hukum tidak menimbulkan kemaknagandaan dan kesamaran, sehingga menjamin kepastian hukum.[212] Kejelasan delik juga akan memberikan ketegasan dalam penegakan hukumnya.

Dalam UU ITE tersebut masih memiliki keterbatasan dalam mendefinisikan delik, keterbatasan ini menciptakan kekhawatiran tentang ketidakmampuan dalam pelaksanaannya. Delik-delik yang ada di dalam UU tersebut belum mampu mencakup keseluruhan aktivitas *cybercrime* yang dapat memasuki berbagai bidang kehidupan modern. *Cybercrime* dapat mencakup

---

[211] Rapin Mudiardjo, "Kajian Aspek Pidana", dalam Edmon Makarim, *Pengantar Hukum Telematika: Suatu Kajian Kompilasi*, (Jakarta: Rajagrafindo Persada, 2005), hal. 419.

[212] Anggara, Supriyadi W.E., dan Ririn Sjafriani, *Kontroversi Undang-undang ITE: Menggugat Pencemaran Nama Baik di Ranah Maya*, (Jakarta: Degraf, 2010), hal. 66.

kejahatan di semua aspek kehidupan manusia, termasuk semua bentuk kejahatan tradisional seperti dalam KUHP.[213]

Dapat diambil satu aktivitas *cybercrime* yang terkait dengan berbagai pasal dalam KUHP, yaitu mengenai *hacking*. Dalam kejahatan dengan memanfaatkan internet sebagai media, hacking komputer sebagai aktivitas awal (perbuatan awal) sebelum seseorang melakukan suatu tindak pidana, seperti mencari dan menyadap sistem komputer, menyadap *password*. Setelah diperoleh "kunci masuk", yang bersangkutan dapat melakukan tindakan yang merupakan perwujudan dari niat (*intention*), yang dilakukan dapat berupa memasuki atau melewati sistem (tresspass) seperti yang tertuang dalam Pasal 167 KUHP, melakukan pencurian (362 KUHP), pembocoran rahasia negara (112, 113, 114 KUHP), pembocoran rahasia perusahaan (322, 323, 431 KUHP) yang dapat dikategorikan *data diddling*, penghinaan (310 KUHP), pengrusakan sistem (*cracking*) (406 KUHP).[214]

Keterkaitan satu aktivitas *cybercrime* dengan sedemikian banyak delik dalam KUHP memperlihatkan bahwa dalam menciptakan suatu produk hukum khusus *cybercrime*, diperlukan pula pendefinisian delik-deliknya secara lebih spesifik. Dalam *Cybercrime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors,* Anthony Reyes menjelaskan:

> *How about if I told you that John committed the act of cyber stalking? Would it have the same effect if I had stated just the word "stalking"? In these two examples, we remove the element of the crime from its traditional meaning when using cyber terminology. When we use these terms, the underlying crime definition weakens, and the impact or shock value it has on us is reduced*.[215]

---

[213] Lihat, Barda Nawawi Arif, *Tindak Pidana Mayantara*, (Jakarta: Raja Grafindo Persada, 2006), hal. 42-43.

[214] Mudiardjo, *op.cit*., hal. 419.

[215] Anthony Reyes, et.al, *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors*, (Rockland, MA: Syngress Publising, 2007), hal. 9.

Demikianlah pada kenyataannya, definisi kejahatan di dunia darat sungguh berbeda,[216] dan akan menyederhanakan kerumitan dalam definisi *cyber*, jika diterapkan begitu *saja*. Menjelaskan pemahaman tersebut kepada publik bukanlah hal yang mudah, terlebih untuk menjabarkannya dalam pemahaman yang baru, atau setidaknya bentuk kejahatannya telah mengalami peningkatan (*up-grade*) dalam bentuk dan definisinya.

Masalah lain yang dihadapi ketika memakai terminologi *cyber* adalah kecenderungan menyimpulkan bahwa kejahatan tidak terjadi secara lokal dan korban tidak berada dalam ancaman yang bersifat darurat. Dunia *cyber* cenderung menempatkan dirinya pada sebuah ketidaknyataan atau kesalahan dan tempat yang jauh. Dari semua itu, *cyberspace* tidaklah nyata secara fisik, *cyberspace* adalah ruang virtual[217]. Satu lagi pemahaman yang bisa jadi bermasalah dengan menjelaskan bahwa kejahatan di dunia maya dapat dihentikan atau tidak bisa dijalankan saat seseorang tidak dapat mengakses komputer pada saat bersamaan kejahatan itu terjadi di dunia *cyber*. Karena dalam teknologi *cyber* pengelolaan waktu dilakukannya suatu tindakan bisa dengan otomatisasi (sebagaimana pengaturan bom waktu), dan dengan otomatisasi memungkinkan suatu tindakan berjalan terus-menerus walaupun si manusianya tidak lagi mengaksesnya. Dalam pemahaman ini Anthony Reyes menjelaskan:

> *Lastly, when we place the act of crime in a separate cyber category, we infer that it only happens when a computer exists. As you know, this is far from the truth. Often, you can clearly prove a crime has been committed even after removing the computer from the cyber crime itself.*[218]

Anthony Reyes[219] memiliki *banyak* pengalaman dalam hal penanganan *cybercrime* di Amerika Serikat, dan oleh karenanya penjelasannya tentang

---

[216] Saya meminjam diksi dari beberapa *hacker* yang membedakan dunia maya dengan dunia nyata dengan 'maya' dan 'darat'. Mungkin dalam pilihan istilah komunikasi, itu menjelaskan tentang *off air* (tidak mengudara/ di darat) dan *on air* (meng-'udara').

[217] Reyes, *op.cit.*, hal. 10.

[218] Ibid.

[219] Pada halaman awal dari buku "*Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors*" dijelaskan tentang Anthony Reyes dan pengalamannya:

kerumitan dalam permasalahan perubahan definisi kejahatan konvensional kepada kejahatan mayantara lebih dekat dalam kenyataan.

Permasalahan yang lebih mendominasi dan menyebabkan banyaknya kasus kejahatan mayantara, menurutnya adalah karena tindak-tindak kejahatan di dalamnya tidak dipandang *dengan* serius sebagai sebuah *"true crime"*. Untuk menghindari hal ini, kiranya para penegak hukum harus berusaha menguraikan kejahatan mendasar yang telah dilakukan saat menyebut suatu kejahatan *cyber* untuk seorang pemula.[220]

Jadi penjelasan yang 'diinginkan' oleh Anthony Reyes adalah, agar pemahaman mengenai tindak kejahatan mayantara dapat disebut sebagai sebuah kejahatan saat komputer hadir sebagai alat bantu dalam melakukan suatu tindak kejahatan. Atau jika ada definisi kejahatan di dalam hukum konvensional (*non-cyber*) akan didefinisikan sebagai sebuah *cybercrime*, maka jangan menyebutnya sebagai sebuah *cybercrime* sebelum dapat menjelaskan bahwa di dalam melakukannya melibatkan komputer sebagai bagian dari tindakan itu.

Ketidaksederhanaan *cybercrime*, jika memakai definisi kejahatan *non-cyber* akan memberikan kenyataan yang sulit bagi model penegakan hukum konvensional, Anthony Reyes menjelaskan tentang sulitnya objektifitas dalam pengertian *cybercrime*, jika melulu menanganinya dengan bentuk-bentuk definisi *non-cyber*, dikarenakan penanganan *cybercrime* harus menyadari kenyataan yang meliputi beberapa logika berikut:

---

*Anthony Reyes is a retired New York City Police Department Computer Crimes Detective. While employed for the NYPD, he investigated computer intrusions, fraud, identity theft, child exploitation, intellectual property theft, and software piracy. He was an alternate member of New York Governor George E. Pataki's Cyber-Security Task Force, and he currently serves as President for the High Technology Crime Investigation Association. He is the Education & Training Working Group Chair for the National Institute of Justice's Electronic Crime Partner Initiative. Anthony is also an Associate Editor for the Journal of Digital Forensic Practice and an editor for The International Journal of Forensic Computer Science.*

*He is an Adjutant Professor and is the Chief Executive Officer for the Arc Enterprises of New York, Inc. on Wall Street. Anthony has over 20 years of experience in the IT field. He teaches for several government agencies and large corporations in the area of computer crime investigations, electronic discovery, and computer forensics. He also lectures around the world.*

Anthony Reyes, et.al, *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors*, (Rockland, MA: Syngress Publising, 2007), hal. v.

[220] *Ibid*., hal. 10.

- *The proliferation of PCs and Internet access has made the exchange of information quick and inexpensive.*
- *The use of easily available hacking tools and the proliferation of underground hacking groups have made it easier to commit cyber crimes.*
- *Anonymity allows anyone to hide his identity while committing crimes.*
- *E-mail spoofing, creating fake profiles, and committing identity theft are common occurrences, and there is nothing to stop it, making investigation difficult.*
- *With cyber crimes, there is no collateral or forensic evidence, such as eye witnesses, fingerprints, or DNA, making these crimes much harder to prosecute*.[221]

Beberapa contoh yang disampaikan pada kenyataannya adalah apa yang tumbuh dan berkembang dalam ruang *cyber* (*cyberspace*), tak terkecuali di Indonesia. Kini tiap negara memiliki tantangan yang sama dalam menghadapi bentuk-bentuk kejahatan dalam dunia maya yang memengaruhi apa yang kita punyai di dunia nyata. Memang kesadaran tentang kemajuan peningkatan kebutuhan manusia tentang komputer dan akses internet merupakan hal yang secara umum disampaikan sebagai pengantar tentang resiko kita dalam menghadapi keniscayaan kebutuhan akan teknologi dan kejahatan yang bersembunyi di dalamnya.

Namun empat hal berikutnya, yang disampaikan oleh Reyes, belum dipahami secara umum oleh publik. Walau bagaimanapun, satu demi satu semuanya akan menjadi keniscayaan yang semestinya disadari publik, seiring dengan perkembangan kebutuhan dan peningkatan ketergantungan dengan *cyberspace*. Terlebih dalam penegakan hukum, dalam menghadapi permasalahan dan menyelesaikannya dengan sebaik mungkin.

Perkembangan teknologi komputer dan internet berpotensi memberi celah yang lebih banyak bagi kejahatan untuk menyisipi kelemahan keamanan di

[221] *Ibid*.

dalamnya. Di sisi lain pelaksanaan *law-enforcement* serta upaya investigasi terhadap kejahatan yang dilakukan terus terjadi setiap hari. Gambaran ini memberikan tantangan yang tidak habis-habisnya bagi mereka yang selalu berjuang menegakkan hukum.

Peningkatan jumlah individu yang terhubung dengan internet, dan meningkatnya kejahatan dengan jumlah pelaku potensial yang cenderung meningkat, tidak hentinya menebarkan kekhawatiran publik mayantara dalam melakukan aktifitasnya, terutama yang berkaitan erat dengan ekonomi, kebutuhan pokok, hingga privasi.

Dalam menjelaskan mengenai kejahatan mayantara (*cybercrime*) terdapat beberapa pemahaman yang perlu diperjelas bagi siapa saja yang tertarik menelaahnya. Bagi mereka yang kesehariannya berurusan erat dengan dunia maya tentu sebagian penjelasan akan menjadi hal yang biasa, dan sebagian mungkin hanya didapati dalam pembahasan di wilayah hukum. Bagi yang benar-benar baru dalam *cyberspace,* mungkin akan memberikan beberapa kejutan di dalamnya, betapa perubahan pemahaman bentuk kejahatan dari dunia nyata ke dalam dunia maya memiliki konsekuensi yang tidak murah harganya, terlebih saat menyadari bahwa ketergantungan terhadap teknologi internet kian membesar.

### 3.2.1 Persepsi tentang *Cybercrime*

Terdapat beberapa contoh kejahatan yang memanfaatkan perkembangan alat telekomunikasi elektronik. Semenjak 1990-an Internet telah berkembang menjadi bagian kehidupan dari manusia di seluruh dunia, terutama mereka yang memiliki aktifitas di dunia Barat, yang lebih maju. Dengan penuh kewaspadaan, dan antusias terhadap, perubahan-perubahan tersebut telah ditampakkan oleh ketakutan-ketakutan akan bahaya-bahaya yang dimunculkan dan ancaman-ancaman yang datang bersama internet terhadap kehidupan dan keamanan kita.[222] Bersama munculnya internet

[222] Majid Yar, Cybercrime and Society, Sage Publication: London, 2006, hal. 3.

berkembang juga sebuah konsepsi dunia baru yang disebut dengan *cyberspace*.

*Cyberspace* menjadi ruang realitas dalam kehidupan yang terkomputerisasi, manusia berinteraksi di dalamnya dan hampir semua aktifitas telah terkomputerisasi. Yasraf Amir Piliang dalam essay pembuka dari "Post-Realitas" (Yasraf, 2010) mengatakan bahwa, *cyberspace* adalah ruang artifisial hasil konstruksi teknologis, yang di dalamnya ada relasi kompleks antara tanda dan realitas. Bila secara konvensional tanda menjelaskan relasi antara sesuatu yang menandakan (penanda) dan sesuatu yang ditandai (realitas), tanda di dalam *cyberspace* melampaui realitas itu. *Cyberspace* memungkinkan situasi bagaimana tanda tidak memiliki sama sekali relasi alamiah dan substansial dengan realitas. Tanda dibangun berdasarkan produksi mandiri dari dan untuk dirinya sendiri (*self production system*)—inilah tanda artifisial. *Cyberspace* menciptakan kondisi bagaimana tanda terputus dari realitas, dan membangun prinsip perujukan sendiri (*self-reference*), yang di dalamnya tanda tidak menunjuk pada sesuatu di luar dirinya, tetapi pada dirinya sendiri.[223]

Pemaparan Yasraf secara ringkas dan mendalam mampu menjelaskan relasi kuat antara dunia nyata dan ruang artifisial yang disebut *cyberspace*. Penjelasan semiotisnya memberikan penegasan kepada kita, bahwa pada akhirnya *cyberspace* benar-benar terlepas dari dunia nyata, karena ia mampu memproduksi tanda sendiri. Ini menyebabkan semua tanda tidak berhubungan sama sekali dengan realitas, tanda berputar dalam ruang virtual ini tanpa henti bereproduksi sendiri.

Kemandirian ruang virtual *cyberspace* ini memberikan jangkauan yang lebih luas dan leluasa kepada pelaku kejahatan untuk melakukan aksinya, dan sekaligus lebih cepat. Saat semua bisa dilakukan secara *remote* (kendali jarak jauh) maka resiko yang diambil jauh lebih kecil jika

[223] Yasraf Amir Piliang, *Post-Realitas: Realitas Kebudayaan dalam Era Post-Metafisika*, (Yogyakarta: Jalasutra, 2010), hal. xxxiii.

dibandingkan melakukan kejahatan di dunia nyata. Tindak kejahatan di dalam ruang virtual ini pun tidak lagi memperhitungkan jarak, bahkan waktu.

Memasuki sistem kehidupan baru sebagaimana halnya internet bukanlah sesuatu yang mudah bagi masyarakat secara luas. Pertengahan 1990-an adalah masa maraknya pembicaraan tentang ketakutan pada teknologi internet. Diinformasikan bahwa dengan menggunakan internet akan menjadikan setiap orang rentan terhadap berbagai bentuk baru tindak kriminal. Ketakutan-ketakutan tersebut semakin intensif dengan ketakutan akan Y2K "*Millennium Bug*", ketakutan yang tersebar di masyarakat adalah akan adanya sebuah kesalahan sederhana dalam desain sistem operasi komputer yang diperkirakan akan menyebabkan hancurnya instalasi-instalasi kunci dalam infrastruktur nasional.[224] Ketakutan akan keterbukaan dan potensi-potensinya dalam mengakses secara langsung ruang-ruang privat merupakan bentuk bayangan negativitas yang lazim dipahami dengan mengerti secara langsung bagaimana teknologi internet itu dibentuk.

Demikianlah dilema dari kemajuan teknologi komunikasi untuk kemudahan manusia itu sendiri, di dalamnya tetap terdapat ketakutan untuk membuka dan membiarkan orang lain mengetahui privasi kita. Semakin fragmen-fragmen intim diri kita menyingkapkan diri dalam kontak intersubjektif, semakin kita menyadari perbedaan kita satu sama lain sebagai seorang pribadi yang khas. Heterofobia yang muncul jelas berasal lebih dari gambaran yang salah tentang manusia lain yang timbul dari defisit kontak dan rasa takut untuk bersentuhan atau singkatnya: dari blokade komunikasi.[225]

Sekat-sekat yang saling terhubung oleh komunikasi kemudian seringkali menimbulkan keseimbangan dan rasa kebersamaan, dengan

[224] David S. Wall, ed., *Crime and The Internet,* (New York: Routledge, 2001), hal. 1-2.

[225] F. Budi Hardiman, *Memahami Negativitas: Diskursus tentang Massa, Teror, dan Trauma*, (Jakarta: Kompas, 2005), hal. 19.

keterbukaan itulah seseorang bisa seolah menjadi orang lain (empati). Empati dapat dijelaskan secara sederhana, bagaimana seseorang bisa menjadi bukan dirinya (Budi Hardiman: 2005). Dalam keterbukaan komunikasi itu jugalah diperlukan adanya kemampuan fragmentasi ruang, yaitu: kemampuan melipatgandakan ruang-ruang kontak dengan berbagai individu.[226] Dalam usaha untuk menghilangkan ketakutan akan keterbukaan, pada akhirnya kita melihat meningkatnya keterampilan tiap individu dalam berkomunikasi dalam ruang yang telah demikian terbuka. Yaitu keterampilan untuk mendeferensiasikan, memilah-milah antar tiap relasi dan menjadikannya selalu dapat berempati dengan yang lain secara keseluruhan. Hal inilah yang kemudian membangkitkan gerakan-gerakan sosial dalam era internet.

Sebagai contoh gerakan sosial adalah seperti yang dilakukan oleh blogger dan pengguna internet di Indonesia. Antara lain adalah gerakan 1.000 buku yang menyalurkan buku bagi mereka yang membutuhkan namun tidak punya biaya. Ada juga gerakan *Coin A Chance* pada kasus Prita. Ketika itu Prita didakwa dengan ancaman hukuman denda hingga Rp202 juta, tetapi gerakan sosial yang mengalir berhasil mengoleksi koin hingga sekitar Rp850 juta. Gerakan Indonesia Unite, yang muncul sejak tragedi bom di Hotel JW Marriot dan Ritz Carlton. Dan juga gerakan 'Satu juta Facebooker dukung pembebasan Bibit-Chandra.[227]

*Paranoia* (ketakutan) adalah munculnya gambaran tentang segala bentuk negativitas yang sudah terbayang, dari hal buruk yang menimpa mekanisme kehidupan hingga potensinya terhadap pelanggaran hak-hak dalam kehidupan. Seperti halnya dalam contoh kasus Prita Mulyasari yang memaksanya ke pengadilan karena dinilai telah mencemarkan nama baik

[226] *Ibid*.

[227] Muhammad Firman dan Muhammad Candra Taruna, "2009 Jadi Tonggak Sejarah Internet Indonesia," <http://teknologi.vivanews.com/news/read/168958-2009-jadi-tonggak-sejarah-internet-indonesia>, diakses pada 15 Desember, Pukul 14.00 WIB. (wawancara vivanews.com dengan seorang pengamat internet Indonesia, Enda Nasution).

sebuah institusi rumah sakit yang dia anggap melakukan malpraktik terhadap anaknya. Apa yang disebarluaskan oleh Prita bukanlah melalui forum terbuka yang bersifat konvensional, tetapi melalui forum dalam sebuah jejaring sosial internet, karena pembocoran keluhan Prita oleh salah satu teman dalam forum itulah yang menjadikannya harus membayar 202 juta rupiah. Ketakutan akan negativitas semacam ini kemudian melahirkan perhatian publik terhadap tekanan yang dialami Prita, beban Prita tidak hanya menjadi lebih ringan, empati yang datang dari publik akhirnya berhasil menggalang donasi untuk Prita melebihi dari yang diharapkan.

Meskipun contoh kasus Prita tidak secara keseluruhan ada di ranah ruang mayantara, namun persepsi masyarakat terhadap bentuk-bentuk kejahatan mayantara telah diberikan dengan banyaknya publikasi tentang permasalahan-permasalah hukum yang berkaitan dengan (atau yang kemudian memanfaatkan) dunia internet di berbagai media, dan efek yang diberikan adalah gerakan sosial yang bermunculan baik dengan maupun berada di luar jalur internet sebagai efek samping pemberitaan. Dan tanggapan publik adalah seiring dengan informasi media, atau bisa juga memberikan kritikan terhadapnya.

Media massa seperti televisi, radio, koran, dan majalah mengalami regenerasi dalam era internet, dalam bentuk yang lebih digital, seperti siaran televisi *video-streaming*, siaran *air*-radio, koran *downloadable printed edition*. Masyarakat lebih mudah mendapatkan informasi dengan lebih cepat dan juga berkomunikasi dengan lebih mudah.

### 3.2.2 Mendefinisikan *Cybercrime*

*Cybercrime merupakan* bagian dari kejahatan komputer. Definisi tentang *cybercrime* tidak dapat ditemukan secara khusus di dalam berbagai kamus populer yang beredar di masyarakat.[228] Tetapi setiap pemaparan

[228] Di dalam kamus Oxford sendiri tidak menjelaskan tersendiri apa itu *cybercrime*. Di sana menjelaskan tentang *cyberspace* sebagai: *imaginary place where electronic messages, pictures, etc. exist while they are being sent between computers.* Dan *cybersquatting* sebagai: *illegal activity of buying and officially recording an address on the internet that is the name of an existing company,*

tentang *cybercrime* cenderung memunculkan penjelasan yang beragam, menurut persepsi masing-masing pembahas. Meskipun demikian pemahaman tentang kata *cybercrime* sendiri tidak menuntut penjelasan terlalu khusus, atau setidaknya tidak memerlukan konsensus untuk menyepakatinya. Tetapi dengan memahami definisi tiap-tiap unsurnya serta bentuk-bentuknya semoga bisa cukup membantu.

Buku, media massa, atau melalui berbagai blog yang bertebaran di internet mungkin pernah memberikan gambaran kepada siapa saja tentang bagaimana *cybercrime* itu terjadi, dan keadaan seperti apa yang membuatnya mungkin dengan peralatan semisal komputer. Karena peretasan (*hacking*) pun dapat dilakukan dengan perangkat yang lebih sederhana, karena kini terus berkembang peralatan-peralatan (*gadgets*) yang merupakan penyederhanaan konsep komputer, menjadi lebih ringkas dengan tidak meninggalkan kemampuan komputer yang dimilikinya, demi prinsip ergonomis (*user friendly*) dan dinamis (*mobile*).

Perangkat *komputer* atau pun jaringan komputer dapat dilibatkan dalam tindak kejahatan dengan berbagai cara yang berbeda:

- *The computer or network can be the tool of the crime (used to commit the crime).*
- *The computer or network can be the target of the crime (the "victim").*
- *The computer or network can be used for incidental purposes related to the crime (for example, to keep records of illegal drug sales).*[229]

Penjelasan sederhana dan bersifat teknis ini memberikan fokus kepada definisi, bahwa tidak hanya komputer sendiri yang potensial sebagai alat *to commit the crime*. Pemakaian tambahan "*or network*"

---

*with the intention of selling it to the owner in order to make* money. Di dalamnya hanya dijelaskan bahwa kata *cyber-* adalah prefix yang bisa dikaitkan dengan kata apa saja, yang dengannya akan memiliki arti berhubungan dengan komunikasi elektronis, dan berkaitan dengan internet. Lihat, Victoria Bull, ed., *Oxford Learner's Pocket Dictionary*, 4th edition, (Oxford: Oxford University Press, 2009), hal. 111.

[229] Debra Littlejohn Shinder, *Scene of the Cybercrime: Computer Forensics Handbook*, (Rockland, MA: Syngress Publishing, 2002), hal. 5.

menjadi opsi penentu bahwa *cybercrime* bukanlah kejahatan komputer semata. *Cybercrime* dalam sebagian tindakan *commit to crime*-nya dilakukan dalam jaringan (*network*), baik intranet (*local*) maupun internet (*global*).

Memahami hal teknis dalam *cybercrime* memiliki cakupan yang amat luas dan membutuhkan basis data yang selalu terbarui, demikian juga kebaruan dalam pemahaman serta penjabaran permasalahan. Majid Yar (2006: 10) mengutip pendapat David S. Wall (2001: 3-7), menjabarkan empat hal yang menurut Wall *merupakan* empat wilayah yang merupakan aktifitas berbahaya, yaitu:

1. *Cyber-trespass – crossing boundaries into other people's property and/or causing damage, e.g. hacking, defacement, viruses.*
2. *Cyber-deceptions and thefts – stealing (money, property), e.g. credit card fraud, intellectual property violations (a.k.a. 'piracy').*
3. *Cyber-pornography – breaching laws on obscenity and decency.*
4. *Cyber-violence – doing psychological harm to, or inciting physical harm against others, thereby breaching laws relating to the protection of the person, e.g. hate speech, stalking.*[230]

David S. *Wall* dalam karyanya yang dikutip oleh Majid Yar menjelaskan masing-masing:

- *"(Cyber)-trespass"*, atau hacking/cracking, adalah pelanggaran tanpa hak dari batasan atas sistem komputer ke dalam ruang-ruang dimana hak-hak kepemilikan atau *tittle* yang telah *established*.
- *"(Cyber)-deceptions/thefts"*, mendeskripsikan perbedaan berbagai jenis upaya mendapatkan sesuatu secara berbahaya yang bisa terjadi di dalam *cyberspace*.

[230] Yar, *op.cit.*, hal. 10.

- *"(Cyber)-pornography/obscenity"*, sebagaimana makna yang ada, adalah merupakan penerbitan atau perdagangan material-material yang mengumbar seksualitas di dalam *cyberspace*.
- *"(Cyber)-violence"*, menjelaskan kejahatan yang berakibat pada aktifitas mayantara pihak lain terhadap individu atau kelompok politis.[231]

Empat pembidangan wilayah kejahatan yang dijelaskan oleh Wall ternyata dijelaskan dengan cara lain oleh Majid Yar, mungkin Yar hanya mengambil pemahamannya sendiri dengan istilah yang disebutkan oleh Wall. Ini memperlihatkan bahwa penjelasan tentang cybercrime, baik secara umum atau pun secara khusus berbeda-beda, namun kemudian berusaha dijabarkan oleh masing-masing *pemapar* dengan caranya sendiri untuk mendekati kebenaran dari konteksnya. Akan tetapi apa yang dimaksudkan oleh Wall terlihat berbeda dengan cara ia menuliskan tiap istilahnya. Kata *"cyber-"* sengaja ditulis dengan *"(cyber)-"*, bukan sekedar prefix, tetapi David S. Wall ingin menjelaskan bahwa, baik itu *trespass*, *deception/thefts*, *pornography/obscenity*, atau *violence*, merujuk pada karakter dan makna aslinya dalam dunia nyata. Karena kejahatan yang ada di dunia nyata ternyata dapat juga dilakukan melalui media internet.

### 3.2.3 Akibat dari *Cybercrime*

> *By breaking the analysis of cybercrimes down into different levels and types of impact, criminological debates can engage more clearly with the issues at hand. Furthermore, criminologists are then spared the frustation of comparing, for example, the "apples" of cyber-violence with, say, the "Tuesday" of cyber-theft. But while this taxonomy might usefully assist criminologists to sing from the same song sheet, the following impediments frustate their abilities to sing in tune and conduct research into cybercrimes.*[232]

Dalam teknis pembentukan sistem keamanan di dalam internet pada awalnya seorang programer akan bertindak sebagai seorang *hacker* dalam

[231] Wall, *op.cit.*, hal. 3-7.
[232] *Ibid*, hal. 7

menguji keamanan situs yang ia *kelola*. David Wall menjelaskan bahwa para *hacker* memerankan peranan yang penting dalam awal masa pembentukan konsep dari internet, mengkombinasikan pengetahuan tingkat tinggi yang terspesialisasikan untuk menguji dan membangun ide-ide baru dengan sebuah etika kuat yang meyakini kemerdekaan dalam mengakses semua informasi.[233]

Sebuah film yang menggambarkan tentang seberapa besar kerugian yang bisa muncul oleh *cybercrime* yang berdasarkan oleh kisah nyata, *"Takedown"*,[234] film yang dibintangi oleh Skeet Ulrich, menceritakan Kevin Mitnick dan upaya penangkapannya. Di dalam poster film tersebut saat diedarkan di Amerikan diberi judul "Track Down" dengan pengantar: *"Based on the incredible True Story of Catching America's #1 Computer Outlaw Kevin Mitnick!"*[235]

Film tersebut menuturkan tentang bagaimana Kevin Mitnick dengan ketertarikannya *yang* luar biasa berusaha mengungkap kesalahan sebuah perusahaan telekomunikasi Amerika. Dia berusaha mencuri sistem selular perusahaan tersebut, memanipulasinya. Tidak hanya sampai di sana, di dalam film juga digambarkan bahwa Kevin menemukan ada sebuah celah yang dengan teledor dibiarkan oleh teknisi perusahaan telekomunikasi tersebut, Tsutomu Shimomura.

Pada awal pembentukan sistem dalam jaringan perusahaan awalnya Tsutomu memang *mengujinya* dengan menerapkan semacam serangan

---

[233] Ibid., hal. 4.

[234] Lihat, http://www.takedown.com/, diakses pada 17 Mei 2011, 17.30 WIB. Dalam situs ini terdapat narasi tentang kejadian nyata, bukti-bukti rekaman terkait kasus Kevin Mitnick (http://www.takedown.com/evidence/index.html). Dari sisi Tsutomu Shimomura.

[235] (Lihat: http://www.imdb.com/title/tt0159784/, akses pada 17 Mei 2011, 17:00 WIB) Meskipun berdasarkan kisah nyata, namun film ini mendapat banyak protes keras dari para *hacktivists* di Amerika, meski dirilis pada tahun 2000 dengan judul "Takedown" namun di Amerika sendiri film ini baru dirilis pada 2004 dengan judul "Track Down". Berbagai sanggahan yang mendukung Kevin Mitnick, yang dinilai dalam film ini telah dipojokkan, datang kepada produsen film, Miramax. Film tersebut terlalu menjustifikasi hal-hal yang mendukung seorang yang dipersonifikasikan sebagai pakar teknologi dari perusahaan yang diserang Kevin, Tsutomu Shimomura, dan merendahkan/ memojokkan Kevin yang tidak dapat membela diri, yang saat film tersebut diproduksi (1998) masih berada dalam penjara, sedangkan Kevin Mitnick baru keluar dari penjara pada tahun 2000.

terhadap sistem dengan serupa virus/ trojan horse. Tetapi Tsotomu tetap menyimpan file virus itu di dalam sistem, yang kemudian dengan kemampuannya sebagai *hacker*, Kevin menemukannya dan berusaha mengungkapkan bahwa itu adalah kesalahan Tsutomu yang membiarkan kelemahan sistem terbuka dan menyimpan data yang bisa membahayakan sistem di dalamnya. Film tersebut kemudian mendapat perlawan dengan rilisnya film dokumenter tentang gerakan yang dilakukan Kevin Mitnick dan dunia *hacker*, dengan judul *"Freedom Downtime"*.[236]

Dari uraian singkat tentang kasus Kevin Mitnick tersebut kita dapat melihat bahwa jargon "kejahatan terjadi bukan hanya karena ada niat, tetapi juga karena adanya *kesempatan*" tetap berlaku di *cyberspace.* Peluang yang menuntun seorang pelanggar hukum untuk melaksanakan aksinya. Dan jika keteledoran dalam mengamankan sistem terjadi karena orang dalam, tentu akibat yang terjadi bisa sangat berat bagi sebuah perusahaan.

#### 3.2.3.1 Pengaruh Ekonomi

Dengan kemampuan tinggi yang terspesialisasi maka potensi kerusakan yang muncul akan lebih besar jika dibandingkan kejahatan yang dilakukan dengan kemampuan biasa dan tidak memiliki spesialisasi. Dalam *"Cybercrimes: A Multidisciplanary Analysis"*, Michael Erbschloe menjelaskan tentang pengaruh *cybercrime* terhadap ekonomi (*economic consequences*), dalam permasalahan kejahatan dengan memanfaatkan berbagai kasus besar serangan kode berbahaya (*malicious code attacks*) di dunia dalam tabel:

| Year | Malicious Code | Worldwide economic impact ($US) |
|---|---|---|
| 2001 | Nimda | 635 million |

[236] http://www.imdb.com/title/tt0309614/, diakses pada 17 Mei 2011, pukul 17.30 WIB. Editor 2600, sebuah penerbitan media *hacker* di Amerika juga mengkritik "Takedown". Untuk artikel kritik tersebut, lihat: http://www.2600.com/news/view/article/2038, diakses 17 Mei 2011, pukul 17.30 WIB.

| | | |
|---|---|---|
| 2001 | Code Red(s) | 2.62 billion |
| 2001 | SirCam | 1.15 billion |
| 2000 | I Love You | 8.75 billion |
| 1999 | Melissa | 1.10 billion |
| 1999 | Explorer | 1.02 billion |

*Tabel 3.3. Economic impact of malicious code attacks, by incident.*[237]

| **Year** | **Worldwide economic impact ($US billion)** |
|---|---|
| 2001 | 13.2 |
| 2000 | 17.1 |
| 1999 | 12.1 |
| 1998 | 6.1 |
| 1997 | 3.3 |
| 1996 | 1.8 |
| 1995 | 0.5 |

*Tabel 3.4. Economic impact of malicious code attacks, by year.*[238]

Perhitungan global yang dialami oleh banyak orang ataupun perusahaan karena *malicious code attacks* baik dalam bentuk uang maupun data berharga hingga kerusakan sistem sendiri sudah sangat besar kerugiannya, belum lagi berbagai kerugian yang sifatnya psikologis terhadap setiap orang yang merasa dirugikan ataupun merasa terancam karena pemberitaan tentang kasus-kasus kejahatan mayantara tersebut. Dan pengaruh psikologis bagi publik bisa beragam, bisa menciptakan sikap antisipatif, sikap antipati, atau bahkan memunculkan ketertarikan untuk melakukan tindak kejahatan, yang dalam kriminologi biasa dikenal dengan *social learning theory*, yang dalam hal psikologis bisa juga ditautkan dengan kajian *psychoanalytic*.

[237] Sumit Ghosh, Elliot Turrini (ed.), Cybercrime: A Multidisciplinary Analysis, Springer: Heidelberg, 2010, hal. 132.

[238] *Ibid*., hal. 133.

> *"The average take on a bank robbery is $3,000. The persons committing that crime run an extremely high risk of something bad happening to them. You can run a phishing scam and make hundreds of thousands of dollars."*[239]

Pernyataan Thomas X. Grasso tersebut sungguh merupakan perbandingan yang signifikan antara perampokan tradisional dengan perampokan dengan teknik *phising*[240] di dunia *cyber*. Selain lebih aman bagi seorang pelaku dalam melakukan aksinya, tanpa perlu menghadapi resiko adu tembak dengan polisi dan tertangkap kamera kemudian terekam CCTV tindak kejahatannya, kejahatan di dunia maya sungguh lebih menjanjikan hasil lebih besar dan cara yang lebih sederhana. Namun, tentunya dengan kemampuan teknis yang lebih baik.

> *According to a 2004 report released by Gartner, Inc., an IT marketing research firm, phishing exploits cost banks and credit card companies an estimated $1.2 billion in 2003. Moreover, according to the Anti-Phishing Working Group (a nonprofit group of government agencies and corporations trying to reduce cyber fraud), more than 2,800 active phishing sites were known to exist.*[241]

Melihat dari data laporan dari Gartner, Inc. sebuah firma *IT marketing reseach* tersebut,[242] kejahatan dengan *phising* dapat

---

[239] Pernyataan Thomas X. Grasso, seorang anggota FBI yang dikutip oleh "McAfee North America Criminology Report", Organized crime and the Internet 2007, hal. 3.

[240] Di bidang keamanan komputer, *phishing* adalah proses pidana penipuan dari percobaan untuk mendapatkan informasi sensitif seperti *username*, *password* dan rincian kartu kredit dengan menyamar sebagai entitas yang dapat dipercaya dalam komunikasi elektronik. Pada komunikasi ini mengaku dari situs populer, situs web sosial, situs lelang, atau biasanya digunakan untuk menarik perhatian publik agar tidak menaruh curiga. Lihat: http://opensource.telkomspeedy.com/wiki/index.php/Phising, diakses pada 19 Mei 2011, pukul 16.00 WIB.

Sedangkan di dalam Webster's New World *Hacker* Dictionary, phising lebih jelasnya adalah sebuah bentuk pencurian identitas (identity theft) dimana seorang scammer memakai email yang seakan-akan memiliki otentisitas dari sebuah perusahaan besar untuk menerapkan trik supaya para penerima email memasukkan informasi pribadinya, seperti nomer kartu kredit atau kode akun di bank. (Bernadette Schell, *Webster's New World Hacker Dictionary*, (Indianapolis: Willey Publishing, 2006), hal. 246).

[241] Bernadette Schell, *Webster's New World Hacker Dictionary*, (Indianapolis: Willey Publishing, 2006), hal. 246

[242] http://www.gartner.com/technology/home.jsp, merupakan situs resmi Gartner, Inc.

meraup keuntungan 1,2 juta dollar selama tahun 2003 melalui rekening-rekening bank dan perusahaan-perusahaan kartu kredit. Dan lebih lanjut sebuah kelompok non-profit *Anti-Phising Working Group*[243] (disingkat APWG) mendapati bahwa terdapat lebih dari 2.800 situs-situs yang masih aktif di tahun itu dan melakukan aktifitas *phising*-nya.

Dampak terhadap ekonomi tidak melulu sesuatu yang diperhitungkan dengan uang, akan tetapi terdapat beberapa kesebandingan nilai uang dengan berbagai bentuk property dalam *cyberspace*, dan baik dalam dunia nyata maupun di dalam *cyberspace*, properti sama-sama memiliki nilai ekonomis yang juga dapat diperhitungkan secara ekonomis.

Dalam kasus *phising*, lebih jelasnya adalah sebuah bentuk pencurian identitas (*identity theft*) dimana seorang *scammer* memakai email yang seakan-akan memiliki otentisitas dari sebuah perusahaan besar untuk menerapkan trik supaya para penerima email memasukkan informasi pribadinya, seperti nomer kartu kredit atau kode akun di bank.[244] Dan di Indonesia terdapat sebuah kasus monumental mengenai tindakan yang dicurigai sebagai upaya melakukan pencurian identitas (*identity theft*), adalah kasus 'klikbca' yang populer terutama bagi para nasabah bank BCA di Indonesia.

Steven Hariyanto, yang juga merupakan seorang programer web yang cukup populer, merupakan pelaku pembelian beberapa nama domain situs yang mirip dengan klikbca.com, yaitu 'wwwklikbca.com', 'kilkbca.com', 'clikbca.com', 'klickbca.com', dan 'klikbac.com'. Apa yang dilakukan oleh Steven kelihatannya sederhana tetapi cukup untuk membuat banyak nasabah bank BCA

[243] http://www.antiphishing.org/, merupakan situs resmi APWG.

[244] Bernadette Schell, *Webster's New World Hacker Dictionary*, (Indianapolis: Willey Publishing, 2006), hal. 246

secara khusus, dan para pengguna jasa *online-banking* mengalami ketakutan dan memperketat kewaspadaan mereka dalam mengakses internet dengan tujuan untuk melakukan transaksi secara *online*.[245]

Namun, yang dilakukan oleh Steven bukanlah perbuatan dengan kesengajaan untuk mendapatkan kode dan nomer rekening para pengguna akses situs klikbca.com, yang secara kebetulan salah memasukkan alamat situs sebenarnya, akan tetapi Steven justru memberikan arahan kepada para pengguna, bahwa situs yang mereka tuju adalah salah, dan ia mencoba mengarahkan pengguna kepada alamat yang benar. Hal ini bisa kita lihat pada sebuah presentasi *powerpoint* oleh Onno W. Purbo, yang diunggah di situs http://kambing.ui.ac.id/.[246] Dalam alamat pengembangan *open source* milik Universitas Indonesia tersebut, Onno W. Purbo mencoba mendukung pernyataan Steven tentang kelemahan sistem jaringan online milik BCA tersebut yang justru bisa merugikan nasabah dan BCA sendiri.

Selain permasalahan "*Typo Site*", atau kemungkinan salah ketik dan kemudian nasabah bertransaksi di alamat yang salah, terdapat juga permasalahan jaringan internet yang memungkinkan penyedia layanan keamanan transaksi tersebut, yang saat itu dipercayakan kepada pihak lain, bisa mendapatkan salinan seluruh informasi yang diketikkan oleh nasabah melalui transaksi online tersebut. Hal tersebut dijelaskan secara teknis oleh Onno W. Purbo dalam *file* presentasinya yang diunggah di situs pengembangan *open source* milik Universitas Indonesia tersebut.

---

[245] http://opensource.telkomspeedy.com/wiki/index.php/Surat_Steven_Haryanto_ke_BCA_6_Juni_2001. Alamat link tersebut menampilkan pernyataan maaf Steven Haryanto kepada pihak BCA

[246] http://kambing.ui.ac.id/bebas/v09/onno-ind-1/network/network-security/ppt-situs-klikbca-palsu-06-2001.ppt. Diakses pada 23 Mei 2011, pukul 18.00 WIB.

Apa yang dilakukan Steven Haryanto tersebut merupakan kritik terhadap sistem perbankan nasional yang saat itu tengah memasuki era *internet banking*. Tidak semua bentuk serangan terhadap suatu sistem *cyber* oleh para kritikus *cyber* yang memiliki kemampuan tinggi melulu merupakan kejahatan. Karena tindakan tersebut terkadang juga dapat merupakan penangkalan kejahatan, atau sebagai kritik kepada suatu institusi agar berhati-hati, supaya tidak timbul kerugian ekonomis yang jauh lebih besar di kemudian hari.

### 3.2.3.2 Pengaruh Psiko-Sosial

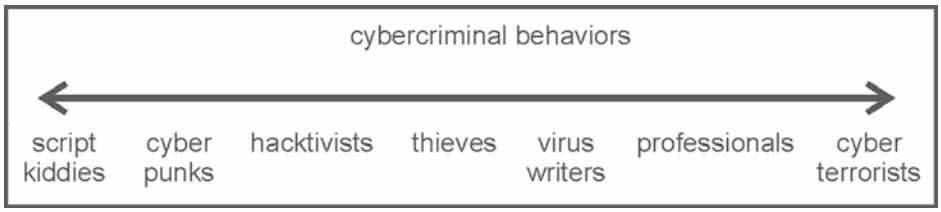
Pengalaman yang dialami oleh para pengguna klikbca.com di atas tidak hanya merupakan ketakutan akan kerugian ekonomi, yang untungnya terselamatkan karena tindakan Steven Haryanto, akan tetapi juga memberikan akibat yang berkepanjangan bagi psiko-sosial. Keadaan psikologis masyarakat akan terus terpengaruhi oleh permasalahan yang pernah dihadapi oleh Bank BCA tersebut sebagai pembelajaran, dan juga ketakutan.

Dalam *"Cybercrime: A Multidisciplinary Analysis"* Markus K. Rogers memberikan suatu pemaparan tentang *"The Psyche of Cybercriminals: A Psychosocial Perspective"* yang ada di dalam pembahasan tentang *"Psycho-Social Impact of Cybercrime"*.[247] Dia memberikan uraian tentang siapakah yang bisa tertarik ke dalam *cybercrime* dan kenapa seseorang melakukan tindak pidana mayantara.

**1) Para Pelaku *Cybercrime***

Dengan mengenali bagaimana siapa saja mereka yang terlibat dalam berbagai bentuk *cybercrimes* kita akan mengenali peranan mereka dalam tiap tindak kejahatan yang mereka lakukan sejauh mana akibat yang ditimbulkan.

[247] Ghosh, *op.cit.*, hal. 217.




*Gambar 3.4. Taxonomy of cybercriminal behaviors.*[248]

Berbagai istilah atau penyebutan dalam gambar di atas sudah cukup populer bagi para pengamat permasalahan *cybercrimes*, mari kita uraikan satu persatu.

*Scriptkiddie*, disebut juga sebagai *newbie*, dalam pengertian umum disebut juga sebagai *cracker* yang masih miskin pengalaman yang baru mulai menyadari susunan dan sebatas sebagai pemakai software untuk melakukan *computer exploits*.[249]

*Cyber-punks*, kelompok yang dalam pengertiannya merupakan perluasan makna dari kata "punk" di dunia nyata, dalam hal ini mentalitas punk itulah yang dibawa ke dalam *cyberspace*. Para individual ini memiliki sikap yang jelas tidak menghargai otoritas dan simbol-simbolnya, dan tidak menganggap adanya berbagai norma sosial. Tindakan mereka dijalankan oleh kebutuhan akan adanya pengakuan atau kepopuleran dari teman-temannya atau lingkungannya.[250]

---

[248] Marcus K. Rogers *"The Psyche of Cybercriminals: A Psychosocial Perspective"*, dalam Cybercrime: A Multidisciplinary Analysis, edited by Sumit Ghosh and Elliot Turrini, (Heidelberg: Springer, 2010), hal. 218.

[249] Bernadette Schell, *Webster's New World Hacker Dictionary*, (Indianapolis: Willey Publishing, 2006), hal. 280.

[250] Marcus K. Rogers, *op.cit.*, hal. 219. Punk merupakan ekspresi reproduktifitas pakaian dalam sejarah, yang menggambarkan kelompok pekerja muda pasca perang, yang mengkombinasikan berbagai elemen dari berbagai kisah sejarah (lihat: Dick Hebdige, *Subculture: The Meaning of Style*, (London: Routledge, 1979), hal. 26). Semangat yang mereka usung adalah upaya untuk meraih pengakuan dengan cara menunjukkan eksistensi mereka dengan kemampuan yang lebih dari yang lain, sebagaimana dalam kajian *subculture*, namun pada saat yang sama mereka tidak mempedulikan berbagai bentuk otoritas di sekitarnya kecuali dari kelompoknya sendiri sehingga melanggar, dalam hal cybercrime, adalah cara meraih pengakuan tersebut. Gambaran tentang semangat kelas pekerja pasca-perang adalah adanya pencitraan ketertindasan dan pemberontakan.

*Hacktivists* dan *hacktivism*: internet telah mengubah *landscape* perbincangan politik dan advokasi sejak era 1990-an, sebagian memiliki pengertian lebih universal dalam mempengaruhi berbagai kebijakan nasional dan luar negeri. Dengan kemampuan internet bagi *mainstream* masyarakat telah mengakibatkan pertumbuhan dalam demam politik baik bagi para *white hat*[251] ataupun *black hat*[252]—demam ini lebih dikenal dengan "*hacker activism*" atau "*hacktivism*." Mereka yang melakukan *hacktivism* dikenal sebagai *hacktivist*—pribadi-pribadi ini mencocokkan kebutuhan mereka akan *activism* dengan kemampuan *hacking* mereka untuk lebih memperluas pidato politis mereka di penjuru dunia—jika mereka *White Hat*—atau membawa beberapa misi politis yang bisa jadi mengakibatkan kerusakan pada website yang menjadi sasarannya—jika mereka *Black Hat*.[253]

*Thieves* (pencuri), merupakan kategori seperti umumnya para pelaku kriminal di dunia nyata. Para individu tersebut melakukan tindakan kejahatan maya dan bersembunyi di belakang label-label di dunia maya untuk mengalihkan tuduhan bersalah secara langsung kepada mereka. Secara primer mereka termotovasi oleh uang dan keserakahan. Kelompok ini disebut

---

[251] *White Hats* atau *Ethical Hackers* atau *Samurai Hackers* (pengertian umum): *hacker* yang menggunakan kemampuan komputer kreatif mereka untuk kebaikan bagi masyarakat lebih daripada alasan-alasan yang merusak (lihat: Schell, *op.cit.*, hal. 357).

[252] *Black Hat* (pengertian umum): sisi buruk dari tindakan kriminal suatu komunitas *hacking*—salah satu jenis kejahatan *cyber*. Praktik-praktik yang dilakukan *Black Hat* meliputi pengeksploitasian komputer yang muncul sebagai sebuah motivasi dari seorang *cracker* untuk balas dendam, sabotase, blackmail, atau meraup keuntungan dengan serakah. Jika digambarkan dalam kejahatan di luar ruang *cyber*, apa yang dilakukan oleh *Black Hat* bisa mengakibatkan hal berbahaya terhadap properti ataupun pada seseorang (lihat: Schell, *op.cit.*, hal. 36).

[253] *Ibid*., hal. 148. Operasi yang biasa dilakukan dalam hacktivis termasuk menjelajahi web untuk mendapatkan informasi; mengotak-atik website dan memposting informasi kepada pemilik web dan para pengaksesnya; mengirimkan berbagai publikasi elektronis dan surat-surat melalui email; dan memanfaatkan internet untuk mendiskusikan berbagai isu, membentuk koalisi, dan merencanakan serta mengkoordinasikan berbagai aktifitas.

juga "T group", yang menargetkan terhadap sistem-sistem untuk memperoleh uang dan, beberapa, tertarik untuk mendapatkan nomer-nomer kartu kredit dan akun-akun bank yang bisa mereka gunakan sewaktu-waktu saat ada kebutuhan mendesak. Kelompok ini bisa dibilang sangat picik dalam melakukan tindak kriminalitas, dengan alasan bahwa biasanya kemampuan anggota dalam kelompok ini tidak bisa dibilang canggih, hanya dengan penipuan transfer online sederhana dan penipuan nomer kartu kredit; dan bahwa kehidupan dasar mereka secara umum tidak tergantung pada tindakan-tindakan kriminal tersebut. Sebuah kecenderungan yang mengkhawatirkan dalam grup ini adalah meningkatnya keterlibatan dalam pencurian identitas (*identity theft*). Sang penjahat *cyber* selalu berusaha keras mencari cukup informasi tentang sasaran untuk mendapatkan asumsi tentang identitas si korban dan kemudian dengan satu kesalahan akan berusaha mendapatkan kartu kredit, pinjaman, dan bahkan hipotek.[254]

*Virus Writer (VW),* sebuah kelompok yang melakukan aksi di balik berbagai virus yang bertebaran dalam jaringan internet hingga komputer personal yang tidak pernah terkoneksi internet, yang terinfeksi melalui berbagai jenis perangkat keras penyimpan data yang terhubung dengannya. Sarah Gordon menjelaskan tentang asumsi seorang *virus writer* karena efek yang diakibatkan dari tindakannya. *Virus writer* telah dikarakterisasikan sebagai seorang yang buruk, jahat, tidak berakhlak, maniak, teroris, *technophatic*, jenius yang menggila,

[254] Rogers, *op.cit.*, hal. 220. Di Amerika Serikat, hampir mendekati 1.2 juta laporan tentang pencurian identitas (identity theft) di awal dekade 2000-an ini. Tentu saja tagihannya tidak pernah terbayarkan dan para duafa, korban yang tidak tertolong, dibiarkan menenteng tas penuh anggapan. Para korban juga dibiarkan dengan keberanian mereka untuk membersihkan nama mereka dan tingkat kreding dengan memanfaatkan institusi keuangan yang berbeda dan biro-biro kredit.

sakit secara sosial. Citra ini telah demikian populer tidak hanya di media, tetapi juga oleh beberapa pelaku *virus writer* dalam melakukan aksinya itu sendiri. Namun dalam papernya Sarah menjelaskan bahwa mereka memberikan publikasi elektronik, dan kenyataannya tidak semua tingkatan para *cybercriminals*, dalam hal ini para *virus writers*, bisa dikatakan sebagai orang-orang yang tidak memiliki etika (*unethical people*).[255]

Sarah Gordon berusaha melakukan klasifikasi berdasarkan usia bagi para *virus writers* sebagai upaya memahami kondisi kejiwaan masing-masing tingkatan dalam ukuran rata-rata. Klasifikasi tersebut ada dalam empat kelas: (a) *the young adolescent individual* (13-17 tahun, setidaknya telah menulis dan menyebarkan secara liar sebuah virus); (b) *the college student* (18-24 tahun, setidaknya telah menulis dan menyebarkan sebuah virus secara liar, mereka dalam tingkatan mahasiswa); (c) *the adult/professionally employed individual* (mereka adalah para profesional, *post-college* atau dewasa, setidaknya telah menulis satu buah virus dan menyebarkannya secara liar); (d) *the mature reformed ex-writer of viruses* (setidaknya telah menulis satu buah virus, dan virusnya telah diketemukan secara bebas, si pelaku harus bisa membuktikan keterlibatannya dalam penulisan virus. Sarah membatasi setidaknya enam bulan sebelum risetnya si *virus writer* setidaknya masih aktif menulis virus).[256]

Dari hasil wawancaranya kepada para narasumber yang telah ia kelompokkan ia mengamati bahwa tiap kelompok memiliki pandangan yang berbeda terhadap kepentingan orang

[255] Sarah Gordon, "The Generic Virus Writer," <http://www.research.ibm.com/antivirus/SciPapers/Gordon/GenericVirusWriter.html>, diakses pada 24 Mei 2011, 17.00 WIB.

[256] *Ibid*.

lain, yang menjadikan mereka lebih beretika. Sarah memasukkan kelompok *the mature reformed ex-writer* of *viruses* secara sengaja—biasanya usia ini tidak dihiraukan, dan terlebih penelitiannya adalah pada tahun 1994—dengan tujuan untuk memahami akan seperti apa ketiga kelompok lainnya kelak. Dan hasilnya, semakin seseorang berada dalam tingkat usia yang lebih matang, para *virus writer* ini lebih memahami dan menghargai kepentingan orang lain sebagai kepentingan yang lebih besar, di dalam kehidupannya.[257]

*Professionals*, mewakili gambaran kelompok yang memang memiliki posisi paling elit dalam kelompok *cybercriminal* dan seringkali dihubungkan secara langsung dengan pengertian *cybercriminal* itu sendiri, kepandaian kompetitif dan aktifitas yang bersifat *white* dan *grey*. Para individu ini bisa jadi terlibat dalam penipuan-penipuan luar biasa atau spionase korporasi. Mereka akan menjual informasi dan *intellectual property* kepada pihak yang bisa menawar lebih tinggi. Sangat sedikit yang diketahui tentang kelompok tersembunyi ini karena mereka memakai anonimitas secara sempurna untuk menutupi aktifitasnya. Bagi mereka, kegiatan kriminalnya adalah pekerjaan dan mereka melakukannya dengan professional. Diyakini bahwa grup ini dibentuk dalam jumlah besar dari berbagai operasi ex-intelejen. Ketika USSR dan beberapa negara Blok Timur berjatuhan dalam pertengahan 1990-an, banyak pemecatan intelejen secara cepat, orang-orang melaporkan mereka kemudian menjadi tentara bayaran. Bagi para individual tersebut, moralitas ataupun etika dalam tindakan mereka tidak memiliki gambaran yang sepadan. Mereka telah dengan sangat baik terindoktrinasi melawan suatu

[257] *Ibid*.

mekanisme pengaturan-diri oleh pelatihan intelejen dan spionase mereka sebelumnya. Mereka lebih seperti pada tahapan *post-conventional* pengembangan moral dimana etika-etika didiktekan oleh prinsip-prinsip pilihan-pribadi.[258]

Dan terakhir adalah *Cyber-Terrorists (CT)*. DR. Mudawi Mukhtar Elmusharaf dalam uraiannya "*Cyber Terrorism: The New Kind of Terrorist*",[259] paper tersebut dimuat dalam situs populer dalam riset kejahatan komputer (www.crime-research.org). DR. Mudawi menjelaskan bahwa peranan luar biasa berbagai tindak kejahatan yang disimulasikan dengan teknologi komputer menjadikannya sebagai alat yang lebih tepat dalam melancarkan serangan terhadap sasaran mereka. internet telah memberikan ruang tempur virtual bagi berbagai negara-negara yang memiliki masalah satu sama lain seperti Taiwan melawan China, Israel melawan Palestina, India melawan Pakistan, China melawan Amerika Serikat, dan berbagai negara lain.

Perubahan metode-metode terorisme dari tradisional kepada metode-metode elektronik adalah merupakan salah satu tantangan terbesar bagi masyarakat modern. Dengan tujuan untuk memerangi terorisme jenis ini banyak upaya semestinya dilakukan pada tingkatan personal, tingkat negara, tingkat regional, sebagaimana dilakukan juga dalam tingkat internasional dalam memerangi kejahatan transnasional semacam ini. DR. Mudawi menambahkan beberapa keuntungan *cyber-terrorism*:

- Lebih murah dari pada metode-metode tradisional.

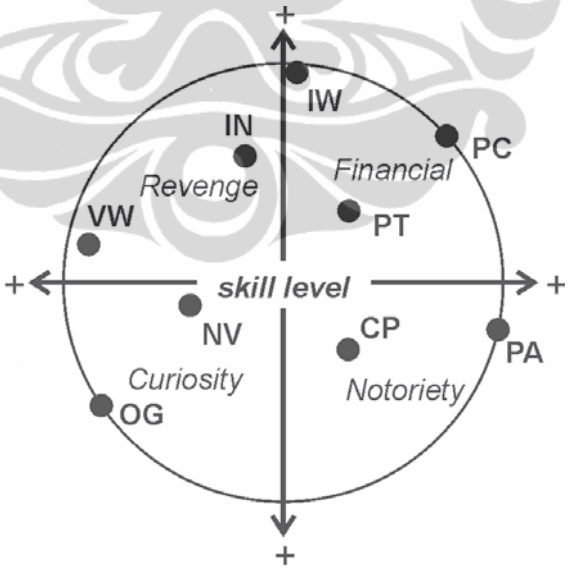
---

[258] Rogers, *op.cit.*, hal. 220.

[259] Mudawi Mukhtar Elmusaraf, "Cyber Terrorism: The New Kind of Terrorism," <http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism/>, April 08, 2004, diakses pada 24 Mei 2011, pukul 20.00 WIB.

- Aksi yang dilakukan sangat sulit dilacak.
- Para pelaku dapat menyembunyikan identitas dan lokasi.
- Tidak terdapatnya batas-batas fisik atau pun *check points* untuk dilintasi.
- Mereka dapat melakukannya secara remote dari berbagai tempat di dunia.
- Mereka dapat memakai metode ini untuk menyerang sasaran-sasaran dalam jumlah besar.
- Mereka dapat memberikan pengaruh kepada orang-orang dalam jumlah besar.[260]

Para teroris *cyber* bisa membahayakan keamanan sebuah negara dengan melancarkan serangan pada pusat-pusat atau sumber informasi sensitif dan rahasia, yang bisa saja dilakukan dengan cara mencuri data, merusak pusat informasi dan menutupnya, atau menyebarkan ceramah kebencian suatu negara, lembaga, atau pribadi.




*Gambar 3.5.* Sebuah model *circumplex* (*novice* (NV), *cyber-punks* (CP), *petty thieves* (PT), *virus writers* (VW), *old guard hackers* (OG), *professional*

[260] *Ibid*.

*criminals* (PC), *information warriors* (IW), dan *political activists* (PA) dimasukkan sebagai sebuah poin pembahasan saja).[261]

Onno W. Purbo memberikan pembagian yang berbeda dari apa yang dilakukan oleh Markus K. Rogers tersebut:

1. *Elite*: merupakan ujung tombak industri keamanan jaringan. Mereka mengerti sistem operasi luar dalam, sanggup mengkonfigurasi dan menyambungkan jaringan secara global. Sanggup melakukan pemrograman setiap harinya.
2. *Semi Elite*: biasanya lebih muda dari pada *Elite*. Mereka juga mempunyai kemampuan dan pengetahuan luas tentang komputer. Mereka mengetahui tentang sistem operasi termasuk lubangnya.
3. *Developed Kiddie*: kelompok masih muda (ABG) dan masih sekolah. Mereka membaca tentang metode *hacking* di berbagai kesempatan. Mencoba berbagai sistem dan berusaha berhasil.
4. *Script Kiddie*: sebagaimana *Developed Kiddie* dalam hal aktifitas, seperti juga *Lamers*, mereka hanya memiliki pengetahuan teknis *networking* yang minimal.
5. *Lamer*: mereka adalah orang tanpa pengalaman yang ingin menjadi *hacker* (*wanna-be hacker*). Mereka biasanya membaca atau mendengar tentang *hacker* dan ingin seperti itu.[262]

Namun jika dilihat dari sisi pengelompokan dan definisi, baik apa yang didukung oleh Markus maupun Onno sama-sama memberikan strata. Akan tetapi klasifikasi Markus lebih sesuai untuk menjelaskan dan mengkaji lebih jauh dalam

[261] Rogers, *op.cit.*, hal. 220.
[262] Onno W. Purbo, *Filosofi Naif Kehidupan Dunia Cyber*, (Jakarta: Republika, 2003), hal. 132-133.

permasalahan pidana, terutama motif-motif kejahatan yang melatarbelakangi tiap grup, serta bentuk kejahatannya. Sehingga lebih mudah bagi para penegak hukum untuk mengamati kecenderungan pelaku dari apa yang telah dia lakukan. Sedangkan apa yang diuraikan Onno W. Purbo jelas merupakan klasifikasi kemampuan (*skill*) seseorang dalam jenjang dunia *hacking*.

Dan dalam suatu komunitas, *hacker* satu dengan yang lainnya saling menghargai terutama dalam hal senioritas. Bukan hanya untuk mendefinisikannya secara kriminal seperti dipaparkan Markus, karena etika dalam komunitas juga ditegakkan dengan saling menghargai.

> "Tidak perlu memaksa orang lain untuk menyebut kita *hacker*. Jika ada yang memanggil kita *hacker*, bersyukurlah. Kalau disebut *lamer*, jangan marah. Pastilah yang menyebut kita lamer itu berilmu tinggi."[263]

**2) Ketertarikan Melakukan Kejahatan Mayantara (Perspektif Kriminologi)**

Dalam melakukan suatu tindak kejahatan terdapat alasan-alasan logis yang mendorong atau menyeret seseorang *to commit crime*. Pada gambar.2 di atas terdapat pemilahan dalam empat kategori seseorang memiliki kecenderungannya masing-masing, dalam grup kriminal yang berbeda-beda. *Revenge*, *financial*, *curiosity*, dan *notoriety* menjadi pertimbangan dalam melakukannya secara umum.

Kajian sosiologi, psikologi, dan kriminologi berusaha membantu menyumbangkan teori untuk menjelaskan kenapa seseorang terdorong untuk melakukan suatu tindakan kriminal secara umum. Dalam bidang-bidang tersebut tidak dapat

[263] Wawancara dengan PZ, 19 April 2011.

menguraikan secara tepat alasannya hanya dengan satu sudut pandang, karena tindak kriminal memiliki berbagai alasan yang berbeda-beda. Dan kali ini akan kita dekati dengan teori-teori kriminologi.

Dalam karya Ronald L. Akers, *Criminological Theories*, dan karya Freda Adler (*et.al.*), *Criminology*, kita bisa mendapatkan penjelasan yang kita butuhkan tentang hal-hal yang mendorong seseorang *to commit crime*, sebagaimana diuraikan dan dipilah-pilah dalam beberapa grup dalam sub bab sebelumnya. Akers, kriminolog Amerika, yang terkenal dengan teori *social learning*-nya menyampaikan beberapa teori kriminologi, akan tetapi tidak semuanya bisa dengan mudah dikaitkan dengan sederhana, terutama untuk permasalahan *cybercrime* secara umum.

Dalam arus informasi dalam dunia digital internet, pembelajaran dalam ruang sosial adalah hal utama yang dapat mendorong seseorang untuk memiliki keahlian dalam melakukan tindak kriminal. Perkembangan komunitas dan peningkatan jumlah media pembelajaran dalam bentuk cetak, *online*, maupun *offline* (seminar seputar *cybercrime* dan sebagainya), serta pencitraan dalam berbagai media massa tentang kejahatan *cyber*, merupakan bentuk pembelajaran yang juga mendukung tumbuh kembangnya penyebaran keahlian publik tentang dalam hal tehnik *cyberspace*. Baik untuk kebutuhan positif atau untuk kepentingan negatif.

Ilmu pengetahuan dalam hal ini selalu dipahami sebagai sesuatu yang netral dalam asalnya, ia hanya akan menjadi berbahaya saat digunakan dengan dorongan jahat, dan akan menjadi bermanfaat untuk masyarakat luas —bukan untuk

kepentingan pribadi yang sempit dan merugikan orang lain—saat dimanfaatkan dengan bijaksana.

Dalam hal ini akan lebih sesuai untuk menekankan pada konsep *Social Learning Theory*-nya Akers, ditambah dua bagian lain yang mendorong seseorang to commit crime dalam *cybercrimes* dari gagasan Markus K. Rogers, yaitu *Moral Disengagement* dan *Anonymity*. Teori-teori tersebut tidak bisa menjadi superior dari teori kriminologi yang lain, sebagaimana Markus: "*While no single theory has been proven to be superior than any other,…*"[264]

**a) *Social Learning Theory***

Pada 1947 Edwin H. Sutherland memberikan konsep tentang konflik dan disorganisasi dari pernyataan dalam teorinya. Dia menjelaskan tentang "*differential social organization,*" dan Akers menjelaskan bahwa semestinya konsep itu diterapkan pada *social disorganization*. Teori yang telah dia jabarkan adalah sebagai berikut:

1. *Criminal behavior si learned.*
2. *Criminal behavior is learned in interaction with other persons in a process of communication.*
3. *The principal part of the learning of criminal behavior occurs within intimate personal groups.*
4. *When criminal behavior is learned, the learning includes (a) techniques of commiting the crime, which are sometimes very complicated, sometimes very simple, and (b) the specific direction of motives, drives, rationalizations, and attitudes.*

[264] Rogers, *op.cit.*, hal. 223.

5. *The specific direction of motives and drives is learned from definitions of the legal codes as favorable of unfavorable.*
6. *A person becomes delinquent because of an excess of definitions favorable to violation of law over definitions unfavorable to violation of law.*
7. *Differential associations may vary in frequency, duration, priority, and intensity.*
8. *The process of learning criminal behavior by association with criminal and anti-criminal patterns involves all of the mechanisms that are involved in any other learning.*
9. *Although criminal behavior is an expression of general needs and values, it is not explained by those general needs and values, because noncriminal behavior is an expression of the same needs and values.*[265]

Dari semua poin-poin tersebut, Akers menjelaskan bahwa pada poin keenamlah yang disebut dengan "*principle of differential association.*" Akan tetapi tiap-tiap bagian dari penjelasan Shuterland tidaklah dihilangkan oleh Akers, *differential association* justru menjadi penguat dalam menegaskan konsep *social learning theory*. Akers menemukan bahwa social learning theory menjelaskan tindak kriminal dan menyimpang lebih cermat dari pada bentuk asli *differential assosiation theory.*[266] Di dalam social learning theory terdapat beberapa kunci pokok, yaitu: *differential association, definition, differential reinforcement, imitation.*

[265] Ronald L. Akers, *Criminological Theories*, (Chicago: Fitzroy Dearborn Publisher, 1999), hal. 59-61.

[266] *Ibid*., hal. 62.

*Differential association* merujuk pada proses dimana seseorang diarahkan kepada definisi-definisi normatif tentang menguntungkan atau tidak menguntungkan atas tindakan illegal atau legal. *Differential association* memiliki baik tindakan interaksional maupun dimensi-dimensi normatif. Dimensi interaksional adalah asosiasi langsung dan interaksi dengan yang lainnya, yang bertautan dalam perilaku yang tertentu, sebagaimana asosiasi tak langsung dan pengidentifikasian dengan grup-grup referen yang lebih berjauhan. Dimensi normatif adalah pola-pola yang berbeda dari norma-norma dan nilai-nilai atas yang mana suatu individu diperkenalkan pada asosiasi tersebut.[267] *Definitions* adalah sikap seseorang sendiri atau sesuatu yang melekat pada karakter watak bawaan. Yaitu, orientasi, rasionalisasi, definisi situasi, dan evaluasi lain dan sikap-sikap moral yang didefinisikan sisi tindakan sebagai benar atau salah, baik atau buruk, diinginkan dan tidak diinginkan, adil atau tidak adil. *Differential reinforcement*, merujuk pada keseimbangan atas antisipasi atau penghargaan dan hukuman aktual yang mengikuti atau merupakan konsekuensi dari tindakan. Apakah individual akan menahan diri untuk melakukan kejahatan di setiap waktu yang ada (dan apakah mereka akan melanjutkan atau berhenti dari melakukan lagi di masa depan) tergantung pada masa lalu, kini, dan masa depan yang terantisipasi dari hukuman dan penghargaan atas tindakan mereka. Sedangkan *imitation*, merujuk pada kesepakatan dalam sikap setelah observasi atas sikap yang serupa pada orang lain.[268]

[267] *Ibid*., hal. 64.
[268] *Ibid*., hal. 64-67.

Sesuai dengan *social learning theory*, mekanisme pembelajaran yang utama termasuk *differential reinforcement* dan *imitation*. Pertama, *differential association* terjadi, menciptakan sebuah lingkungan sosial. Kedua, dalam lingkungan sosial, keterbukaan kepada definisi-definisi dan *imitation* atas model terjadi. Dalam kajian *cybercriminal* para anggota yang memiliki visi moral dan etika yang sama berinteraksi dalam *computer-mediated communication* (CMC), yang bisa berupa *chat-room* (didefinisikan sebagai komunikasi sinkronis, *real-time*) atau email, *news-group* (didefinisikan sebagai komunikasi asinkronis, tidak *real-time*). Dalam komunikasi semacam inilah komunikasi mereka yang mewakili komunikasi dunia di nyata, dan di dalamnyalah hubungan antar individu dijaga dan terus terjadinya pemberian pengaruh dan pembelajaran. Dalam ruang-ruang komunikasi maya tersebut juga terjadi pendidikan bagi pemula dan pengenalan terhadap *software* serta penerapannya, bahkan transaksi berbagai perangkat atau barang terlarang. Dalam lingkungan internet *underground* sebagian anggota justru merasa lebih nyaman dalam komunikasi maya semacam ini dibandingkan komunikasi dalam dunia nyata. Komunikasi dalam dunia nyata bisa digambarkan sebagai komunikasi dalam *bandwidth* tinggi, sedangkan komunikasi dalam ruang maya bisa dikatakan sebagai komunikasi dalam *bandwidth* rendah. Dan dalam *bandwidth* rendah bisa melahirkan salah pengertian, salah interpretasi dalam pembelajaran dan transfer pengetahuan, argumentasi, dan lemahnya landasan sosial.[269]

[269] Rogers, *op.cit.*, hal. 224-225.

Menurut *social* learning *theory*, dimana keseluruhan rasio penegasan untuk menghukum sangat tinggi, pengembaraan perilaku akan berlanjut tak teredam, dan dalam banyak kasus, meningkat. Perilaku kriminal dipengaruhi oleh mekanisme tradisi pembelajaran, termasuk pembelajaran *klasikal* dan instrumental. Lebih jauh, variasi rasio dari penekanan positif untuk menghukum dihasilkan dalam paradigma pembelajaran yang sangat ulet, mengurangi kesulitannya untuk menetralisir perilaku menyimpang. Perilaku menyimpang akan cepat berbalik ketika penekanan positif diperkenalkan kembali kepada lingkungan.[270]

Uraian Sutherland memberikan kontribusi pada penekanan atas *social learning theory* dalam masyarakat komunikasi yang mendasarkan pada fungsi komunikasi dalam memahami dan menyalurkan nilai satu sama lain. Dan Akers menambahkan beberapa batasan peristilahan fokusnya yang bisa membantu seseorang untuk lebih teridentifikasi dalam ketertarikannya *to commit crime*. *Social disorganization* telah diarahkan kepada *social learning* theory, pemahaman Akers atas konteks yang dimaksudkan oleh Sutherland, yang sebelumnya telah coba dimurnikan oleh *para* penerusnya seperti Cressey dan Luckenbill, tetapi mereka tidak memberikan perubahan.[271] Dan dalam bentuk komunitas dan pembelajaran dengan banjiran arus informasi yang luas di dunia maya, teori *social learning* adalah cara yang efektif bagi seseorang *to commit crime*. Dengan

[270] *Ibid*., hal. 225-226.
[271] Akers, *op.cit.*, hal. 62.

batasan-batasan pemfokusan dalam peristilahan Ronald L. Akers.

***b) Moral Disengagement***

*Moral disengagement,* lepas dari moral (*moral disengagement*) merupakan bagian dari kriminalitas. Seorang *cybercriminal* memerlukan justifikasi atas tindakan menyimpangnya dari suatu kelompok, untuk mendapatkan kehormatan dan posisi sosial yang lebih kuat, terutama dalam kelompoknya. Ini yang merupakan pembuktian dari suatu pencapaian atas suatu kemampuan (*skill*), di sisi pandang mereka melakukan 'serangan' terhadap sasaran yang lebih ternama dan memiliki sistem keamanan yang tinggi akan jauh diapresiasi, dan dalam situasi tertentu jumlah juga merupakan isu penting dalam pengertian ini.[272]

Proses kompleksnya dengan baik dapat dipahami melalui teori *social cognitive* Albert Bandura. Menurutnya, manusia menjadi secara alamiah menahan diri dari perilaku-perilaku yang melukai standar-standar moral milik mereka sendiri dan membawa berbagai perasaan pencelaan terhadap diri sendiri dan rasa bersalah. Standar-standar tersebut digerakkan dari agensi moral dan terwujud dalam hubungan mekanisme-mekanisme pengaturan diri, yang terdiri dari tiga sub-fungsi utama, yaitu, *self-monitoring*, *judgmental*, dan *self-reactive.* Pada awalnya dalam melatih kontrol diri adalah dengan *self-monitoring.* Kedua, diikuti sebuah tindakan oleh suatu individu, sebuah fungsi penghakiman

[272] Dalam komunitas internet *underground*, terutama mereka yang memiliki ketertarikan terhadap *defacement* (memasuki sistem suatu web dan merubah isi sebagian atau seluruhnya), melakukan deface secara massal (misalkan, dengan penuh perencanaan dan pengamatan serta penyusupan yang telah lama dilakukan terhadap puluhan atau ratusan situs satu persatu. Perubahan isi dilakukan secara bersamaan dalam satu waktu sebagai '*show off*' di berbagai forum komunitas *underground*) juga bisa mendapatkan penghargaan secara umum.

(*judgmental*) mengeveluasi tingkah laku melawan standar-standar internal dan kondisi situasional. Dan hal itu memberikan *self-reaction*. Dalam teorinya, pelaku kriminal bisa mengalahkan sistem pengaturan diri dengan memisahkan kontrol moral internal dari perbuatan merusak yang mereka lakukan melalui satu dari empat mekanisme. Yang termasuk berikut ini, (1) menjelaskan kembali suatu tindakan, (2) menggelapkan peran penyebab pribadi, (3) salah penggambaran atau tidak menganggap adanya konsekuensi negatif dari aksinya, dan (4) memfitnah para korban dan menyalahkan dan merendahkan mereka.[273]

Sudah jelas bahwa banyak kejahatan *cyber* melakukan salah satu dari empat mekanisme di atas. Terkadang tindakan mereka yang mengagungkan kemampuan teknologi secara bebas menyerang kepada siapa saja, dan ini menjadi teror bagi siapa saja, akan tetapi bagi mereka ini adalah pertunjukan untuk mencapai pengakuan. *Nickname* adalah nama samaran untuk menggelapkan identitas asli, *nickname* biasa digunakan para *hacker* dalam melakukan aksinya, meskipun tidak semua *hacker* adalah pelaku tindak kriminal secara berkelanjutan. Konsep merendahkan korban adalah sikap mereka yang terkadang merasa tidak merusak sistem dan seringkali menyalahkan kelemahan keamanan situs korban. Terlebih lagi dalam *cyber-terrorism*, penyerang biasanya mengarahkan secara membabi-buta cemoohan, atau jika itu bermuatan politis, pelaku akan memberikan pesan yang merendahkan atau menyalahkan suatu institusi atau negara dengan menggunakan situs korban yang sudah

[273] Rogers, *op.cit.*, hal. 226-227.

ia rusak sebagai medianya, seolah-olah tidak peduli apakah korban terlibat atau tidak.

***c) Anonymity***

Ketertarikan seseorang untuk melakukan tindak kriminal mayantara salah satunya adalah karena *anonymity* (anonimitas). Secara umum pemakaian *nickname*[274] dalam *cyberspace* adalah hal yang biasa, tidak terkecuali dalam berbagai situs jejaring sosial yang terbuka. Jika melihat dalam berbagai situs jejaring sosial populer seperti Facebook dan Twitter, atau aplikasi *chatting* populer seperti Yahoo! Messenger, Windows Messenger, atau mIRC, dapat ditemui berbagai nama dan identitas palsu.

Salah satu kesulitan yang kemungkinan besar akan dihadapi oleh penegak hukum *cybercrime* saat mereka telah selesai merekam bukti, adalah mereka tidak dapat menjamin dapat menyeret pelaku dengan mudahnya ke dalam proses pidana. Karena sebagian besar pelaku menggunakan *nickname*, atau nama samaran,

> "… kemungkinan besar bisa, tapi yang terjadi biasanya ada laporan masuk sudah tidak ada tindak lanjut, karena polisi sendiri, entah itu polisi atau dari Depkominfo itu agak susah juga mencari cara untuk menangkap sang pelaku karena identitasnya pelaku kan tidak jelas, karena cuma ada *nickname* tapi tidak ada identitas."[275]

BD menguraikan kesulitan tersebut akan dialami oleh tim penegak hukum yang berusaha untuk melakukan reaksi cepat (jika itu diberlakukan) terhadap tindakan dan pelaku tindak pidana mayantara. Karena satu orang tidak selamanya memiliki satu *nickname*, dan tidak selamanya dalam

[274] *Nickname* atau nama pendek, bisa disebut juga sebagai 'alias' atau a.k.a (*as known as*)
[275] Wawancara dengan BD, 11 April 2011.

melakukan aksinya si pelaku memakai *nickname* yang biasa ia gunakan saat bersosialisasi di ruang publik mayantara. Dan kenyataannya, internet membolehkan hal tersebut secara teknis.

Diijinkannya seseorang untuk memasukkan data palsu ke dalam *personal profile*-nya secara bebas, memberikan peluang seseorang untuk melakukan tindak kejahatan melalui internet dengan resiko rendah. Jika suatu sistem menyetujui identitas palsu tersebut dalam berinteraksi, hal ini akan memberikan si pemakai identitas palsu[276] merupakan daya tarik dalam melakukan tindakan kriminal.

Para peneliti memberikan hipotesa bahwa anonimitas mendorong munculnya kepribadian buruk dalam individu ketika mereka online, diberikannya kesempatan demikian mereka percaya dengan pasti menjadi anonim dan bisa diasumsikan sebagai sosok fiktif. Pada esensinya, tindak-tanduk ketika online bisa merefeksikan watak sesungguhnya suatu individu, dalam ketiadaan kontrol diri dan norma-norma sosial yang terlihat dan tekanan-tekanan. Di dunia nyata, sebagian besar individu memoderasi sikap mereka berdasarkan pada identitas sosial yang bekerjasama dengan norma-norma sosial dan dan moralitas kultural. Karenanya, watak dalam dunia nyata lebih konservatif untuk disesuaikan dalam toleransi sosial yang telah ditentukan. Hipotesis bahwa anonimitas memacu sikap permisif yang menemukan dukungannya dalam teori kontrol sosial (*social control*), yang dinyatakan secara umum, orang akan menahan diri dari sikap menyeleweng dan tindak kriminal karena kehadiran

[276] Pemberian identitas palsu (*fake identity*) adalah juga bentuk anonimitas, dengan menghilangkan identitas asli, menggantikannya dengan identitas buatan.

kontrol-kontrol sosial, termasuk polisi, hukum, pengasingan oleh masyarakat, dan sebagainya. Dimana kontrol-kontrol hilang atau diasumsikan kekuatan dari kontrol tersebut telah hilang, tindakan menyimpang akan bertumbuh.[277]

### 3.2.4 Statistik Global Kejahatan *Cyber*

Pembahasan ini disusun berdasarkan pengelompokan besar dalam karya David S. Wall (2001: 3-7), *Cybercrime and the Internet*, yang juga dikutip oleh Majid Yar (2006: 10) dalam karyanya yang populer di kalangan pengamat cyberlaw, *Cybercrime and Society*. Pengelompokannya adalah: *Cyber-tresspass, Cyber-deception/theft, Cyber-pornography, Cyber-violence.*

#### 3.2.4.1 *Cyber-trespass*

*Deface* dalam pengertian umum adalah berarti merusak atau mengubah website dengan cara yang tidak dikehendaki. Karena sebagian besar web server rentan untuk di-*exploit*, terkadang dilakukan para *cracker* yang mengganti informasi pada halaman web dengan informasi yang mereka kehendaki.[278] *Defacement* diambil sebagai representasi dari *cyber-trespass*, dalam definisi Majid Yar *cyber-trespass* adalah: "*crossing boundaries into other people's property and/or causing damage, e.g. hacking, defacement, viruses.*"[279] Maka akibat yang potensial terhadap korban *defacement* sama dengan kemungkinan yang muncul terhadap, dalam definisi atas, *cyber-trespass*.

*Defacement*, dalam penelitian ini diambil contoh adalah situs zone-h.org[280] yang menjadi *wall of fame* para *defacer*.[281] Berikut adalah report tentang *defacement* pada tahun 2010.

---

[277] Rogers, *op.cit.*, hal. 228.
[278] Schell, *op.cit.*, hal. 93.
[279] Majid Yar, *Cybercrime and Society*, (London: Sage Publication, 2006), hal. 10.
[280] http://zone-h.org, http://zone-ar.com, merupakan dua contoh dari situs populer di kalangan defacer untuk mensubmit hasil defacenya. Di dalam situs tersebut disediakan ruang untuk mirror (menduplikasi) tampilan deface yang sudah dilakukan, kemudian disimpan menjadi file yang

*Last year the Zone-H archived a sad record number, we archived 1.419.203 websites defacements. Why and how this is happening? If you are looking at on the stats, the things remain the same: file inclusion, sql injection, webdav attacks and shares misconfiguration are still at the top ranks of the attack methods used by the defacers to gain first access into the server. As an important factor influencing the stats we consider the fact that last year brought a very high number of the local linux kernel exploits.*[282]

| ***Attacks by month*** | ***Year* 2010** |
|---|---|
| *Jan* | 53.915 |
| *Feb* | 57.867 |
| *Mar* | 73.712 |
| *Apr* | 95.078 |
| *May* | 83.182 |
| *Jun* | 81.865 |
| *Jul* | 87.364 |
| *Aug* | 63.367 |
| *Sep* | 185.741 |
| *Oct* | 194.692 |
| *Nov* | 258.355 |
| *Dec* | 184.064 |

*Tabel 3.5. Defacement attack by month, 2010 (zone-h)*[283]

Serangan yang dilakukan dalam tahun 2010 (dalam hitungan bulan). Terlihat bahwa terdapat peningkatan luar biasa dalam satu tahun saja.

---

bisa dilihat berkali-kali. *Mirror* ini adalah sebagai pigura karya seorang *defacer*, karena bisa jadi segera setelah dilakukan *deface*, pemilik *website* yang menjadi korban segera melakukan *recovery* tampilan webnya dan hilanglah tampilan deface tadi. Dengan kata lain, situs-situs tersebut adalah penyedia layanan pengarsipan hasil tampilan dan tingkat kemampuan deface seorang defacer.

[281] Sejauh pengetahuan penulis, submit defacement di dalam zone-h.org sebagian besar meliputi berbagai *defacement* mirrors yang dilakukan oleh para defacer dunia, namun tidak semua *hacker* adalah defacer, dan tidak semua defacement di-submit ke dalam situs ini. Tetapi setidaknya inilah salah satu situs yang populer yang bisa dimanfaatkan oleh para defacer lokal.

[282] Marcelo Almeida (Vympel) dan Boris Mutina (Minor), "Defacements Statistics 2010: Almost 1,5 million websites defaced, what's happening?", <http://zone-h.org/news/id/4737>, 6 Januari 2011.

[283] *Ibid*.

| ***Special Attacks by month*** | ***Year* 2010** |
|---|---|
| *Jan* | 891 |
| *Feb* | 1.851 |
| *Mar* | 1.228 |
| *Apr* | 1.361 |
| *May* | 1.693 |
| *Jun* | 1.711 |
| *Jul* | 1.198 |
| *Aug* | 1.411 |
| *Sep* | 1.265 |
| *Oct* | 1.463 |
| *Nov* | 1.227 |
| *Dec* | 1.576 |
| *Total* | 16.875 |

*Tabel 3.6. Defacement special attack by month, 2010 (zone-h)* [284]

| ***Single attacks by month*** | ***Year* 2010** |
|---|---|
| *Jan* | 10.332 |
| *Feb* | 10.936 |
| *Mar* | 11.908 |
| *Apr* | 14.333 |
| *May* | 12.496 |
| *Jun* | 15.352 |
| *Jul* | 13.762 |
| *Aug* | 13.449 |
| *Sep* | 16.559 |
| *Oct* | 13.366 |
| *Nov* | 32.829 |
| *Dec* | 24.316 |
| *Total* | 189.638 |

*Tabel 3.7. Defacement single attack by month, 2010 (zone-h)* [285]

[284] *Ibid*.
[285] *Ibid*.

| ***Mass attacks by month*** | ***Year* 2010** |
|---|---|
| *Jan* | 43.583 |
| *Feb* | 46.931 |
| *Mar* | 61.804 |
| *Apr* | 80.745 |
| *May* | 70.686 |
| *Jun* | 66.513 |
| *Jul* | 73.602 |
| *Aug* | 49.918 |
| *Sep* | 169.182 |
| *Oct* | 181.326 |
| *Nov* | 225.526 |
| *Dec* | 159.748 |
| *Total* | 1.229.564 |

*Tabel 3.8. Defacement mass attack by month, 2010 (zone-h)* [286]

*Mass attacks* adalah serangan terhadap banyak situs dari satu alamat IP sekaligus dalam satu waktu. Terkadang kerja tim dibutuhkan dalam *mass attacks defacement*, tiap anggota diberi tugas tertentu sesuai dengan kemahirannya sehingga defacement dapat dilakukan secara cepat dan serentak. Contoh kasus dalam mass attacks *defacement* adalah pada beberapa kali saat para *defacer* (*hacker*) Indonesia melakukan *deface* massal kepada ratusan situs dalam wilayah (IP *address*) Malaysia, saat Indonesia dan Malaysia terjadi perselisihan yang turut membakar semangat para *defacer* untuk melakukan aksinya.

| ***Attack Method*** | ***Year* 2010** |
|---|---|
| *File Inclusion* | 634.620 |
| *Attack against the administrator/user (password stealing/sniffing)* | 220.521 |

[286] *Ibid*.

| | |
|---|---|
| *Other Web Application bug* | 124.878 |
| *SQL Injection* | 98.250 |
| *Not available* | 91.402 |
| *Known vulnerability (i.e. unpatched system)* | 42.849 |
| *Undisclosed (new) vulnerability* | 25.552 |
| *Other Server intrusion* | 19.528 |
| *Web Server intrusion* | 18.976 |
| *FTP Server intrusion* | 15.619 |
| *SSH Server intrusion* | 15.214 |
| *Configuration /admin. Mistake* | 13.901 |
| *URL Poisoning* | 13.191 |
| *Remote administrative panel access through bruteforcing* | 12.132 |
| *Brute force attack* | 10.145 |
| *Shares misconfiguration* | 9.530 |
| *RPC Server intrusion* | 7.911 |
| *Telnet Server intrusion* | 7.530 |
| *Web Server external module intrusion* | 7.368 |
| *Mail Server intrusion* | 6.260 |
| *social engineering* | 4.776 |
| *DNS attack through cache poisoning* | 3.689 |
| *DNS attack through social engineering* | 2.878 |
| *Rerouting after attacking the Firewall* | 2.550 |
| *Rerouting after attacking the Router* | 2.458 |
| *Remote service password bruteforce* | 1.987 |
| *Remote service password guessing* | 1.917 |
| *Access credentials through Man In the Middle attack* | 1.752 |
| *Remote administrative panel access through social engineering* | 992 |
| *Remote administrative panel access through password guessing* | 849 |

*Tabel 3.9. Attack Methods, 2010 (zone-h)*[287]

[287] *Ibid*.

Dengan melihat teknik-teknik yang digunakan, kemampuan seorang *defacer* juga dapat dikenali. Keberhasilan suatu teknik juga tergantung kepada keamanan dari situs yang diserang, dan ini juga memperlihatkan seperti apa kemampuan si penjaga situs atau pun servernya.

| Attack Reason | Year 2010 |
|---|---|
| Heh…just for fun! | 829.975 |
| I just want to be the best defacer | 289.630 |
| Not available | 94.017 |
| Patriotism | 58.970 |
| Political reasons | 57.083 |
| Revenge against that website | 45.093 |
| As a challenge | 44.457 |

*Tabel 3.10. Attack Reasons, 2010 (zone-h)*[288]

Dengan mengakses zone-h.org atau zone-ar.com kita dapat melihat berbagai alasan penyerangan terhadap situs-situs tertentu dalam bentuk tampilan yang muncul pada *mirror* hasil *deface* yang dilakukan oleh seorang *defacer*. Dan seringkali seorang *defacer* atau satu *defacer team* memiliki satu alasan yang serupa dalam berbagai serangannya, atau bahkan secara keseluruhan sama.

Marcelo Almeida (Vympel) dan Boris Mutina (Minor) menjelaskan bahwa permasalahannya berasal dari *web-site code*. Mereka membahas soal *exploits* pada *local kernel*, tetapi masalah pertama adalaha pada *code* yang tersusun dalam website. Sebagai contoh, mereka menerima begitu banyak *single defacements* yang menyerang sistem CMS yang tidak beres, sedangkan pengembang CMS baru mempublikasikan perbaikannya beberapa bulan kemudian. Marcelo dan Boris menjelaskan bahwa para pengembang CMS masih melakukan pengembangan dengan tidak aman dan ini

[288] *Ibid*.

dapat merugikan bagi para pemakai.[289] Tulisan tersebut menyampaikan bahwa pada kenyataannya pihak webserver dan pihak pengembang kode masih berada dalam dunia yang berbeda, komunikasi antara kedua pihak ini diperlukan untuk memperkuat sistem keamanan di dalam berbagai situs internet yang berada di bawah pengawasan mereka.

**3.2.4.2 *Cyber-deception/theft***

"*Stealing (money, property), e.g. credit card fraud, intellectual property violations (a.k.a. 'piracy').*"[290] Kutipan tersebut merupakan pengertian (batasan) ringkas yang diberikan oleh Majid Yar terhadap *cyber-deception and theft*. Sedangkan konsep asli dari David S. Wall memberikan pengertian, bahwa *cyber-deception/theft* digunakan untuk mendeskripsikan bermacam jenis cara untuk mendapatkan sesuatu dengan beresiko yang terjadi di dalam *cyberspace*.[291] Pemahaman 'beresiko' di sini dapat diartikan berbahaya bagi si korban.

Dalam statistik sebagai contoh adalah statistik tentang aktifitas *phishing* dalam *cyberspace*. *Phishing* dalam pengertian umum adalah sebuah bentuk pencurian identitas (*identity* theft) dimana seorang penipu menggunakan sebuah email yang tampak asli dari sebuah korporasi besar untuk menipu penerima email, untuk mendapatkan informasi pribadi *online* yang bersifat sensitif, seperti nomer kartu kredit atau kode akun bank.[292]

*The Anti-Phishing Working Group* (APWG) merupakan asosiasi pan-industrial global dan penegakan hukum yang

[289] CMS (*content management system*): Rangkaian kode-kode bahasa pemrograman web yang disusun oleh pihak pengembang CMS, dipublikasikan kepada publik untuk digunakan demi mempermudah para pemilik situs atau blog dalam menciptakan tampilan yang mudah untuk melakukan *posting*, *managing web*, dan *sharing*, tanpa perlu kemampuan khusus dalam tehnik informatika.

[290] Yar, *op.cit.*, hal. 10.

[291] Wall, *op.cit.*, hal. 3.

[292] Schell, *op.cit.*, hal. 246.

memfokuskan diri pada upaya menghilangkan penipuan (*fraud*) dan pencurian identitas (*identity theft*) yang diakibatkan dari segala jenis *phishing*, *pharming* dan *email spoofing*.[293] APWG secara berkala menerbitkan secara *online Average Uptime for Phising Sites Report*, berikut *global report*-nya sepanjang paruh kedua tahun 2010 (2H2010):

- Terdapat setidaknya 67.677 serangan *phishing* di seluruh dunia. Ini lebih besar dari 48.244 yang diamati pada 1H2010, tetapi secara signifikan kurang dari catatan 126.697 yang terpantau pada 2H2009 yang berada dalam ketinggian atas serangan *botnet*[294] dari Avalanche.[295] Peningkatan pada 2H2010 utamanya karena adanya data baru *phishing attack* terhadap sasaran-sasaran di Cina. "*Attack*" didefinisikan sebagai sebuah situs phising yang menyerang sebuah merek atau sasaran tertentu. Satu *domain name* bisa meng-host beberapa *discrete attacks* terhadap bank-bank yang berbeda, sebagai contoh. Penurunan dalam hal serangan bertujuan untuk mengurangi aktifitas oleh gang *phising* yang bernama Avalanche.
- Serangan-serangan terjadi pada 42.624 *unique domain names*. Ini sebuah pencapaian tinggi dalam laporan kami pada 2007, dan peningkatan dikarenakan adanya data baru tentang *phishing*

[293] Situs resmi APWG (The Anti-Phising Working Group): http://www.antiphishing.org/ .

[294] *Botnet: a number of computers connected to the Internet, controlled from a single location without the owner of these computers being aware of this fact.* (Botnet: sejumlah komputer yang terhubung dengan internet, yang dikontrol dari satu tempat tanpa adanya peringatan kepada si pemilik komputer tentang hal tersebut) Lihat: Schell, *op.cit.*, hal. 96.

[295] Phishing Trend Report (www.internetidentity.com) melaporkan tentang Avalanche: berbagai situs yang dimiliki Avalanche merupakan tempat produksi berbagai tehnik *phishing* massal dan distribusi *malware*. Berbagai situs phishing pada berbagai domain milik Avalanche menyasar terhadap platform perbankan komersial dari lebih 30 institusi finansial, berbagai pelayanan online utama, dan berbagai penyedia pencarian lapangan kerja.

Sumber: http://www.internetidentity.com/images/stories/docs/phishing_trends_report_q2-2009_by_internet_identity.pdf, diakses pada 09.00 WIB, 3 Juni 2011.

negara Cina. Jumlah domain names di dunia tumbuh dari sekitar 196 juta pada Mei 2010 menjadi 205,6 juta pada Oktober 2010.

- Dalam laporan tambahan, 3.051 serangan terdeteksi pada 2.318 *unique IP addresses*, lebih banyak daripada *domain names*. (sebagai contoh: http://96.56.84.42/ClientHelp/ssl/index.htm.) Ini dapat dibandingkan dengan 2.018 unique IP yang muncul pada 1H2010. Kami tidak mengamati *phishing* pada IPv6 *addresses*.
- Dari 42.624 *phishing domains*, kami mengidentifikasi 11.769 yang kami yakini terdaftar dengan sengaja untuk membahayakan pihak lain (*maliciously*), oleh pelaku *phishing* (28%). Dari itu semua, 6.382 telah terregistrasi untuk melakukan phishing terhadap berbagai sasaran di Cina. 30.855 domain lainnya telah di-*hack* atau menggunakan jasa web hosting yang mudah diserang. Registrasi yang dengan kesengajaan untuk berbuat jahat tampaknya berada pada 56 TLD.[296]
- *Phishing* terkonsentrasi pada *namespaces* tertentu. Enam puluh persen serangan terjadi dalam empat TLD: .COM, .CC, .NET, dan .ORG. Dan 89 persen *malicious domain registrations* dibuat dalam empat TLD: .COM, .TK, .NET, dan .INFO.[297]

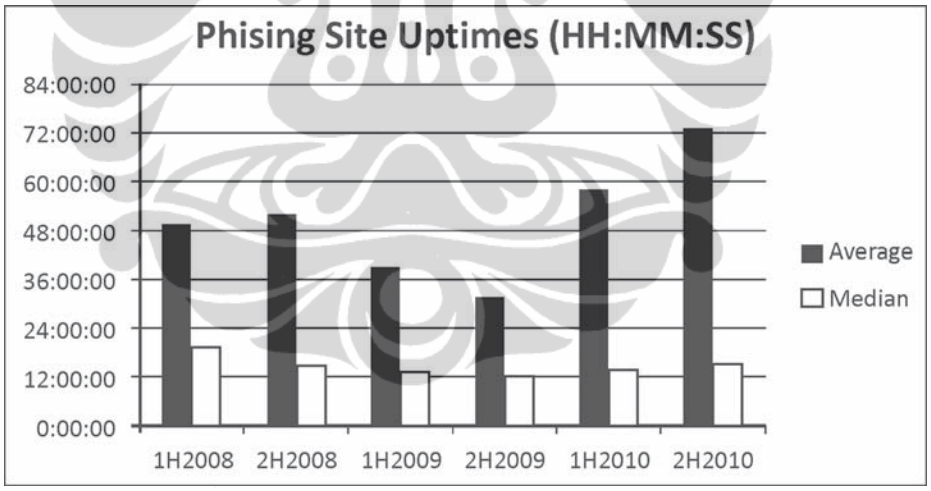
Setelah mencapai titik rendah yang bersejarah pada 2H2009, rata-rata dan nilai tengah (median) dari *phishing attack* meningkat sekitar 2010. Rata-rata uptime-nya 73 jam, merupakan rata-rata terlama bagi sembarang waktu periodik sejak APWG memulai pengukuran *uptime* tiga tahun lalu. Nilai tengahnya adalah 15 jam 19 menit, salah satu nilai tengah yang pernah dicatat APWG.

[296] TLD: *Top Level Domain*, adalah domain pada level tertinggi dari DNS (*Domain Name System*) di internet. Misalkan sebuah domain name: "www.universitas.com", *top-level domain*-nya adalah ".com". Dan sebagainya.

[297] APWG, Global Phishing Survey: Trends and Domain Name Use in 2H2010, http://apwg.org/reports/APWG_GlobalPhishingSurvey_2H2010.pdf, April 2011, hal. 4-5.

*Uptime* atau waktu keberadaan dari serangan phishing adalah pengukuran vital untuk melihat seberapa merusaknya serangan-serangan tersebut, dan merupakan pengukuran kesuksesan atas upaya-upaya untuk penanggulangan (*mitigation*).[298]

Semakin lama *phishing attack* yang dimaksud aktif, semakin banyak uang para korban dan target institusional yang hilang. Dua hari pertama dari sebuah serangan *phishing* diyakini sebagai yang paling menguntungkan bagi seorang *phisher* (pelaku phishing), maka pembekukan secara cepat merupakan hal esensial. *Phish* yang berjalan lama bisa jadi sebuah kecenderungan dalam rata-rata sejak beberapa situs *phishing* bisa jadi berjalan beberapa sejak minggu terakhir atau bahkan bulan, maka nilai tengahnya juga menjadi barometer yang berguna bagi keseluruhan upaya penanggulangan.[299]




*Grafik 3.1. Historic trend phishing site uptime* (2008-2010).[300]

| All Phish, All TLDs | Average (HH:MM:SS) | Median (HH:MM:SS) |
|---|---|---|
| Dec 2010 | 38:54:53 | 11:35:02 |
| Nov 2010 | 70:38:07 | 15:37:53 |

[298] *Ibid*., hal. 7.
[299] *Ibid*.
[300] *Ibid*.

| | | |
|---|---|---|
| Oct 2010 | 70:24:08 | 17:13:35 |
| Sep 2010 | 101:57:45 | 14:44:43 |
| Aug 2010 | 78:02:08 | 18:23:03 |
| Jul 2010 | 74:56:01 | 14:05:05 |
| **2H2010** | **73:05:31** | **15:19:41** |
| 1H2010 | 58:10:16 | 13:42:16 |
| 2H2009 | 31:38:00 | 11:44:15 |
| 1H2009 | 39:11:00 | 13:15:32 |
| 2H2008 | 52:01:58 | 14:43:15 |
| 1H2008 | 49:30:00 | 19:30:00 |

*Tabel 3.11. Uptime for the last three years* (2008-2010).[301]

Dari *uptime* yang ditunjukkan dalam tabel dan grafik, terlihat bahwa semakin lama waktu hidup suatu *phishing scam*, yang memanfaatkan berbagai situs lemah (atas serangan peretasan), dan bisa jadi situs tersebut telah mengalami *defacement* sedemikian rupa untuk mendapatkan identitas para korban dengan memanfaatkan salah *login* dan semacamnya. Maka semakin besar kerugian yang dapat dibayangkan, dengan melihat bahwa semakin hari semakin besar ancaman tersebut secara global.

### 3.2.4.3 *Cyber-pornography/obscenity*

Dalam ruang maya setiap orang dapat dengan leluasa berinteraksi dengan berbagai sumber informasi yang dia ingin ketahui, dan orientasi tentang keinginan berkembang seiring dengan perkembangan serta perubahan psikologisnya. Muatan pornografi merupakan salah satu yang menarik untuk diamati, karena keberadaannya jelas terdapat banyak peraturan di dunia nyata yang melarangnya akan tetapi demikian mudahnya mendapatkannya di dunia maya, bagi siapa saja, selama memiliki kemampuan berselancar dan mengaksesnya atau memiliki kemampuan untuk membeli beberapa akses khusus atau layanan tambahan.

[301] *Ibid*., hal. 8.

*Cyber-pornography* atau *cyber-obscenity* terkadang menjadi penilaian negatif terhadap keberadaan jaringan internet, secara awam kebebasan akses internet terkadang dipahami juga sebagai kebebasan dalam mengakses konten negatif semacam ini. Pandangan skeptis terhadap internet dan pornografi dan terkadang memberi label negatif merupakan salah satu pendorong keinginan untuk lebih mengaksesnya. Dan semakin luasnya akses terhadap berbagai konten pornografi di dunia maya berpengaruh terhadap pola pikir dan moralitas masyarakat.

| **Pornography Time Statistics** |
|---|
| Every second - $3,075.64 is being spent on pornography. |
| Every second - 28,258 internet users are viewing pornography. |
| Every second - 372 internet users are typing adult search terms into search engines. |
| Every 39 minutes: a new pornographic video is being created in the United States. |

*Tabel 3.12. Pornography time statistics.*[302]

| **Internet Pornography Statistics** | |
|---|---|
| Pornographic websites | 4.2 million (12% of total websites) |
| Pornographic pages | 420 million |
| Daily pornographic search engine requests | 68 million (25% of total search engine requests) |
| Daily pornographic emails | 2.5 billion (8% of total emails) |
| Internet users who view porn | 42.7% |
| Received unwanted exposure to sexual material | 34% |
| Average daily pornographic emails/user | 4.5 per Internet user |
| Monthly Pornographic downloads (Peer-to-peer) | 1.5 billion (35% of all downloads) |

[302] Jerry Ropelato, "Internet Pornography Statistics," <http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html>, diakses pada 4 Juni 2011, 09.00 WIB.

| | |
|---|---|
| Daily Gnutella "child pornography" requests | 116,000 |
| Websites offering illegal child pornography | 100,000 |
| Sexual solicitations of youth made in chat rooms | 89% |
| Youths who received sexual solicitation | 1 in 7 (down from 2003 stat of 1 in 3) |
| Worldwide visitors to pornographic web sites | 72 million visitors to pornography: Monthly |
| Internet Pornography Sales | $4.9 billion |

*Tabel 3.13. Pornography statistic* (2005-2006).[303]

Banyaknya akses dan besarnya 'kebutuhan' para 'pemakai internet' terhadap konten pornografi secara global sungguh mencengangkan. Tidak sebatas mencari akses gratis, pendapatan dari berdagang konten pornografi pun dikatakan, secara global, bisa mengalahkan perusahaan-perusahaan besar:

> *It's big business. The pornography industry has larger revenues than Microsoft, Google, Amazon, eBay, Yahoo, Apple and Netflix combined. 2006 Worldwide Pornography Revenues ballooned to $97.06 billion. 2006 & 2005 U.S. Pornography Industry Revenue Statistics, 2006 Top Adult Search Requests, 2006 Search Engine Request Trends are some of the other statistics revealed here.*[304]

*Obscenity* (*pornography*) di ruang *cyber* adalah permasalahan yang dihadapi generasi bangsa sebagai sebuah tantangan hebat, terutama mereka yang tengah mencari jati diri, hal ini dapat mendorong meningkatnya kejahatan seksual dan menekan moralitas anak bangsa secara besar-besaran jika tidak dilakukan pengendalian. Peningkatan jumlah situs dengan muatan pornografi yang demikian mencengangkan dan jejaring bisnis di dalamnya mengingatkan tentang bagaimana "kesenangan tidak dapat

[303] *Ibid*.
[304] *Ibid*.

dikuantifikasikan" dalam pembahasan Henry Hazlitt tentang moralitas (Henry Hazlitt, 1964). Hazlitt menjelaskan bahwa pada kenyataannya kita tidak bisa mengukur kesenangan dalam hal kuantitas.[305] Hal ini biasa kita definisikan sebagai memaksimalkan kepuasan atas kesenangan.

Sebagaimana kesenangan terhadap konten pornografi yang sulit dikendalikan, hal ini terlihat dalam grafik yang selalu meningkat dalam informasi yang disampaikan oleh Jerry Ropelato, semakin awal taraf usia yang disulut ke dalam kenikmatan atas konten pornografi, maka keuntungan yang didapatkan akan lebih meningkat dan produksi konten tersebut akan jauh lebih banyak dari sebelumnya, dan seterusnya hingga sulit menahan perputaran dan memotong mata rantainya.

| **Children Internet Pornography Statistics** | |
|---|---|
| Average age of first Internet exposure to pornography | 11 years old |
| Largest consumer of Internet pornography | 35 - 49 age group |
| 15-17 year olds having multiple hard-core exposures | 80% |
| 8-16 year olds having viewed porn online | 90% (most while doing homework) |
| 7-17 year olds who would freely give out home address | 29% |
| 7-17 year olds who would freely give out email address | 14% |
| Children's character names linked to thousands of porn links | 26 (Including Pokemon and Action Man) |

*Tabel 3.14. Children internet pornography statistic* (2005-2006).[306]

[305] Henry Hazlitt, *Dasar-Dasar Moralitas* (*The Foundation of Morality*), diterjemahkan oleh Cuk Ananta Wijaya, (Yogyakarta: Pustaka Pelajar, 2003), hal. 34-36.

[306] Ropelato, *Ibid*.

### 3.2.4.4 *Cyber-violence*

Majid Yar mendefinisikan *cyber-violence* sebagai: "*…doing psychological harm to, or inciting physical harm against others, thereby breaching laws relating to the protection of the person, e.g. hate speech, stalking*."[307] Hal ini bisa didapatkan pada definisi mengenai cyber-bullying.

Sifat alami dan bentuk-bentuk dari *bullying* dan *cyber-bullying* didukung oleh banyak faktor yang mendasarinya. Faktor tersebut bisa memengaruhi cara hukum diintrepretasikan dan diterapkan.[308] *Cyber-bullying* secara umum berbentuk gangguan verbal maupun tertulis. Komunikasi tertulis, khususnya online, bisa seringkali disimpan dan direproduksi, dan memiliki elemen yang bersifat permanen, dimana kata yang diucapkan, jika tidak terekam, sulit untuk direproduksi.[309]

- *71% of teen girls and 67% of boys who sent or posted sexually suggestive content say they sent it to a boyfriend or girlfriend.*
- *Female teens are far more likely than male teens to post personal photos or videos of themselves online.*
- *22% of teenage girls say they posted nude or semi-nude photos or videos of themselves online.*
- *Only 15% of parents are "in the know" about their kids' social networking habits, and how these behaviors can lead to cyberbullying.*
- *70% of children 7 to 18 years old have accidentally encountered online pornography, often through a web search while doing homework.*
- *Girls are more likely than boys to be the target of cyber bullying.*

---

[307] Yar, *op.cit.*, hal. 10.

[308] Shaheen Shariff, *Confronting Cyber-Bullying*, (Cambridge: Cambridge University Press, 2009), hal. 52.

[309] *Ibid*., hal. 43.

- *The largest group of Internet porn consumers is children ages 12-17.*
- *20% of teenaged Internet users have been the target of an unwanted sexual solicitation (requests for sexual activities, chat, or information).*
- *41% of unwanted sexual solicitations, 29% of unwanted exposure to sexual materials, and 31% of harassment occurred when children were online with their friends.*
- *In 2004, there were at least 3,433 child abuse domains online; in 2006 there were at least 10,656.*
- *70% of kids ages 8-18 have accidentally encountered online pornography, very often by entering an innocent search term while doing their homework.*
- *31% of kids ages 12-18 have lied about their age in order to access a website.*
- *90% of children ages 8-16 have seen online pornography.*
- *Law enforcement officials estimate that more than 50,000 sexual predators are online at any given moment.*
- *20% of all Internet pornography involves children, with more than 20,000 new images posted weekly.*
- *65% of 8-14 year olds have been involved in a cyber-bullying incident.*
- *96% of teens use social networking applications such as Facebook, MySpace, Chat rooms, and blogs.*
- *69% of teens regularly receive online communications from strangers and don't tell a parent or caretaker.*
- *86% of the girls polled said they could chat online without their parents knowledge – 57% could read their parents e-mail, and 54% could have a cyber relationship.*

- *Approximately 89% of sexual solicitations of youth were made in chat rooms or through Instant Messaging.*
- *95% of parents don't know common chat room acronyms teenagers use such as when a parent is watching. The acronyms are POS (parent over shoulder), P911 (parent alert), and A/S/L (age/sex/location).*
- *An estimated 725,000 children have been "aggressively" asked for sex, defined as an offer to meet in person.*
- *The FBI reports a 2000 percent increase in the number of child pornography images on the internet since 1996.*
- *According to the FBI, Chat rooms offer the advantage of immediate communication around the world and provide the pedophile/predator with an anonymous means of recruiting children into sexually illicit relationships.*
- *Only 1/3 of households with Internet access are protecting their children with filtering or blocking software.*
- *1 in 33 youth received an aggressive sexual solicitation – Translation – A predator asked a young person to meet, called a young person on the phone, or sent the young person correspondence, money, or gifts.*
- *77% of the victims for online predators were age 14 or older.*[310]

[310] http://www.guardchild.com/statistics/, diakses pada 6 Juni 2011, pukul 21.00 WIB.

# BAB IV
# PENEGAKAN HUKUM TERHADAP *CYBERCRIME*

## 4.1 Peran Publik Mayantara dalam Penegakan Hukum

Dalam pertemuan dengan para aktifis dunia maya (terutama para *hacktivist*), ditemukan banyaknya semangat (optimisme) akan kemampuan hukum berjalan dengan baik. Pada kenyataannya mereka tidak menyampaikan pesimisme terhadap kondisi *cyberspace* yang melaju dengan kencang, berikut kejahatan di dalamnya. Mereka memahami dalam aktifitas mereka, bahwa dunia maya dan kegiatan di dalamnya dapat dikelola.

Di dunia nyata seseorang yang menyampaikan pemahaman tentang *cyberspace* cenderung melewatkan (bahkan tidak menyentuh sama sekali) fase untuk berinteraksi secara baik dengan *cyberspace* itu sendiri, dan hal ini memberikan dua kecenderungan. *Pertama,* para pengamat yang membawa kesan-kesan kehidupan *nyata* dan keteraturannya kemudian secara *a priori* menyatakan bahwa bagaimanapun *cyberspace* harus diatur sebagaimana keteraturan di dunia nyata dikelola, namun mereka sendiri tidak pernah melakukan interaksi secara aktif dalam *cyberspace*. *Kedua*, para pengamat yang mengamati bagaimana kemajuan dunia maya, kekacauan di dalamnya, menyerap hegemoni media massa yang cenderung menyampaikan pesimisme tentang keteraturan di dalamnya dan terpengaruh olehnya, yang kemudian memandang bahwa tidak mungkin *cyberspace* dikontrol dengan keteraturan atau hukum. Bagi mereka kekacauan dalam *cyberspace* bisa memunculkan *hysteria*.

Pihak kedua bisa jadi muncul dari kalangan aktifis di dunia maya yang menikmati kesehariannya dengan internet dan semua yang berlalu lalang dan melihat kekacauan di *dalamnya*. Para *blogger* bisa jadi salah satunya, yang menyampaikan banyak keluhan ke dalam internet. Dan sebagian akan mengeluh kepada internet bukan kepada mereka yang mengelola sistemnya. Ini terjadi karena kurangnya pemahaman tentang kewajiban pemberian keamanan atas pemakaian jasa melalui internet, hal ini juga memungkinkan kecenderungan

kurangnya laporan dari masyarakat tentang kejahatan yang mereka alami dan bagaimana memprosesnya secara hukum.

Karena itulah banyak anggapan tentang *cyberspace* dari mereka yang tidak memahaminya dengan sebaik mungkin. Meminjam pemahaman sosiologis Habermasian, bisa disebut dengan "solidaritas tanpa intimitas"[311] dalam sisi negatifnya, yaitu anggapan yang muncul bahwa sulit mengatur *cyberspace* sedangkan mereka tidak memahami benar (intimitas) bagaimana *cyberspace* itu berjalan dan dapat dikelola. Oleh karena itulah pendekatan tentang *cyberspace* semestinya disampaikan oleh para pakar *cyber* yang hidup dan berkecimpung dalam *cyberspace*.

Para penegak hukum akan menghadapi banyak tantangan baru dalam upaya menyelesaikan sebuah tindak kejahatan yang melibatkan komputer (*computer-facilitated crimes*), yang berkembang seiring dengan ketergantungan kita terhadap komputer, yang dengan seksama akan memberikan pengaruh lebih besar juga dalam *menciptakan* peluang bagi tindak kejahatan dengan tingkat perusakan yang jauh lebih besar. Seperti kita pahami, teknologi komputer dan internet yang mengikutinya, memberikan banyak manfaat bagi manusia. Komputer dan internet meringkas banyak pekerjaan dan meningkatkan efektifitas, bahkan bisa disebut—jika kita meminjam istilah Yasraf Amir Piliang— "dunia yang terlipat", sebuah judul buku yang ia tulis. Dan sesuatu yang telah demikian ringkas di mata kejahatan benar-benar menjadi sebuah materi yang termampatkan, yang untuk menghanguskan semuanya menjadi lebih mudah. Seperti menyimpan seisi rumah ke dalam sebuah kardus kecil untuk meringkasnya, dan untuk mencuri atau memusnahkan keseluruhan akan jauh lebih mudah dari sebelumnya.

[311] Meski yang dimaksud sebenarnya adalah solidaritas seperti yang terjadi pada gempa bumi di Timur Laut lepas pantai Jepang pada Maret 2011, kemudian media menyampaikan berbagai sisi pandang laporan pemberitaan yang dapat memengaruhi setiap mereka yang menerima informasi itu untuk menyampaikan bantuan secara sukarela. Dengan modernisme inilah kita dapat membangun solidaritas tanpa intimitas di dalam diri kita untuk mereka yang tidak pernah kita dengar sekalipun namanya.

### 4.1.1 Pelaksanaan Penegakan Hukum dan Tantangannya

Penegakan hukum dalam *cyberspace* di Indonesia oleh seluruh narasumber penelitian ini masih dipandang tidak efektif. DM memberikan uraian dan beberapa contoh permasalahan,

> "Negara masih sering melakukan *policy* yang tidak memperhatikan realitas para *netter*. Contohnya, melakukan *sweeping* Windows *original* di warnet, namun sosialisasi belum meluas. Negara bisa membuat *operating system* sendiri dengan biaya murah, tetapi lebih asyik dengan pemblokiran. Negara memilih menyehatkan bank dengan biaya tinggi, daripada menempatkan *security professional* di bank-bank itu. Jadi berdasarkan berita yang saya ikuti, *policy* pemerintah belum memperlihatkan cara berpikir lateral, yang bisa mengantisipasi masalah yang lebih besar."[312]

Dalam beberapa wawancara dan tanya jawab melalui internet, dapat dilihat masih kurangnya pelaksanaan penegakan hukum. Dari penilaian Onno W. Purbo dan beberapa orang *founder* komunitas *hacker*, serta aktivis dunia maya, dapat dilihat bahwa sebagian besar tindak kriminal di dalam ruang maya masih minim penanganan. Hal tersebut didukung dengan minimnya kemampuan dan perbekalan teknis yang dimiliki penegak hukum, terutama kepolisian yang merupakan ujung tombak dalam penanganan berbagai bentuk pelanggaran hukum.

Bahkan dikatakan oleh KYF bahwa penegakan hukum di dunia maya sepenuhnya, karena UU khusus *Cybercrime* belum ada, walaupun begitu tetap ada upaya penegakan hukum dengan UU yang ada walaupun belum maksimal.[313] Dan XP, lead founder *Hacker* Cisadane, menilai bahwa penegak hukum di Indonesia sudah menjalankan tugasnya, tetapi menurutnya masih kurang maksimal. Onno W. Purbo, KYF, XP, DM, BD, dan PZ yang mewakili komunitas masing-masing menyatakan bahwa penegakan hukum beserta undang-undang secara *general* belum memadahi.

Dalam situs zone-h.org, dengan mendata beberapa nama *hacker* populer di Indonesia yang memampang hasil *defacement*-nya di berbagai

[312] Wawancara dengan DM, 9 April 2011
[313] KYF, 16 April 2011.

situs di dunia maya. Dapat dilihat bahwa nama-nama yang populer di ruang maya (terutama komunitas *hacker* Indonesia), dua di antaranya ada dalam catatan sepuluh besar dan memiliki rekaman aksi *defacement*-nya dalam jumlah yang luar biasa.[314]

| No. | Notifier | Single def. | Mass def. | Total def. | Homepage def. | Subdir def. |
|---|---|---|---|---|---|---|
| 1. | Iskorpitx | 61822 | 380038 | 441860 | 257082 | 184778 |
| 2. | Hmei7 | 26175 | 11591 | 37766 | 2101 | 35665 |
| 3. | 1923Turk | 25794 | 105644 | 131438 | 57587 | 73851 |
| 4. | GHoST61 | 22200 | 254108 | 276308 | 167007 | 109301 |
| 5. | Fatal Error | 20256 | 38152 | 58408 | 52107 | 6301 |
| 6. | KaMtiEz | 12163 | 14266 | 26429 | 9919 | 16510 |

*Tabel 4.1 Notifier Statistic Zone-h.org Juni 2011.*[315]

Terlihat sebagai contoh *Hmei7* dan *KaMtiEz* adalah dua *hacker* (*defacer*) lokal yang populer di Indonesia dan dunia, sedangkan *iskorpitx* dan *1923Turk* adalah dua *hacker* (*defacer*) dari Turki.[316] Tidak semua defacer menjadi notifier di forum zone-h, terdapat juga situs semacam zone-h.org dan zone-ar.com di Indonesia yang memiliki sangat banyak notifikasi dari berbagai situs lokal.

Coba dibandingkan dengan data statistik tahun 2010 tentang web hacking statistik:

| | | |
|---|---|---|
| 1. | 77,85% | Origine non determinata (undetermined origin) |
| 2. | 3,80% | Turchia (Turkey) |
| 3. | 3,16% | Romania (Romania) |
| 4. | 2,53% | Cina |
| 5. | 2,53% | Russia |

[314] http://www.zone-h.org/stats/notifier, diakses pada 13 Juni 2011, pukul 18.00 WIB.

[315] Lihat http://www.zone-h.org/stats/notifier, diakses pada 13 Juni 2011, pukul 18.00 WIB. Zone-h.org dan zone-ar.com adalah dua situs populer untuk mengunggah dan merekam (sebagai mirror) dari *defacement result*.

[316] Data *hacker* dan *defacer* populer bisa dilihat dari berbagai *mirror* (*link* atau rekaman layar hasil aksi *defacement* yang di-*posting* dalam forum semacam zone-h.org). sebagian besar *defaced link* akan menunjukkan jejak (nama) *defacer*-nya, dan sekaligus ucapan terima kasih (*thanks to*) kepada teman-teman atau *hacker* atau defacer lain yang menginspirasi.

| | | |
|---|---|---|
| 6. | 1,27% | Libano (Lebanon) |
| 7. | 1,27% | Indonesia |
| 8. | 1,27% | India |
| 9. | 1,27% | Ucraina (Ukraine) |
| 10. | 0,63% | Argentina – Iran – Bulgaria – Danimarca |

*Tabel 4.2 Klasifikasi cyberattack berdasarkan sumber geografis.*[317]

Dan kemudian sebagai contoh adalah Amerika Serikat, dapat diambil data *Internet Crime* Report dari Internet *Crime Complaint Center* (IC3).[318] Dari data tiga tahun (2008, 2009, 2010) terlihat perbandingan antara *complaints received* dengan *referrals*:

| **Year** | **Complaints received** | **Referrals** |
|---|---|---|
| 2008 | 275,284 | 72,940 |
| 2009 | 336,655 | 146,663 |
| 2010 | 303,809 | 121,710 |

*Tabel 4.3 Coplaints – referrals: cybercrimes (2008-10) di Amerika Serikat.*[319]

Data-data dari tabel-tabel tersebut di atas dapat menjadi gambaran sederhana bahwa ancaman global secara konstan mengalami peningkatan, baik dari dalam maupun dari luar. Bahwa supremasi hukum semestinya ditunjukkan dengan kekuatan alat-alat hukum dalam wilayah hukumnya. Di dalam negeri sendiri terdapat berbagai kelemahan dalam pelayanan PANDI (Pengelola Nama Domain Internet Indonesia),[320] sebagaimana diterangkan dalam wawancara dengan BD.

> "Dan PANDI kan sebagai pengelola domain, PANDI-nya sendiri kalau bisa itu *user*-nya itu dibuat sendiri-sendiri. Jadi nggak perlu macam-macam. Orang mau mengurus sudah malas karena kebanyakan syarat. katanya untuk keamanan, nyatanya nyolong KTP

[317] http://www.oversecurity.net/2010/12/01/web-hacking-statistiche-2010-1%C2%B0-puntata-da-dove-originano-gli-attacchi-globali/, diakses pada 13 Juni 2011, pukul 18.00 WIB.

[318] http://www.ic3.gov/media/annualreports.aspx, diakses pada 13 Juni 2011, pukul 19.00 WIB.

[319] *ibid.*

[320] http://www.pandi.or.id/.

> di Google saja bisa buat syarat, dan jadi. Dari hal seperti itu kan jadi *image* buat masyarakat."[321]

Kelambanan manajemen internal PANDI dan jika terdapat kelemahan keamanan dari sisi sistemnya akan memudahkan serangan dari dalam dan luar negeri terhadap berbagai situs dengan TLD (*Top Level Domain*) *.id, baik dengan mencurangi saat meregistrasikan alamat, maupaun menipu keamanannya.

Di lain sisi berbagai kebijakan yang diambil pemerintah yang cenderung tidak teliti dan merugikan aktifitas mayantara justru bisa menimbulkan perlawanan,

> "Kalau tahu dunia maya itu enak-enak nggak enak, karena kalau *kesenggol* satu, gerak semua, membahayakan *server-server* Indonesia. Bedanya dengan Malaysia. Kalau masalah dengan Malaysia, hari-hari besar Malaysia itu tidak usah diperintah, *defacer-defacer* Indonesia itu sudah aktif sendiri, dan jauh-jauh dari hari sebelumnya sudah mencari target dulu, pada saatnya tinggal eksekusi. Nah kebanyakan yang terjadi seperti itu."[322]

Apa yang diungkapkan BD bisa menjadi saran bahwa semestinya Pemerintah beserta Depkominfo dalam memberikan berbagai kebijakan yang melibatkan kepentingan orang banyak di mayantara perlu mempertimbangkan sensitifitasnya. Pada kenyataannya sosialisasi terkadang belum diberikan dengan benar dalam ruang maya, tetapi eksekusi dan operasi sudah dilakukan besar-besaran, seperti dicontohkan DM tentang operasi Operating System di atas.

Dari melihat beberapa statistik, meskipun Indonesia bukanlah yang tertinggi dalam tingkat kejahatan internet. Menurut statistik dalam situs oversecurity.net pada tabel di atas, Indonesia ada pada peringkat ke tujuh dalam tingkat *cybercrime* menurut peta geografis. Namun, sekali lagi kita melihat kenyataan bahwa, kemahiran dalam melakukan tehnik serangannya, seorang yang *commit to crime* akan mempertimbangkan baik-baik sisi keselamatannya dan potensi tertangkapnya. Kita melihat bahwa

[321] Wawancara dengan BD, 11 April 2011.
[322] *ibid*.

*undetermined origin* ada dalam skala terbesar (77,85%). Kenyataannya, secara sederhana di dunia maya terdapat berbagai situs penyedia jasa penyembunyian IP address pelaku secara gratis dan tanpa registrasi. Sedangkan dalam kajian hukum masih luas pembahasan tentang wilayah hukum mayantara, yang sebagian mempersepsikan IP address itulah identifikasi wilayah hukum suatu tindak kejahatan terjadi. Tantangan dan ancaman semakin berkembang saat kemampuan untuk melangkah lebih jauh dari potensi kejahatan sangat minim.

Dari statistik yang diberikan oleh IC3 (*Internet Crime Complaint Center*) tersebut di atas terlihat bahwa *complaints* (laporan atas tindak kejahatan mayantara yang dialami oleh setiap pelapor) selalu jauh lebih besar dalam perhitungannya dibandingkan dengan *referrals* (laporan yang diproses, dilanjutkan kepada lembaga penegakan hukum di masing-masing negara bagian). Dalam tahun 2008, perbandingan laporan yang layak proses dengan keseluruhan laporan masuk adalah 1:3,77, pada 2009 perbandingannya: 1:2,29, dan pada 2010 sebesar 1:2,49.

Lantas bagaimana cara membandingkannya dengan Indonesia? Apakah proses pelaporan *cybercrime* kita sudah memiliki mekanisme yang layak? Masih terlalu banyak keraguan dalam penanganannya. Dan semuanya berawal pada dua tahap utama inisiatif penegakan hukum oleh lembaga yang ada. Yaitu mekanisme pelaporan yang terjamin dengan baik, serta adanya jaminan pemrosesan (*referral*) laporan tersebut. BD menguraikan mekanisme yang logis untuk keadaan Indonesia,

> "Menangkap? Jadi topologinya begini. Sekarang ada pemilik website itu melapor, entah itu website pemerintah, temen. Melaporkan kepada pihak Depkominfo untuk menangkap si pelaku penjebol. Ya, kan mesti laporan dulu, laporan baru diusut, dan itukan ada proses sampai tertangkapnya si pelaku, tahapnya nggak sedikit. Makan waktu, dan yang pasti butuh pendalaman. Karena sang *defacer* untuk membobol website itu biasanya juga *behind proxy*, susahnya kan disitu nanti untuk *trace*, untuk menangkap si pelaku kan susahnya di situ. Padahal untuk ISP juga agak susah untuk dimintai keterangan IP ini kepemilikannya siapa? Dan alamat di mana? Itu agak susah. Kecuali

untuk pihak yang berwenang mungkin bisa. Mendapat IP itu kan ada prosesnya juga, tidak semudah itu bisa mendapat."[323]

Dan jika yang dilakukan terhadap *cybercrime* masih melalui proses sebagaimana polisi menangani kejahatan di dunia nyata dan dengan peralatan yang tidak sesuai dengan teknologi pelaku kejahatan yang mereka hadapi, bisa jadi seiring dengan bergantinya hari atau jam, pemrosesan tindak kejahatan untuk menyeret pelakunya ke pengadilan akan gagal. Dan saat para korban tidak dapat lagi merasakan pembalasan kerugian dan rasa aman yang lebih terjamin, kembali lagi kepada kepercayaan publik pada supremasi hukum.

Pada kenyataannya, saat berusaha mencari cara bagaimana melakukan pelaporan terhadap kejadian tindak pidana mayantara di Indonesia, secara teknis cukup ragu setelah melihat halaman pada situs POLRI, http://www.polri.go.id/laporan-all/lpm/adu/. Pada halaman aduan ini, aduan tentang berbagai bentuk kejahatan masih dianggap sama, baik kejahatan konvensional maupun kejahatan *cyber* yang berciri transnasional isian form aduannya dibuat sama dengan pilihan jenis laporan yang minim, dan adanya kelemahan/ kekurangan dalam penyempurnaan halaman aduan tersebut.[324]

Langkah selanjutnya adalah berusaha mencari *form* aduan pada situs interpol.go.id (dalam kategori kejahatan dunia maya). Secara khusus tidak disediakan form yang memadai untuk melakukan laporan *digitalcrime* terutama *cybercrime*, yang dalam situs tersebut masuk dalam kategori

---

[323] *Ibid*.

[324] http://www.polri.go.id/laporan-all/lpm/adu/, diakses pada 13 Juni 2011, pada pukul 23.00 WIB. Saat mengakses situs tersebut pada jam dan waktu yang sama, dapat dilihat secara sederhana terdapat cacat dalam form. Pada bagian bawah isian deskripsi aduan terdapat script/texts: " To use reCAPTCHA you must get an API key from https://www.google.com/recaptcha/admin/create." reCAPTCHA adalah cara pemilik situs untuk membedakan laporan yang dilakukan oleh manusia atau yang dilakukan oleh *bot* (*robot system*, sistem yang bisa berjalan sendiri beraktifitas dalam ruang digital secara *remote*). Dan adanya teks tersebut memperlihatkan bahwa pembuatan situs belum tuntas, dan keamanan (dalam hal jaminan keaslian) laporannya pun diragukan. Dan lebih jauh, dalam hal *cybercrime* yang membutuhkan banyak verifikasi atas kejadian yang dialami korban yang berkaitan erat dengan keamanan digital, hal ini menimbulkan keraguan besar dalam memenuhi syarat formal aduan kejahatan digital.

kejahatan transnasional.[325] Form pelaporan yang ada pada situs Interpol tersebut jauh lebih sederhana daripada situs POLRI. Di sisi lain, situs Kominfo milik Kementerian Komunikasi dan Informatika Republik Indonesia tidak memiliki halaman keluhan atau aduan yang sekiranya bisa bekerjasama dengan POLRI sebagai lembaga penegakan hukum.[326] Sedangkan *Internet Crime Complaint Center* (IC3) adalah sebuah *partnership* antara *Federal Bureau of* Investigation (FBI), *National White Collar Crime Center* (NW3C), dan *Bureau of Justice Assistance* (BJA). Dengan cara pandang serius maka koordinasi dari berbagai lembaga terkait sangat diperlukan.

Jika dibandingkan dengan Indonesia, Amerika Serikat melalui situs "ic3.gov" memberikan alur pelaporan terjadinya tindak kejahatan mayantara yang lebih selektif dan terarah. Dalam satu laporan disertai dengan berbagai pilihan yang mampu mengarahkan pelapor kepada fokus masalah, hal ini membantu pelapor untuk memahami situasi yang ia hadapi secara bersamaan dengan pihak IC3 memfokuskan klasifikasi dan memferifikasi permasalahan pelapor tahap demi tahap laporan secara mandiri. Pada kenyataannya basis data informasi laporan tersebut digunakan juga sebagai alat survey bagi pihak penegak hukum untuk memberikan pendidikan yang baik kepada masyarakat (yang terdapat dalam berbagai *e-book* gratis) melalui situs tersebut. Sekaligus bermanfaat bagi penegakan hukum yang lebih mampu mengantisipasi trend perkembangan cybercrime di negara tersebut. Pihak IC3, dengan mekanisme yang sedemikian fokus dan logis menyatakan bahwa setiap laporan dapat diproses secara hukum dan dipergunakan dalam trend analysis (*cybercrime*).

---

[325] http://www.interpol.go.id/id/kejahatan-transnasional/kejahatan-dunia-maya, diakses pada 13 Juni 2011, pukul 23.00 WIB.

[326] http://www.kominfo.go.id/. Namun muatan informatif dan edukatif dari situs Kominfo patut didukung demi memberikan kesadaran publik untuk senantiasa menjelajahi dunia maya dengan beretika, aman, dan nyaman.

> *Complaints are submitted to IC3 at www.ic3.gov. The information is reviewed, categorized and, when appropriate, referred to local, state or federal law enforcement. All complaints are accessible to law enforcement and are used in trend analysis. These complaints help provide a basis for future outreach events and educational awareness programs.*[327]

Melihat apa yang ada dalam IC3 sekiranya dapat menjadi contoh yang baik bagi Indonesia dalam memberikan fasilitas penegakan hukum bagi publik yang lebih responsif. Dan Indonesia pun sebagaimana negara-negara lain yang telah melihat ancaman permasalahan hukum yang besar dalam *cyberspace* masih terus berusaha membenahi dan meningkatkan kemampuannya. Onno W. Purbo menegaskan:

> "Segelintir penegak hukum seperti Pak Petrus Golose dan kawan-kawan, dari unit *cybercrime* bisa dan punya kemampuan penegakan hukum di dunia *cyber* tapi sebagian besar sih gak."[328]

Upaya kepolisian untuk terus membekali jajarannya yang ada di baris depan persinggungan dengan kejahatan mayantara patut diapresiasi dengan baik. Akan tetapi perkembangan kejahatan dan ledakan populasi di dunia maya adalah tantangan yang terlampau besar untuk dihadapi sendiri oleh kepolisian. Dari wawancara lapangan BD mengungkapkan bahwa kini mekanisme penggalian data yang dilakukan oleh pemerintah (Depkominfo dan Kepolisian) dalam melacak jejak dan menggali rekaman digital tindak kejahatan di dunia maya, secara terus-menerus diamati metode yang diterapkan, dan kemudian para calon yang potensial dalam melakukan tindak kejahatan pun bisa mengantisipasinya dengan cermat.

> "Kalau anak *underground* sekarang itu sudah cerdas, cerdas dalam arti sudah tahu prosedur dari atas (Depkominfo). Istilahnya kalau mau *ngetrace* atau mau apa? Mencari berkas. Dalam arti yang mau dicari itu, rata-rata sudah tahu jalurnya, alurnya bagaimana. Dari segi

[327] http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf. Merupakan laporan tahunan (2010) atas berbagai laporan kejahatan cyber yang didapatkan oleh IC3.

[328] Wawancara dengan Onno W. Purbo, 20 Mei 2011.

> permintaan *pengen ngetrace* apa? ataupun suruh *njebol* apa? itu mungkin sudah tau langkah-langkahnya."[329]

Dalam wawancara dengan BD dan PZ, mereka banyak mengingatkan tentang pentingnya penegak hukum yang khusus menangani masalah cybercrime untuk selalu mengikuti perkembangan masalah dan teknik pemecahannya di dunia maya, demi menjaga agar kemampuan penegak hukum tidak tertinggal jauh dari para *cybercriminal*.

### 4.1.2 Partisipasi Publik (Masyarakat)

> "Publik harus belajar *dan* mengikuti perkembangan teknologi. Setiap hari muncul pengetahuan baru serta kemungkinan untuk disalahgunakan. Menggunakan internet itu persoalan teknis. Seseorang mengisikan *form* (formulir) atau mencobakan artikel *"proof of concept"* itu persoalan metode (cara), tetapi, apa yang dia isikan di form ataupun web siapa yang sedang dia coba, akan menjadi bermasalah jika sudah melanggar hukum. *Wireless* yang tadinya menggunakan udara milik bersama, akan menjadi bermasalah jika sudah ada dominasi *bandwith*. Maka masyarakat harus mengikuti perkembangan itu, karena ada kemungkinan kasus dan penyelesaian tindak kejahatan akan dipengaruhi perkembangan teknologi berikutnya. Misalnya, jika kelak internet sudah digunakan di setiap ponsel."[330]

Peran serta publik dalam menanggapi berbagai permasalahan hukum dalam ruang maya selalu muncul, terutama dalam bentuk tanggapan dan sumbang-saran di berbagai jejaring sosial, seperti twitter dan facebook. Sebagaimana disampaikan Onno W. Purbo, bahwa perhatian masyarakat terhadap permasalahan hukum (terutama *cybercrime*) baik yang disampaikan melalui facebook maupun di twitter sudah cukup banyak. Akan tetapi perhatian dari pemerintah dalam menampung aspirasi masyarakat tidak direspon positif. Onno W. Purbo mencontohkan twitter milik Tifatul Sembiring (@tifsembiring) yang sering mendapat kritik dan saran dari para pengguna twitter maupun di media, yang tak kurang juga

[329] Wawancara dengan BD, 11 April 2011.
[330] Wawancara dengan DM, 9 April 2011.

masyarakat berusaha memberikan aspirasinya sebagai publik mayantara melalui twitter tersebut, dan sangat minim respon.[331]

Kurang terserapnya aspirasi publik mayantara dirasakan PZ juga dalam penyusunan UU ITE, yang berpotensi berkurangnya perhatian terhadap undang-undang tersebut,

> "Terbukti, masih banyak *hacker* yang tidak terlalu peduli dengan UU ITE tersebut. Contoh jelasnya saya yang belum menyentuh UU ITE tersebut, padahal perhatian mereka sangat diperlukan demi kenyamanan dunia maya ya? Harusnya. Mungkin satu lagi mas yang menjadi masalah. Saat pihak yang berwajib mensahkan UU ITE tersebut, tidak ada kalangan dari "*hacker*" yang ikut terlibat. Jadi, mungkin gimana mereka mau peduli. seperti pensahan peraturan sepihak."[332]

KYF juga mendukung perlunya melibatkan para aktifis *cyber* dalam pembuatan UU yang berhubungan dengan *cybercrime*,

> "Kontribusi yang dapat diberikan agar penegakan hukum dapat lebih responsif adalah ajakan untuk merangkul teman-teman cyber agar lebih peduli dengan permasalahan cybercrime, tapi sebelum sampai ke langkah itu maka perlu kepedulian dari para pembuat UU melibatkan mereka dalam pembuatan UU yang berhubungan dengan cybercrime."[333]

Di dalam jejaring sosial lokal Kaskus.us, aktifitas 3 juta anggota terdaftar (*members* terdaftar pada hingga Juni 2011) di dalamnya terdapat juga berbagai pembahasan dan informasi sebagai pendidikan bagi publik secara luas didiskusikan. Dalam komunikasi semacam forum terbuka Kaskus inilah peran masyarakat secara luas dapat disarikan, diambil sebagai contoh untuk diterapkan oleh pemerintah. Saat setiap informasi bisa didapatkan dan dipahami sebaik mungkin oleh masyarakat, dan dalam posisi yang sejajar masyarat dapat memperhatikan arus diskusinya. Kaskus hanyalah salah satu contoh yang dapat diambil bagaimana partisipasi publik dalam mendiskusikan suatu masalah dapat berjalan terbuka dan demokratis.

---

[331] Disarikan dari wawancara dengan Onno W. Purbo, 20 Mei 2011
[332] Wawancara dengan PZ, 19 April 2011.
[333] Wawancara dengan KYF, 16 April 2011.

Dalam bidang *cybersecurity*, peran para peretas tidak hanya dalam posisi yang patut selalu diawasi, akan tetapi mereka juga secara berkelanjutan mempublikasikan berbagai kelemahan sistem terbaru yang belum diketahui oleh para penyedia layanan *Operating System, Web hosting, Content Management System* situs, atau pun sistem-sistem lain yang terhubung dengan interaktifitas dunia maya.

> "Kebanyakan untuk mengumpulkan paretas-paretasnya, dan segala macam *exploit*. Kalau exploit-id merujuknya ke exploit-db. Karena *defacer* Indonesia itu untuk mencari *bug* bisa. Seorang *defacer* bisa *deface* kan dari kaya gitu. Dan bisa digunakan, istilahnya itu untuk CMS yang berbau kenektor. Para *carder* mencari ID. Tapi kalau tidak di-*submit* dilema juga, (yang mengetahui *bug* itu hanya orang itu). Kan untuk penyedia CMS sendiri kan nggak tau kalau itu ada *bug*-nya, lama-lama (kalau dibiarkan korbannya) makin banyak. Kalau ada CMS di-*update* itu ya gitu, yang buat CMS langsung keluarin versi *update*-nya, *fix bug* apa, yang harusnya menambali."[334]

BD memberikan contoh situs 'exploit-db.com',[335] situs tersebut adalah sebuah situs yang menyediakan ruang bagi para aktifis *hacking* yang menemukan kelemahan-kelemahan atau lubang-lubang (*bugs*) di dalam berbagai *management system* yang terhubung dengan interaktifitas *cyber*. Dan dari *post-report* yang terdapat pada situs tersebutlah—post-report tersebut terbuka untuk umum, para produsen *management system* atau *vendors* (peritail) layanan tersebut kemudian membuat *patch* (tambalan) bagi kelemahan sistem, yang oleh mereka kemudian *patches* tersebut dipublikasikan dengan tujuan untuk *bug-fixing* (pembetulan celah sistem), untuk diterapkan kepada *management/ operating system* yang mereka produksi.

Dalam diskusi dengan BD maupun PZ, mereka menyatakan bahwa kelemahan-kelemahan yang selalu muncul inilah yang selalu dimanfaatkan

[334] Wawancara dengan BD, 11 April 2011.

[335] Di Indonesia sendiri juga terdapat situs exploit semacam exploit-db.com, yaitu exploit-id.com, yang memiliki fungsi yang serupa, akan tetapi tidak populer. Karena para *submitter* lokal tentu lebih memilih untuk *submit bug* yang mereka temukan dalam situs yang bertaraf internasional daripada lokal, demi publikasi luas, dan terkadang demi gengsi.

oleh para peretas (*hacker*), dan akan menjadi sebuah bencana jika para *hacker* itu tidak memposting bugs yang mereka temukan, dan menyimpannya untuk kepentingan sendiri, pastilah menjadi ancaman bagi setiap pengguna di seluruh dunia yang memiliki/ memakai *management/ operating system* yang telah mereka ketahui *bug*-nya tetapi tidak mereka publikasikan.

Pada kenyataannya, para produsen *operating system* seperti Microsoft juga tergantung pada para *hacker* di seluruh dunia. Microsoft sendiri tidak melepas produknya dalam kondisi sempurna, saat dirilis mereka membiarkan publik atau karyawannya menemukan dan kemudian mempublikasikan *bugs* yang ditemukan dalam *system* yang mereka kembangkan.

BD dan PZ sepakat bahwa, semestinya pihak aparat penegak hukum yang memiliki spesialisasi dalam bidang *cybercrime*, senantiasa melakukan *update* pengetahuan secara berkelanjutan dan konsisten. Karena jika tidak, pastilah akan tertinggal jauh oleh para pelaku kejahatan *cyber* yang terus-menerus meneliti secara luas berbagai kelemahan di ruang mayantara yang bisa mereka manfaatkan untuk dilakukan kejahatan. Kenyataannya perkembangan jumlah bugs tersebut menurut BD selalu bertambah perharinya, bahkan PZ menyatakan penambahan bug yang ditemukan bisa ada tiap kurang dari satu hari, mungkin dalam hitungan jam.

Exploit-db.com bisa dikatakan sebuah situs yang diciptakan oleh para *hacker* untuk masyarakat luas yang mencari solusi keamanan berupa informasi *bugs*. Tetapi bermasalah juga jika bugs yang diketemukan dalam suatu *Operating system* tertentu, tetapi tidak segera diciptakan tambalannya oleh produsennya. Di sinilah para pakar security system kemudian menjadi rujukan, dan tak jarang menciptakan *patch* (tambalan) sendiri yang juga dipublikasikan untuk masyarakat yang membutuhkan.

Dalam situs yang diciptakan oleh para *hacker* tersebut juga dapat diunduh secara gratis *operating system* untuk keamanan sistem dengan

basis *open source* Linux, yaitu 'Back Track', yang saat tulisan ini dibuat telah mencapai versi ke-5. Back Track dilengkapi dengan berbagai kebutuhan para *hacker* untuk melakukan uji keamanan sistem dan jaringan internet secara luas dan profesional. Sayangnya, tidak sedikit pula yang memanfaatkannya untuk kepentingan jahat, untuk mencari kelemahan sistem kemudian melakukan hacking terhadapnya. Maka kembali lagi, setiap orang yang memasuki dunia *hacking* baik atau buruknya tergantung pada niat tiap individu.

Komunitas *hacker* dan para *hacker*. Atau mereka yang masih belajar maupun yang mengambil manfaat komunitas untuk pengetahuan dengan cara dan tujuan beragam lainnya, memiliki peran yang patut diperhatikan dalam memberikan pemahaman publik,[336] terutama dalam keterkaitan eratnya dengan keamanan, keselamatan, dan penyelesaian masalah mereka di dalam hal-hal teknis *cyberspace*.

- Lingkup pelanggaran hukum di dunia maya cukup banyak subnya sehingga pengalamanpun kalau dilihat secara empiris bisa banyak, secara pribadi saya melihat banyak tindakan hacking secara ilegal tidak banyak ditindak karena berbagai faktor seperti karena UU khusus mengenai ini belum ada, pembuktian yang tidak mudah, dan sebagainya.
- Kalau tindakan *hacking* ilegal dari members ya ada tapi tindakan yang dilakukan oleh member adalah tanggung jawab pribadi, komunitas tidak bertanggung jawab atas tindakan para membersnya karena YF tidak dibatasi untuk kelompok-kelompok tertentu saja tapi semua orang dari

[336] Sekali lagi, pengertian publik di dalam ruang publik tetap berciri utilitarian, selama publik yang dimaksud berusaha mencari informasi pada komunitas (group atau forum) tentang masalah yang mereka hadapi yang berkaitan dengan cybercrime, maka publisitas dan publikasi yang disebarkan oleh komunitas-komunitas *hacker* tersebut tidak melulu mengarah pada para anggotanya saja. Maka selama pencari informasi secara spesifik mencari fungsi dari suatu informasi yang mudah ditemukan karena publisitasnya, demikianlah dapat didefinisikan bahwa wawasan yang ada di dalam komunitas senantiasa bersifat publik.

berbagai latar belakang dan sub kultur dapat menjadi members di komunitas hanya dengan mendaftarkan diri di Forum atau Milis.[337]

KYF hendak menjelaskan bahwa: *pertama*, dalam komunitas besar seperti Yogyafree (YF) dan keberagaman individu di dalamnya, serta kemudahan dalam cara mendaftar sebagai anggota komunitas menjadikan kontrol tidak bisa efektif terhadap tiap-tiap anggota, yang bisa jadi mengatasnamakan komunitas dalam melakukan tindak kejahatannya. *Kedua*, lebih awal KYF menyampaikan bahwa renggangnya sistem hukum yang ada secara tidak langsung justru memberikan ruang luas bagi para *cybercriminal* untuk melancarkan aksinya.

Pada beberapa komunitas yang muncul setelah masa-masa awal, muncul berbagai komunitas yang lebih kecil. Komunitas-komunitas tersebut bermula dari individu-individu dalam komunitas besar, yang kemudian secara bersamaan mendirikan komunitas baru dalam ruang lingkup yang lebih dipahami oleh individu-individu tersebut. Dan secara konsisten terus mengasah kemampuannya dan membina generasi yang ada di bawahnya untuk memperkuat pengetahuan mereka dan sekaligus membesarkan komunitas.

Dan dalam komunitas-komunitas yang lebih spesifik, baik secara geografis maupun kekhasan lainnya, keakraban satu sama lain akan membina pertemanan yang lebih kuat, dan berarti juga kontrol ke dalam yang lebih baik. BD menjelaskan untuk kemungkinan adanya tindak kejahatan yang dilakukan oleh seorang anggota suatu komunitas terhadap suatu situs, misalnya,

> "… salah satu tujuan dari adanya komunitas itu untuk saling *sharing*. Bagaimana saling melengkapi kalau ada website teman, atau

[337] Wawancara dengan KYF, 16 April 2011. KYF menjelaskan pendapatnya tentang keterkaitan antara kurangnya penanganan pidana terhadap cybercrime dengan pengalaman pribadi sebagai *hacker* maupun ia sebagai founder komunitas *hacker* Yogyafree.

> tetangga, atau teman kantor lagi ada masalah mungkin bisa minta bantuan. Ya, memberikan solusi terbaiklah."[338]
>
> "Untuk *defacement* kan biasanya laporan, ini webku domain ini, di-*hack* atas nama ini tolong siapa pelakunya. Karena anak-anak *underground* banyak yang kenal, tinggal tanya *sini-situ*, mungkin pasti dijawab, "O, ini anak *situ*.""[339]

Salah satu bentuk kontrol ke luar dari suatu komunitas bisa berupa pemberitahuan pelaku sebagai anggota komunitas tertentu. Namun, dengan keakraban pula komunitas melakukan perlindungan terhadap anggotanya. Dalam pengamatan, terkadang terjadi semacam 'pemanggilan' seorang pemimpin komunitas terhadap anggotanya yang melakukan kejahatan terhadap wilayah anggota komunitas lain.[340] 'Pemanggilan' ini untuk memberikan peringatan atau hukuman karena kesalahannya.[341] Pemberian hukuman dan peringatan tersebut merupakan upaya komunitas melakukan kontrol ke dalam.

Kaskus.us adalah komunitas dengan cakupan luas dan jumlah anggota yang besar, dengan fokus kajian yang beragam. Sedangkan di sisi lain, sebagaimana ditunjukkan dalam sejarah perkembangan komunitas *cyber* di Indonesia, terdapat beberapa komunitas yang fokus pada pembahasan keamanan dan berbagai bidang terkait dengan aktifitas di dunia maya. Dalam kelompok-kelompok *underground* yang terus meningkat jumlahnya dari tahun ke tahun, komunitas *hacker* juga terus mengalami peningkatan kuantitas dan kualitas. Bahkan berbagai ibu kota provinsi seperti Jakarta, Bandung, Surabaya, Yogyakarta, Semarang, Medan, dan Ibu Kota Provinsi lain kini memiliki komunitas-komunitas *hacker underground*-nya sendiri. Trend tersebut menjalar pula ke beberapa

---

[338] Wawancara dengan BD, 11 April 2011.

[339] *Ibid*.

[340] Wilayah, dalam hal ini diartikan ruang kerja yang berada dalam jangkauan pengawasan seorang *hacker*, terutama dalam pekerjaannya sebagai security, administrator atau perawat suatu situs atau server. *Hacker* memiliki pekerjaan yang bermacam-macam, tetapi dominasi ruang kerja mereka tetap tidak jauh dari tehnik informatika, dan internet.

[341] Jika diperhatikan kinerja sistem dalam komunitas *hacker* dalam uraian tersebut dan kontrol di dalamnya, serta korelasinya terhadap komunitas lain yang memiliki kedekatan emosional, seperti kinerja dan kontrol dalam organisasi mafia.

kota lain, seperti Malang, Magelang, dan sebagainya. Sebagian mengidentifikasikan sebagai *white-hat hacker community*, sebagian sebagai *black-hat*, dan ada pula *gray-hat*. Dalam komunitas tersebutlah ditemui banyak solusi dalam permasalahan *cybercrime* dan berbagai cara melakukannya pun bisa didapatkan. Semua ini kembali kepada diri masing-masing aktivis dunia maya, akan menggunakannnya untuk kebaikan ataukah untuk kejahatan.

Kritik merupakan peran massal dari masyarakat yang bisa datang dari siapa saja. Dan terdapat pula kritik yang diletakkan di berbagai situs yang telah di-*hack* oleh seorang *hacker* atau *defacer*, yang berkaitan dengan kelemahan sistem atau keteledoran pihak penyelenggaran layanan transaksi yang melibatkan hak kepemilikan orang banyak, sebagaimana dalam contoh kasus klikbca.com, yang kemudian bisa membantu membenahi kelemahan sistem yang juga mencegah potensi tindak kriminalitas terjadi terhadap sistem tersebut.

Dan peran yang diberikan oleh forum-forum serta komunitas-komunitas *hacker underground* lebih spesifik pada seputar keahlian teknologi *cyber*. Forum atau komunitas yang semakin dewasa memiliki kecenderungan untuk lebih banyak berbagi (*share*) ilmu kepada siapa saja untuk kebaikan setiap mereka yang mau belajar, dan kedewasaan cara berpikir menumbuhkan cara berpikir yang terus berkembang. Sebagaimana dalam penelitian tentang perkembangan psikologis *viruswriter*, para *ex-viruswriter* lebih memiliki empati terhadap orang lain, dan bagaimana memandang bahwa orang lain adalah juga bagian dari dirinya. Pada usia dan pemikiran yang semakin dewasa penghargaan dan apresiasi ‘yang lain’ dalam ruang publik mayantara cenderung memiliki peningkatan.

### 4.1.3 Optimisme Penegakan Supremasi Hukum dalam Mayantara

Pandangan positif terhadap optimisme penegakan hukum yang responsif terhadap keadaan di dunia maya dari para *cyberactivists*

merupakan dukungan atas supremasi hukum itu sendiri. Dan dukungan berupa sikap yang telah terbangun dari para agen sosial yang memiliki kemampuan transformatif ini merupakan dukungan mental bagi penegakan hukum di dunia maya. Dalam interview terlihat bahwa demikian banyak dukungan yang bisa diberikan oleh para *cyberactivists*. Dari optimisme dukungan sosialisasi/penyuluhan hukum,[342] hingga dukungan dalam proses penegakan hukum.

DM lebih optimis dengan melihat pentingnya kerjasama penegakan hukum antara aktivis *cyber* dengan penegak hukum pada keuntungan ekonomisnya,

a. Negara Indonesia tidak diblokir dari transaksi ekonomi di dunia maya.
b. Para *hacker* bisa menjadi *security professional* berkelas dunia. Banyak *hacker* Indonesia dengan kemampuan berkelas dunia.
c. Masyarakat juga bisa berperan dalam kebijakan negara agar anggaran yang dijalankan negara, bisa lebih efisien dan murah. Bayangkan seandainya Indonesia bisa lepas dari hantu pembajakan *software*.[343]

Keberadaan agen-agen sosial yang berada dalam wilayah mereka masing-masing, dan kemungkinan dalam mengenali personal satu sama lain merupakan bentuk organisasi masyarakat di dalam ruang *cyber*. Komunikasi antara para penegak hukum, atau negara dalam mengalirkan kebijakannya tentang *cyberspace*, akan memiliki jalan yang lebih baik selama ada pendekatan-pendekatan khusus kepada tiap komunitas. Di sisi lain sensitifitas dan solidaritas komunitas dengan karakter subkultur dan *underground* patut dipertimbangkan, supaya tidak menimbulkan kesan penerapan hukum yang represif. Karena kuatnya ikatan emosional antar personal—meskipun tidak dalam satu komunitas—dalam dunia

[342] Berinternet sehat dan berbagai pendidikan berinternet yang aman merupakan muatan-muatan yang rata-rata dibagikan dalam komunitas *cyber*, juga dalam komunitas *hacker underground*. Bagi para anggotanya, yang terbuka untuk siapa saja yang ingin bergabung dan membutuhkan berbagai kajian dalam komunitas-komunitas tersebut.

[343] Disarikan dari wawancara dengan DM, 9 April 2011.

*underground* cukup mampu untuk menggerakkan mereka secara bersama-sama melakukan penentangan, atau dukungan.[344]

Karakter solidaritas yang baik merupakan pengikat terbaik dalam suatu masyarakat, dan dalam masyarakatnya penghargaan kepada pemilik kebijaksaan terbaik dengan keahlian baik selalu menjadi prioritas, disamping penghargaan terhadap para pemimpin tiap komunitas. Melihat karakter yang demikian dapat menjadi pertimbangan dalam menangani permasalahan *cybersociety*. Bertautan dengan itu KYF memberikan jawaban tentang bentuk kerjasama yang mungkin dilakukan oleh penegak hukum dengan masyarakat mayantara:

- Aparat penegak hukum perlu mempekerjakan para *hacker*
- Aparat penegak hukum perlu menggandeng komunitas-komunitas internet, tidak hanya komunitas *hacker*s untuk menciptakan kenyamanan masyarakat dalam menjelajah serta memanfaatkan peran internet.[345]

> "Contoh manfaatnya adalah berbagai permasalahan *cybercrime* dapat lebih banyak terpecahkan, untuk sosialisasi terhadap komunitas maka tidak hanya pakar *cyber* saja tapi kita juga perlu pakar sosial."[346]

XP mengurai optimisme atas beberapa hal yang bisa didapatkan dengan adanya kerjasama antara penegak hukum dengan para *cyberactivist* atau *hacker:*

- Terciptanya kerjasama yang baik antara penegak hukum dan masyarakat (Terutama Masyarakat IT).
- Mengurangi tingkat kejahatan *cyber*, karena otomatis para *cyberactivist* maupun *hackers* tidak menyalahgunakan ilmu yang mereka miliki.
- Penyelidikan kasus dan sosialisasi lebih cepat jika para *cyberactivist* maupun *hackers* diikutsertakan sehingga informasi lebih akurat.[347]

---

[344] Disarikan dari pendapat BD dalam wawancara pada 11 April 2011.
[345] KYF, 16 April 2011.
[346] Wawancara dengan KYF, 16 April 2011.

Pemahaman dan pengenalan satu sama lain perlu ditingkatkan untuk kerjasama yang baik, terutama dalam penegakan hukum pidana mayantara, karena tanpa adanya pemahaman satu sama lain yang terbuka dan dengan cara pandang yang tidak merendahkan atau mencurigai yang hanya bisa didapat dengan komunikasi yang baik, niscaya akan tercipta kerjasama yang bermanfaat bagi seluruh masyarakat. Dan keadaan yang belum saling memahami antara penegak hukum dengan para *hacker* disindir dengan ungkapan dan pertanyaan oleh Onno W. Purbo,

> "Kerjasama yang baik hanya akan terbentuk kalau dua belah fihak saling mengenal dengan baik dan saling percaya satu sama lain. Pertanyaanya. Apakah keduanya saling kenal? apakah keduanya saling percaya?"[348]

Yang terpenting untuk mengawali kerjasama yang baik dan demi terciptanya ruang publik mayantara Indonesia yang lebih aman dan nyaman bagi tumbuh kembangnya pengetahuan dan masa depan bangsa, adalah saling memahami satu sama lain. Ruang-ruang demokratisasi untuk kebebasan berpendapat dan mengkritik kekurangan yang ada demi membangun sistem yang lebih baik, perlu dibuka dan dijamin bagi setiap individu.

## 4.2 Kendala Penegakan Hukum Pidana Mayantara Indonesia

Satu fakta bahwa sebagian besar sumber hukum yang digunakan untuk menerjemahkan konsep *cybercrime* ini berasal dari luar negeri dengan sistem yang berbeda. Konsekuensi logis berikutnya tentunya adalah menuntut kita untuk melakukan perbandingan dengan negara-negara lain yang sudah berpengalaman dalam membuat kebijakan dan hukum untuk *cybercrime*. Kesadaran mengenai hal-hal tersebut memerlukan ketelitian dalam mengidentifikasi permasalahan

[347] XP, 27 April 2011.
[348] Onno W. Purbo, 20 Mei 2011.

untuk menentukan arah kebijakan dari *cybercrime* sesuai dengan kebutuhan sosial, budaya, dan kebiasaan yang berlaku di Indonesia.[349]

Penegakan hukum memerlukan pemahaman karakter sosial dengan baik sehingga dapat dijalankan dengan lebih terarah, terlebih hukum pidana adalah hukum yang berbenturan langsung dengan masyarakat. Setiap kebijakan yang diambil oleh pemerintah berkaitan dengan hukum pidana akan bersinggungan dengan hak-hak dasar manusia, dalam mendefinisikan pidana dan dalam menentukan porsi pemidanaan.

Dalam *cybercrime*, pengertian *crime* secara spesifik mengikuti pengertian kajian pidana yang meliputi pelanggaran dan kejahatan. Secara definitif dalam peristilahan, crime di dalam Black Law Dictionary adalah:

> *"Understanding that the conception of Crime, as distinguished from that of Wrong or Tort and from that of Sin, involves the idea of injury to the State of collective community, we first find that the commonwealth, in literal conformity with the conception, itself interposed directly, and by isolated acts, to avenge itself on the author of the evil which it had suffered."*[350]

*Crime* untuk membedakannya dengan peristilahan kesalahan dan dari pengertian dosa, *crime* melibatkan ide tentang pencederaan kepada Negara, negara diasumsikan sebagai komunitas kolektif. Maka pencederaan terhadap publik juga merupakan pencederaan terhadap otoritas publik. Sebagaimana dalam *cybercrime* adalah bagaimana pencederaan kepada publik mayantara. Yang semestinya benar-benar dapat dilihat sebagai pencederaan, dan pemerintahlah yang mengambilalih peran untuk penyelesaiannya untuk memulihkan keadaan.

Kajian terhadap tindak pidana mayantara mengharapkan pendekatan kepada ruang publik maya yang lebih intensif, hukum tak selamanya bergantung pada nilai-nilai ajeg, akan tetapi nilai-nilai dalam masyarakat juga akan berkembang seiring perubahan ruang sosial tersebut. Jika *cyberlaw* dalam

---

[349] Rapin Mudiardjo, "Kajian Aspek Pidana", dalam Edmon Makarim, Pengantar Hukum Telematika: Suatu Kajian Kompilasi, Rajagrafindo Persada: Jakarta, 2005, hal. 419.

[350] Bryan A. Garner (editor in chief), Black's Law Dictionary, 9th edition, Thomson Reuters: MN, 2009, hal. 427. Ini merupakan kutipan dari karya Henry S. Maine, Ancient Law, hal. 320 (17th ed. 1901), yang dikutip untuk membantu menjelaskan pengertian '*crime*'.

*cyberspace* dibayangkan sebagai bentuk perkembangan yang dipengaruhi modernitas, maka modernitas konvensional mesti dibedakan dengan bagaimana cara-cara tradisional dirubah dalam cara-cara digital. Dengan kata lain modernitas yang senantiasa diterjemahkan dengan kemajuan ekonomi, dalam *cyberspace* modernitas mengalami peningkatan lebih lanjut.

Dari pendapat para *cyberactivists* yang memiliki peran dominan dalam ruang publik mayantara, setidaknya dalam komunitas masing-masing, yang terungkap dalam pembahasan bab sebelumnya, dapat dirasakan masih minimnya legitimasi hukum di dalam mayantara. Mereka sebagian besar menilai belum efektif, sedangkan sebagian kecil menyampaikan opini adanya beberapa . Permasalahan mengenai minimnya kemampuan aparat penegak hukum dalam menangani berbagai kasus terkait *cybercrime* lebih mengemuka, dikarenakan besarnya ketergantungan masyarakat dan berbagai peraturan terhadap kemampuan dari para penegak hukum, terutama terhadap hal-hal yang secara teknis bukan sebagai keterampilan yang dimiliki setiap orang, melainkan teknis yang bersifat khusus. Kepada para penegak hukumlah wibawa hukum senantiasa diemban dan dicitrakan, dan masyarakat akan ragu untuk menjalankan proses hukum jika justru dengan melalui proses tersebut akan memperlambat penyelesaian masalah yang mereka harapkan.

Untuk memberikan solusi kepada hukum pidana mayantara yang *legitimate* dalam dinamika kehidupan sosial masyarakat mayantara, maka kita memerlukan analisis tentang bagaimana krisis legitimasi *cyberlaw* itu menjadi mungkin. Dengan perbekalan uraian data dalam pembahasan sebelumnya sebagai bahan uraian fakta sosiologis, perlu diupayakan jalan keluar dari setiap kesulitan sosiologis, sehingga peran hukum sebagai *social control* dan *social engineering* dapat menemukan tumpuannya. Dan tumpuan sosiologis merupakan basis hukum pidana yang kuat.

Atas pertanyaan: *"Apakah alat-alat penegakan hukum milik negara yang ada selama ini bisa menjalankan peranan-peranan hukumnya di dunia maya?"* didapatkan jawaban kurang positif, dan untuk keberlanjutannya jika

mempertahankan kemampuan yang sekarang dimiliki, tentu akan ada sikap pesimistis. Pada kenyataannya aparat penegak hukum dan undang-undang yang mereka jalankan tidak dapat selamanya berjalan sendiri, penegakan hukum selalu butuh peran publik.

Pada penelitian dan upaya mengumpulkan data di lapangan, maka akan diuraikan beberapa bagian kendala pokok dalam upaya penegakan hukum pidana mayantara, yaitu: perkembangan kriminalitas di mayantara, kurangnya kemampuan dalam menangani kejahatan mayantara, belum adanya undang-undang khusus *cybercrime.*

### 4.2.1 Perkembangan Kriminalitas di Mayantara

Dari uraian studi lapangan terhadap komunitas *hacker* secara khusus dan fenomena perubahan konsep kejahatan dari dunia nyata ke dalam dunia maya, dapat dipahami bagaimana perkembangan dalam ragam dan juga kuantitas tiap-tiap bagiannya. Alasan suatu kejahatan berkembang seringkali didukung oleh suasana dan kemungkinan yang terbentuk dari lingkungan sosialnya.

Perkembangan kriminalitas tidak lepas dari teori tentang tindakan kriminal itu sendiri. Karena dengan melihat dan memandang terpenuhinya konsep suatu teori kita dapat meyakini bahwa sesuatu adalah benar secara teoretis dari permulaan hingga alasan keberadaannya di dalam masyarakat.

Dalam *rational choice theory*, kejahatan adalah suatu peristiwa yang dalam faktanya ia dilakukan pada suatu tempat pada waktu tertentu. Keberadaan seorang pelaku kejahatan hanyalah salah satu dari beberapa komponen penting dalam terjadi suatu tindak kejahatan. Kejahatan memerlukan berbagai kondisi yang tidak melekat pada si pelaku kejahatan, seperti kemungkinan benda-benda yang bisa dicuri atau seseorang untuk diserang. Beberapa pakar berargumentasi bahwa jika kejahatan akan dicegah dan kebijakan untuk mengontrolnya disusun, kajian tentang tindak kejahatan harus mengamati dari dekat dengan cermat proses *decision-*

*making* dari pelaku kejahatan dan kepada tindakan-tindakan kriminalnya itu sendiri. "*Rational*" merujuk pada pemahaman, bahwa seorang pelaku kejahatan memproses informasi dan mengevaluasi berbagai kemungkinan. "*Choice,*" anjuran mereka dalam melakukan suatu keputusan bertindak.[351]

Para pelaku kejahatan di dalam ruang maya juga tidak selamanya ceroboh dalam bertindak. Mereka selalu mempertimbangkan cara bagaimana kemungkinan-kemungkinan yang akan mereka tanggung dari melakukan suatu tindak kejahatan. Adler mencontohkan pertimbangan pelaku kejahatan dalam tindak pidana pencurian, secara umum seorang calon pelaku akan mempertimbangkan hal-hal sebagai berikut: a) Jumlah sasaran dan keterjangkauannya; b) kemahirannya dalam metode yang ia gunakan; c) uang yang dihasilkan dari tiap tindak pencurian; d) keahlian yang diperlukan; e) waktu yang dibutuhkan dalam melakukan aksi pencurian; f) bahaya fisik yang ada di dalamnya; dan g) resiko penangkapan oleh yang berwajib.[352]

Contoh 'pilihan rasional' yang diberikan Adler cukup membantu dalam menguraikan pilihan rasional dalam suatu tindak pidana mayantara. Persoalan semakin meningkatnya statistik global kejahatan mayantara tidak sebanding dengan berbagai isu-isu populer di Indonesia yang diidentifikasi sebagai '*cybercrime*' oleh para penegak hukum dan media massa. Negara maju seperti Amerika Serikat yang sudah memiliki sistem informasi dan pelaporan yang cukup baik, serta pelatihan penanganan *cybercrime* yang baik, masih jauh dari kemungkinan untuk dapat menangani, terlebih menyelesaikan, semua tindak kriminal mayantara di wilayahnya.

Dengan mempertimbangkan ketujuh pokok dari contoh yang disampaikan Adler di atas, pertimbangan seorang *cybercriminal* tidak jauh berbeda:

---

[351] Freda Adler, et. al, *Criminology*, (New York: McGraw-Hill, 1991), hal. 203-204.
[352] Lihat, Adler, ibid, hal. 204

- Jumlah sasaran tindak *cybercrime* dan kemampuan mengaksesnya. Hal pertama, semakin hari semakin tinggi dengan semakin banyaknya aktifitas masyarakat di ruang maya. Dan kemungkinan seorang pelaku tindak kriminal mengaksesnya dengan maksud jahat semakin terbuka. Kemungkinan juga diperbesar dengan tingginya informasi sebagai sarana pembelajaran dalam melakukan tindak kejahatan;
- Keakrabannya (dalam memanfaatkan tehnik) dengan metode yang dia gunakan. Semakin luas wawasan seseorang dan semakin mahir dalam tehnik-tehnik yang potensial dalam *cybercrime*, maka akan semakin familiar dalam menerapkan metodenya;
- Uang yang dihasilkan dalam setiap tindak *cybercrime* merupakan pendorong potensial. Tapi tidak semua pelaku *cybercrime* didorong unsur material, bagi mereka yang ingin 'unjuk gigi,' popularitas lebih menjadi dorongan utama. Hal inilah yang seringkali diidentifikasikan sebagai bentuk umum dari gambaran *cybercriminal*, yang melekatkan lebih pada permasalahan psiko-patologi semata yang lepas dari alasan materialistik. Tetapi saat tidak bisa mengendalikannya, justru menjadi *addicted* (kecanduan);
- Keahlian yang diperlukan. Dalam *cybercrime*, keutamaan pelaku yang memiliki potensi keberhasilan yang lebih baik adalah mereka yang belajar dan terus mengasahnya dengan mempraktikkan, dalam kondisi yang memungkinkan untuk melancarkan serangan. Maka dimungkinkan dari berbagai dorongan untuk mendalami suatu tehnik dari berbagai tehnik *hacking*, salah satunya adalah keinginan bertindak jahat;
- Waktu yang diperlukan untuk melakukan suatu tindak kriminalitas. Dalam *cyberspace* bisa menjadi ruang yang sangat memungkinkan untuk melakukan serangan kapan saja dan di mana saja. Bahkan dengan *remote attack*, waktu bisa diatur sedemikian rupa dengan mempengaruhi *routine* suatu *system*;

- Bahaya fisik yang terlibat (dimungkinkan) di dalamnya. Minimnya kemungkinan bahaya fisik seorang pelaku *cybercrime*, karena tidak memerlukan kehadiran fisiknya secara langsung kepada pihak yang dirugikan, maka kemungkinan serangan perlawanan fisik atau resiko lokasi yang berbahaya secara fisik pun jauh lebih minim;
- Resiko penangkapan. Dorongan terbesar bisa jadi adalah ini. Penanganan kejahatan mayantara tidak bisa maksimal selama penangkapan (*arrest* dan atau *detention*) masih sedikit dimungkinkan, dengan perbandingan *possible attack* dari kasus *cybercrime* yang ditangani para penegak hukum. Selain itu kemampuan untuk bersembunyi dan menyembunyikan identitas nyata sudah menjadi hal utama dalam melancarkan kejahatan *cyber*.[353]

Pertimbangan rasional yang menonjol jika kita melihat dalam penanganan hukum di Indonesia adalah kecilnya resiko penangkapan bagi mereka yang memiliki keahlian lebih baik dalam melaksanakan tindak *cybercrime*-nya, karena kurangnya kemampuan penegak hukum dalam melakukan penangkapan inilah memberikan semua kemungkinan yang ada sebelumnya menjadi lebih menjanjikan untuk berhasil dalam melaksanakan aksi-aksinya.

Perkembangan kriminalitas tidak hanya karena faktor penegak hukum, akan tetapi dalam masyarakat juga, sebagaimana dalam lingkungan sosial nyata, terdapat bentuk-bentuk kontrol sosial yang membatasi potensi kejahatan dan mempersempit ruang kemungkinannya dengan menanamkan berbagai etika. Perkembangan tingkat dan ragam kriminalitas akan semakin berkembang seiring dengan perkembangan teknologi yang diusung modernitas.

---

[353] Uraian ini merupakan adaptasi dari penjelasan Adler sebelumnya, untuk mendekatkan pada realitas alasan tajamnya peningkatan angka kejahatan mayantara, dengan pertimbangan-pertimbangan yang dicontohkan Adler yang memang relevan dengan logika para *cybercriminals*. Lihat, Adler, *ibid*, hal. 204.

Seperti dijelaskan oleh PZ dan BD, bahwa ketika ada anggota baru masuk ke dalam komunitas mereka bebas untuk belajar hal-hal yang mereka sukai melalui forum diskusi dan media berbagi yang ada dalam komunitas. Maka saat mereka telah mampu melakukan *hacking* dan layak disebut *hacker*, sikap mereka selanjutnya tergantung dari pribadi masing-masing. Tetapi sebagai pemimpin komunitas mereka akan menerima sanksi atas pelanggaran etika bersama. Etika lebih cenderung ditentukan oleh komunitas, walaupun tidak sepenuhnya lepas dari *hacker ethics* yang dipopulerkan oleh para *hacker* legendaris.

Dari berbagai data statistik global tentang aneka ragam kriminalitas di dalam *cyberspace* yang cenderung meningkat, baik yang dilakukan oleh para peretas luar negeri maupun peretas dalam negeri, bukan tidak mungkin bahwa permasalahan riil yang dihadapi publik mayantara Indonesia adalah sama kadarnya. Hanya saja sistem pelaporan yang kurang akurat justru tidak menjamin tiap laporan dapat diproses dengan baik dan memunculkan kecenderungan publik kurang percaya, sekaligus pihak kepolisian tidak memiliki laporan serta sistem administrasi yang baik untuk memberikan statistik laporan dan kasus yang diselesaikan, atau setidaknya *referral* ke tahap selanjutnya setalah laporan dianggap cukup memadai.

Selain uraian tentang *rational choice* tersebut, dalam komunitas seseorang melengkapi dirinya selama berinteraksi satu sama lain dengan berbagai nilai yang ada dalam komunitas. Di dalam komunitas pulalah mereka belajar dan membentuk kemampuan (*skill*) menjadi seorang *hacker*, berbagai pelajaran teknis mereka dapatkan secara cuma-cuma.

Sebagaimana telah diuraikan dalam alur pemurnian pengetahuan oleh Onno W. Purbo, di dalam komunitas IT ataupun *hacker* berjalan juga mekanisme serupa. Pengetahuan yang didapatkan dari luar komunitas dibawa masuk ke dalam komunitas dengan cara berbagi dalam forum. Dalam forum diskusi terbuka dalam komunitas inilah pengembangan ilmu pengetahuan dilakukan. Walaupun pembelajaran juga pada akhirnya

kembali kepada pribadi masing-masing dalam menggunakan ilmunya, akan tetapi setiap seorang pelaku kejahatan mayantara adalah hasil dari proses pembelajaran dari dan oleh lingkungannya. Dan lingkungan ini adalah website dan segala modifikasinya, sebagai komuitas.

Maka perkembangan kriminalitas memiliki konsep yang sama dengan pemurnian pengetahuan dalam *cyberspace*. Bagaimana kejahatan mayantara itu dapat terus berkembang dengan cepatnya, adalah karena pelaku juga terus belajar dengan mengamati setiap perkembangan pengetahuan di dalamnya dan alur pemurnian yang ada bersamanya. Lalu mempraktikkannya sebagai bentuk pengujian ilmu yang didapatkan, dan lebih jauh digunakan untuk kejahatan.

### 4.2.2 Kurangnya Kemampuan Penegak Hukum dalam Menangani Kejahatan Mayantara

Pertimbangan ini adalah isu yang paling populer di kalangan para penggiat *cyberspace* Indonesia. Sementara itu masih belum terdata dengan baik berapa situs internet yang mengalami serangan dari tindakan *cybercrime*, yang dikarenakan juga masih minimnya perangkat sistem informasi yang dimiliki oleh pihak kepolisian sendiri.

Dari berbagai kemungkinan bentuk serangan cybercrime yang bisa jadi dialami oleh para individu di dalam cyberspace, khususnya Indonesia, salah satunya adalah *defacement attack*. Dengan melakukan pencarian pada basis data situs populer yang mendata hasil defacement para defacer, Zone-H.org, terhadap berbagai nama domain yang dikelola oleh Pandi (Pengelola Nama Domain Internet Indonesia, http://www.pandi.or.id), berikut adalah hasilnya:

| **Nama Domain** | ***Total defacement*** | ***Single* IP *def.*** | ***Mass defacement*** |
|---|---|---|---|
| .co.id | 2.792 | 629 | 2.163 |
| .go.id | 4.282 | 1.454 | 2.828 |
| .ac.id | 2.039 | 654 | 1.385 |

| | | | |
|---|---|---|---|
| .net.id | 92 | 36 | 56 |
| .mil.id | 59 | 34 | 25 |
| .sch.id | 1.090 | 181 | 909 |
| .web.id | 1.454 | 244 | 1.210 |
| .or.id | 1.223 | 387 | 836 |

*Tabel 4.3. Defacement* pada nama domain '.id'. (Zone-H.org)[354]

Daftar yang dihasilkan adalah total keseluruhan hasil defacement yang didaftarkan pada situs Zone-H saja, akan tetapi tidak semua hasil *defacement* maupun hasil peretasan selalu diunggah pada situs ini. Dalam hal ini Pandi bukanlah pihak yang bertanggungjawab atas lemahnya sistem keamanan, Pandi hanyalah pihak yang mengelola pendaftaran nama domain yang menggunakan akhiran '.id'. 'ID' adalah nama domain yang ada 'di dalam' Indonesia, sebagaimana 'ID' adalah kode untuk negara Indonesia yang digunakan secara internasional dalam pengidentifikasian suatu negara, Indonesia.

Sebagaimana yang disinggung oleh BD, bahwa pendaftaran nama domain yang dikelola PANDI ini cenderung dapat dicurangi, misalkan dengan mencuri kartu identitas (contohnya, KTP) yang data (hasil *scan*-nya) bisa didapat dari internet secara liar saja bisa disahkan.[355] Hal ini menunjukkan lemahnya jaminan keselamatan bagi siapa saja yang mengakses situs dengan nama domain yang dicurangi tersebut.[356] Dengan semakin besarnya jumlah situs dengan nama domain yang membutuhkan pendaftaran resmi yang liar, maka akan semakin besar pula kemungkinan data publik yang bisa dimanipulasi.

Sebagaimana dicontohkan dengan kasus *phising*, yang memanfaatkan keteledoran korban untuk memasukkan data pribadi yang sangat penting,

[354] http://Zone-H.org, diakses pada 22 Juni 2011, pukul 03.00 WIB.

[355] Hal ini lebih terkait dengan tidak terdatanya dengan baik identitas penduduk dalam sistem KTP yang ada di Indonesia secara umum.

[356] Registrasi nama domain dengan menggunakan kartu identitas maupun surat berharga lainnya, biasanya adalah untuk pendaftaran nama domain yang berkaitan erat dengan keorganisasian, dan domain yang dikelola atau milik suatu lembaga/organisasi cenderung memiliki pengakses yang besar.

terdapat statistik yang menunjukkan bahwa ada banyak situs yang memang ditujukan untuk mencuri identitas yang tanpa sadar dimasukkan ke dalam sistem situs yang telah dicurangi tersebut. Hal ini memperlihatkan bahwa kelemahan sistem basis data kependudukan juga berpengaruh pada keamanan di dunia maya.

*Phising* adalah satu contoh dari pemanfaatan kelemahan sistem administrasi yang ada, lebih jauh lagi banyaknya serangan terhadap nama domain khas Indonesia tersebut juga merupakan tanggungjawab para penyedia layanan *hosting* basis data situs yang ada, terutama di Indonesia, terhadap layanan penyimpanan datanya yang bisa jadi tidak memperhatikan atau memiliki kelemahan dari segi keamanan data.

Data pada tabel di atas bukanlah gambaran menyeluruh terhadap *defacement* di Indonesia. Selain tidak semua hasil *defacement* diunggah ke dalam situs tersebut, tidak semua situs yang ada di Indonesia menggunakan nama domain khas Indonesia, terdapat jauh lebih banyak presentase situs dengan nama .com, .org, .info, dan lain sebagainya, yang juga tidak menggunakan nama domain khas Indonesia. Dan pelacakan terhadap data situs yang telah terserang di dalam wilayah hukum Indonesia tetapi tidak terlaporkan di luar nama domain '.id' membutuhkan keterampilan yang lebih baik. Terlebih lagi, *defacement* hanyalah salah satu bentuk kejahatan *cyber,* masih terdapat berbagai bentuk serangan lainnya sebagaimana telah dibahas sebelumnya. Defacement diambil sebagai contoh besarnya kasus yang terjadi akan tetapi sebagian besar tidak terpulihkan keadaannya.

Tetapi Kepolisian RI tidaklah tinggal diam, terdapat beberapa kasus perusakan situs milik pemerintah yang masih terus diproses secara hukum, akan tetapi persentasenya (kemungkinan besar, mengingat hasilnya tidak dipublikasikan di situs terkait) jauh dari keseluruhan jumlah korban tindak kejahatan. Para narasumber dalam penelitian ini berpendapat bahwa penanganan *cybercrime* masih minim, dan Onno W. Purbo menjelaskan bahwa ada,

> "Segelintir penegak hukum seperti Pak Petrus Golose dan kawan-kawan dari unit *cybercrime*, bisa dan punya kemampuan penegakan hukum di dunia *cyber*, tapi sebagian besar *sih nggak.*"[357]

Oleh karenanya yang tersiar dan terpublikasikan di berbagai media adalah penyelesaian berbagai kasus *cybercrime* yang jumlahnya masih segelintir dari gunungan kasus lain yang tidak terungkap karena tidak terlaporkan.

Pelatihan yang dilakukan secara berkelanjutan oleh kepolisian maupun kejaksaan untuk membekali jajarannya dengan wawasan *cybercrime* masih perlu terus dipacu dengan sangat maksimal. Perkembangan jumlah pelaku *cybercrime* yang potensial, dari waktu ke waktu terus bertambah, demikian pula potensi yang diakibatkan tentu akan semakin meluas. Jumlah *potential cybercriminals* jauh lebih banyak dan tidak sebanding dengan jumlah penegak hukum yang mampu menangani kasus-kasus *cybercrime* dengan baik.

Pada keadaan yang demikian tragisnya dalam *cyberspace* kita, potensi kejahatan yang terus meningkat, pelayanan pelaporan tindak kejahatan mayantara yang minim, dan tidak adanya data yang jelas, memperlihatkan tidak jelasnya pula penanganan kejahatan mayantara oleh para penegak hukum.

### 4.2.3 Perlunya Undang-Undang Khusus Cybercrime

Beberapa *cyberactivists* yang menjadi narasumber penelitian ini merasa belum mengenal undang-undang yang berkaitan dengan aktifitas mereka di dunia maya. Mereka tidak seluruhnya mengenal UU ITE, karenanya kepedulian dalam mengapresiasi isinya pun tidak sesuai harapan. Pandangan atau penilaian tentang muatan UU ITE ini cenderung sebagai penilaian dari pencitraan yang ditimbulkan saja di dalam ruang publik. Sehingga mereka yang belum membaca isi UU ITE sudah dapat

[357] Wawancara dengan Onno W. Purbo, 20 Mei 2011.

memberikan pendapat tentang bagaimana UU tersebut, dengan kacamata dari sisi pengimplementasiannya di masyarakat.

Muatan UU ITE memang ditujukan bagi terpenuhinya: 1) Asas kepastian hukum;[358] 2) Asas manfaat;[359] 3) Asas kehati-hatian;[360] 4) Asas itikad baik;[361] 5) Asas kebebasan memilih teknologi atau netral teknologi.[362] Akan tetapi definisi-definisi yang digunakan di dalam UU ITE masih terasa umum terlebih sebagai panduan dalam penegakan hukum pidana mayantara.

Perdebatan yang meluas dan populer di masyarakat adalah tentang Pasal 27 ayat (3) UU ITE tentang pencemaran nama baik:

(3) Setiap orang dengan sengaja dan 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.

Kritik yang menonjol di antaranya perihal wacana, dengan tuntutan pidana yang jauh lebih tinggi dari undang-undang yang ada sebelumnya yang terkait penghinaan. Selain itu munculnya delik penghinaan baru dalam UU ITE ini sudah masuh dalam overkriminalisasi.[363] Delik

---

[358] Berarti landasan hukum bagi pemanfaatan Teknologi Informasi dan Transaksi Elektronik serta segala sesuatu yang mendukung penyelenggaraannya yang mendapatkan pengakuan hukum di dalam dan luar negeri. Lihat Penjelasan Pasal 3 UU Nomor 11 tahun 2008 tentang ITE.

[359] Berarti asas bagi pemanfaatan Teknologi Informasi dan Transaksi Elektronik diupayakan untuk mendukung proses berinformasi sehingga dapat meningkatkan kesejahteraan masyarakat. Lihat Penjelasan Pasal 3 UU Nomor 11 tahun 2008 tentang ITE.

[360] Berarti landasan bagi pihak yang bersangkutan harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian, baik bagi dirinya maupun bagi pihak dalam pemanfaatan Teknologi Informasi dan Transaksi Elektronik. Lihat Penjelasan Pasal 3 UU Nomor 11 tahun 2008 tentang ITE.

[361] Berarti asas yang digunakan para pihak dalam melakukan Transaksi Elektronik tidak brtujuan untuk secara sengaja dan tanpa hak atau melawan hukum mengakibatkan kerugian bagi pihak lain tanpa sepengetahuan pihak lain tersebut. Lihat Penjelasan Pasal 3 UU Nomor 11 tahun 2008 tentang ITE.

[362] Berarti asas pemanfaatan Teknologi Informasi dan Transaksi Elektronik tidak terfokus pada penggunaan teknologi tertentu sehingga dapat mengikuti perkembangan pada masa yang akan datang. Lihat Penjelasan Pasal 3 UU Nomor 11 tahun 2008 tentang ITE.

[363] Anggara, et.al, Kontroversi Undang-undang ITE: Menggugat Pencemaran Nama Baik di Ranah Maya, Degraf: Jakarta, 2010, hal. 36.

pencemaran nama baik yang ada di dalam KUHP Pasal 310 sekiranya masih bisa diterapkan untuk melakukan pencegahan. Namun dalam Pasal 27 ayat (3) tersebut memberikan perluasan penjelasan delik dengan kata-kata "mendistribusikan", "mentransmisikan", dan "membuat dapat diakses", dengan maksud untuk mendekatkannya pada pemahaman bidang TI (Teknologi Informasi). Akan tetapi pada kenyataannya dalam Kamus Besar Bahasa Indonesia dan *Black Law Dictionary, Eighth Edition*, ternyata berbeda dengan pengertian mendistribusikan, mentransmisikan, dan membuat dapat diaksesnya sebagaimana dimengerti oleh kalangan yang bergelut dalam dunia TI (Teknologi Informatika).[364]

Selain Pasal 27, terdapat juga permasalahan dalam Pasal 28. Pasal 28 ayat (1) hanya menggunakan unsur "berita bohong" ini juga dapat menyebabkan ketidakpastian, karena bisa jadi informasi atau berita bohong tersebut dilakukan melalui media cetak hanya tujuan transaksinya adalah transaksi elektronik. Pada pasal tersebut juga hanya menggunakan unsur "penyebaran informasi", hal ini menandakan kecerobohan dan ketidakcermatan dari para pembentuk UU ITE karena tidak juga didapatkan penjelasan yang memuaskan kenapa tidak digunakan kalimat informasi elektronik dan/atau dokumen elektronik?[365]

Perlunya perbaikan filosofis masih terbuka bagi UU ITE. Hukum sebagai keseluruhan aturan tingkah laku yang bertujuan mencapai ketertiban dalam masyarakat mengharuskan adanya ketegasan, kejelasan, dan ketepatan dalam penyusunan kalimat. Di samping itu, dituntut pula adanya konsistensi. Semua itu dimaksudkan untuk mencegah agar perumusan norma hukum tidak menimbulkan kemaknagandaan dan kesamaran, sehingga menjamin kepastian hukum.[366] Kejelasan delik juga akan memberikan ketegasan dalam penegakan hukumnya.

---

[364] *Ibid*., hal. 67.
[365] *Ibid*., hal. 35.
[366] *Ibid*., hal. 66.

Dalam banyaknya tindak kejahatan mayantara dan peristilahan khusus yang melekat pada tindak pidana tertentu secara khas, tentunya tidak cukup dijabarkan dalam bentuk-bentuk perbuatan yang dilarang dengan definisi yang berpotensi digunakan dengan tumpang-tindih, meski delik-delik dalam UU ITE masih dapat ditemukan padanannya dalam KUHP. Jan Remmelink (2003) memberi pengarahan bahwa, apabila risiko bahaya hendak dihindarkan, pembuat undang-undang dapat memilih dua cara. Ia dapat memutuskan untuk merumuskan suatu perbuatan tertentu sebagai tindak pidana, karena berdasarkan pengalaman perbuatan tersebut sangat mudah berujung pada pelanggaran kepentingan-kepentingan hukum, tanpa merumuskan lebih terperinci kepentingan-kepentingan hukum seperti apa yang rentan terhadap risiko tersebut. Sebaliknya, ia juga dapat merumuskan suatu tindakan sebagai tindak pidana, apabila tindakan tersebut *in concreto* telah menimbulkan bahaya yang dirumuskan dalam undang-undang. Dalam cara pertama, kita berbicara tentang delik yang menimbulkan bahaya abstrak dan dalam cara kedua tentang delik yang menimbulkan bahaya konkret.[367]

Pengenalan terhadap konteks kemungkinan risiko berdasarkan atas 'pengalaman' perlu mendapatkan masukan dari berbagai sumber tentang potensi-potensi yang sekiranya dapat dikelompokkan ke dalam delik yang dapat menimbulkan bahaya abstrak, atau sebaliknya, tentang delik yang dapat menimbulkan bahaya konkret. Hal-hal tersebut sekiranya cukup sensitif untuk mendapatkan definisi yang tegas dan sesuai dengan konteks tindakan-tindakan di dalam ruang maya.

Beberapa hal memerlukan kejelasan peristilahan dan definisi yang sesuai untuk berbagai istilah teknis TI (Teknologi Informasi), dan peran publik para aktifis *cyber* dan profesional TI secara individu maupun kolektif dari berbagai komunitas, dapat diberdayakan dalam memberikan

[367] Jan Remmelink, *Hukum Pidana* (*Inleiding tot de Studie van het Nederlanse Strafrecht*), diterjemahkan oleh Tristam Pascal Moeliono, (Jakarta: Gramedia, 2003), hal. 62-63.

peran dalam pembentukan kebijakan. Dan lebih jauh dengan terjalinnya saling pengertian dan hubungan baik yang positif demi mendukung terlaksananya supremasi hukum, antara penegak hukum dengan para *cyberactivists*, juga akan memberikan sosialisasi kebijakan publik yang lebih terarah dan berakar kuat. Hal terakhir adalah kendala terbesar yang ada dalam pengimplementasian UU Nomer 11 Tahun 2008, tentang ITE (Informasi dan Transaksi Elektronik).

## 4.3 Peran Hacker dalam Penegakan Hukum Pidana Mayantara Perspektif Teori Diskursus Jurgen Habermas

Dalam penelitian yang dilakukan dengan mengamati beberapa beberapa komunitas *hacker* Indonesia di dunia maya, dan melakukan wawancara kepada beberapa *founder* komunitas *hacker*, *hacker*, profesional tehnik informatika, dan *ex-viruswriter*, yang masing-masing memiliki kombinasi kemampuan yang beragam serta pengalaman mereka menghampiri profesionalisme dalam *cyberspace* juga berbeda-beda.

Pendekatan terhadap komunitas *cyber* terutama yang memiliki fokus terhadap teknologi informasi merupakan arahan dari pemikiran yang memandang bahwa fungsi komunitas tersebut memiliki peran yang signifikan dalam mengkaji lingkungan sosial mayantara, ruang sosial yang dibentuk oleh hasil-hasil kerja tehnik informatika secara kolektif yang terus berkembang dan bergerak maju.

Dalam lingkungan sosial mayantara terdapat konsep ruang yang berbeda dengan ruang sosial dalam dunia nyata. Ruang sosial mayantara meskipun sebagai simulasi atas ruang sosial nyata, tetapi tidak lantas merupakan sebuah penyederhanaan dari ruang sosial nyata. Ruang sosial mayantara adalah simulasi komunikasi dalam ruang sosial dunia nyata, yang kemudian berkembang kepada fungsi-fungsi lain untuk menyederhanakan ruang dan waktu (yang meliputi juga kerja), sehingga banyak konsep-konsep baru yang mengikuti perubahan tersebut, baik perubahan benda, istilah, atau bahkan bahasa serta pengertian juga mengalami regenerasi makna.

Dominasi komunikasi dan berbagai perangkat yang menjadi penyusun ruang mayantara, menjadikan mereka yang memiliki kemampuan utama dalam mengelola, menciptakan, mengembangkan, atau merubah fungsi-fungsi komunikasi dan perangkatnya tersebut, juga merupakan mereka yang menguasai ruang maya. Dengan demikian, terlihat pentinglah kemampuan teknis dalam *cyberspace*.

Mekanisme-mekanisme pengawasan terhadap lingkungan sosial mayantara dan interaktifitas di dalamnya pun mengalami perubahan luar biasa dari bentuk tradisionalnya di dunia nyata. Dengan kemampuan dan seiring perkembangan teknologi peralatan teknis mayantara, maka seseorang dapat mengawasi aktifitas mayantara tidak terikat oleh ruang dan waktu. Berbagai institusi selain negara-negaralah yang justru bisa melakukan kontrol dan pengawasan terhadap ruang sosial mayantara tersebut. Dalam kurun beberapa tahun terakhir kita dapat melihat bagaimana opini publik dan besarnya ruang komunikasi maya untuk menyuarakan suatu gerakan semisal 'Koin Prita', 'Dukungan untuk Candra-Bibit', 'Cicak vs. Buaya', dan gerakan dukungan lainnya merupakan suatu pendorong kepada proses hukum yang lebih memihak pada dominasi isu yang berkembang di mayantara. Dari dinamika yang kita alami tersebut, maka benarlah Habermas saat menyatakan bahwa "ruang publik seluas otoritas publik,"[368] terlebih dalam mayantara.

Dapat dikatakan bahwa hukum pidana mayantara Indonesia mengalami krisis legitimasi dalam wilayah publik. Selain sosialisasi UU ITE yang menjadi penuh kendala, rupanya muatan pasal-pasal di dalamnya juga tidak sensitif terhadap realitas ruang tempat aturan itu diterapkan.

Legitimasi yang berkaitan erat dengan ruang sosial mendapat perhatian Habermas. Secara terpisah dalam gagasan, tetapi ia konsisten terhadap konsep modernisme yang diusung Mazhab Frankfurt dan terus mengkritisinya untuk senantiasa adaptif pada masanya. Dan dari modernisme Habermaslah ditemukan

[368] Jurgen Habermas, *Ruang Publik: Sebuah Kajian tentang Kategori Masyarakat Borjuis* (*Public Sphere: An Inquiry into a Category of Borgeois Society*), diterjemahkan oleh Yudi Santoso, (Yogyakarta: Kreasi Wacana, 2010), hal. 46.

kaitannya dengan ketegasan hukum dalam menciptakan klaim-klaim konsensual dan bagaimana legitimasi hukum dapat dipulihkan. Dari bekal pembahasan yang sudah digelar pada pembahasan-pembahasan sebelumnya sudah kita dapatkan tiap-tiap pihak yang mempunyai peran dialektis dalam memberikan legitimasi hukum pada ruang publik mayantara, yaitu antara: Negara (dan penegak hukum di dalamnya), Komunitas *cyberactivists* (dengan fokus pada para *cyber-hackers*), serta publik mayantara serta mekanismenya yang membentuk ruang publik.

### 4.3.1 Teorema Diskursus Habermas

Dalam teori diskursus Habermas,[369] ia telah melakukan kritik terhadap konsep Immanuel Kant tentang rasio praktis. Menurut Habermas rasio praktis beroperasi dalam model filsafat subjek. Berbeda dengan rasio murni (*reine Vernunft*) yang merupakan kemampuan akal budi manusia untuk memperoleh pengetahuan teoretis, rasio praktis (*praktische Vernunft*) adalah kemampuan akal budi manusia untuk mengetahui baik atau buruknya suatu tindakan. Rasio praktis adalah dasar moralitas dan hukum. Dalam konsep rasio praktis tersebut Kant mengandaikan subjek tindakan sebagai sesuatu yang menimbang-nimbang scara sendirian apa yang seharusnya ia lakukan. Subjek otonom ini menimbang-nimbang, maksim tindakan manakah yang sekiranya legitim sebagai norma penerapan undang-undang (*Gesetzgebung*) untuk semua orang. Kant lalu merumuskan maksim tindakan itu di dalam *imperatif kategorisnya* yang termasyhur itu: "Bertindaklah sedemikian rupa, sehingga maksim kehendakmu kiranya dapat berlaku setiap saat sekaligus dapat ditetapkan sebagai suatu undang-undang yang bersifat universal." Subjek dari rasio praktis ini menurut Habermas mengambil keputusannya secara monologal, yakni tanpa konsensus dengan subjek-subjek lainnya.[370] Keputusan dan pertimbangan yang monologal inilah yang oleh Habermas dipandang sebagai sesuatu

[369] Saya menggunakan rujukan konseptual pada: F. Budi Hardiman, *Demokrasi Deliberatif*, cetakan kelima, (Yogyakarta: Kanisius, 2009).

[370] *Ibid*., hal. 28-29.

yang potensial menuju absolutis dan totaliter. Yang jika diterapkan dalam penetapan hukum suatu negara akan menghasilkan hukum yang totaliter.

Jalan untuk menghindari terjadinya totalitarisme adalah dengan memberikan konsep rasio komunikatif, dan konsep rasio komunikatif tersebut di dalam filsafat politik Habermas dipahami secara *proseduralistis.*[371] Untuk memahami proseduralisme kita harus memisahkannya dari pengertian 'rasio kritis' yang dikritisinya, atau 'rasio instrumental', dan lain sebagainya. Akan tetapi 'rasio prosedural' ini semestinya tidak terpisahkan dari 'rasio komunikatif'.

F. Budi Hardiman memberikan contoh pemahaman rasio prosedural dengan bidang peradilan sebagai contohnya. Di dalam proses pengadilan orang tunduk pada prosedur-prosedur tertentu untuk menyelesaikan konflik-konflik yang terjadi di antara orang-orang yang berperkara. Untuk itu orang harus bertolak dari anggapan bahwa proses pemeriksaan melalui pengadilan itu tidak memihak di hadapan berbagai macam kepentingan yang saling bertentangan. Proses pengadilan tersebut hanya mungkin dan hanya dapat terlaksana, jika proses itu berdasarkan pada sebuah ide yang mengatasi proses itu, yakni ide keadilan. Keadilan memang tak dapat diwujudkan sepenuhnya, karena kepentingan-kepentingan tersembunyi dari pihak-pihak yang berperkara ataupun dari hakim tak dapat dikalkulasi. Akan tetapi fakta dari ide keadilan itu harus diandaikan, supaya proses pengadilan itu dapat berlangsung. Ide keadilan itu bersifat konstitutif, karena tanpanya proses pengadilan itu tak dapat terlaksana. Ide itu sekaligus juga regulatif karena berlaku sebagai prosedur untuk memeriksa apakah proses itu sendiri adil atau tidak.[372]

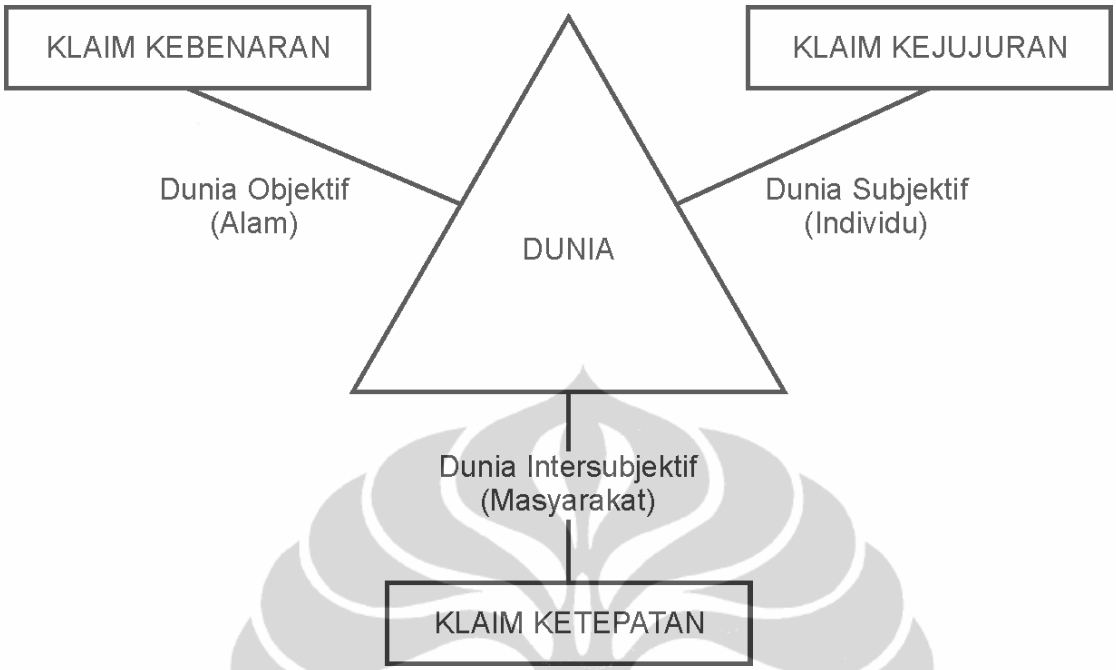
Dengan memahami proses pengadilan sebagai contoh yang dimaksud untuk memahami rasio prosedural, F. Budi Hardiman hendak menjelaskan bahwa apa yang sangat penting dalam rasio prosedural bukanlah

[371] *Ibid*., hal. 31.
[372] *Ibid*., hal. 32.

kemasukakalan konsep yang dirancang oleh seseorang secara monologal, melainkan prosedur yang diakui secara intersubjektif. Lewat prosedur itulah tiap-tiap pihak dengan melalui proses yang rasional mencoba mendapatkan kesahihannya. Dan dengan upaya yang terbuka terhadap pemberian pemahaman timbal-balik dari masing-masing pihak dengan tidak mencampur atau merusaknya dengan suatu otoritas kekuasaanlah keadilan dapat tercapai. Maka mekanisme pengadilan yang memeriksa kebenaran secara intersubjektif dan tanpa adanya kekuasaan otoriter yang mendominasi, namun tetap menggunakan prosedur yang diterima oleh seluruh pihak adalah bentuk formal dari rasio prosedural.[373]

Maka kesahihan keputusan bersama adalah saat tidak ada kekuasaan yang mendominasi dalam pengambilan keputusan, klaim-klaim kesahihan datang dari setiap pihak yang sama-sama memberikan kejujuran performatifnya kepada komunikasi intersubjektif tersebut. Budi Hardiman menjelaskan, karena itulah Habermas lebih menekankan tindakan komunikatif sebagai langkah menuju konsensus adalah lebih utama jika dibandingkan dengan tindakan-tindakan lain yang diupayakan untuk menghasilkan mekanisme koordinasi sosial.

[373] *Ibid*., hal. 33.



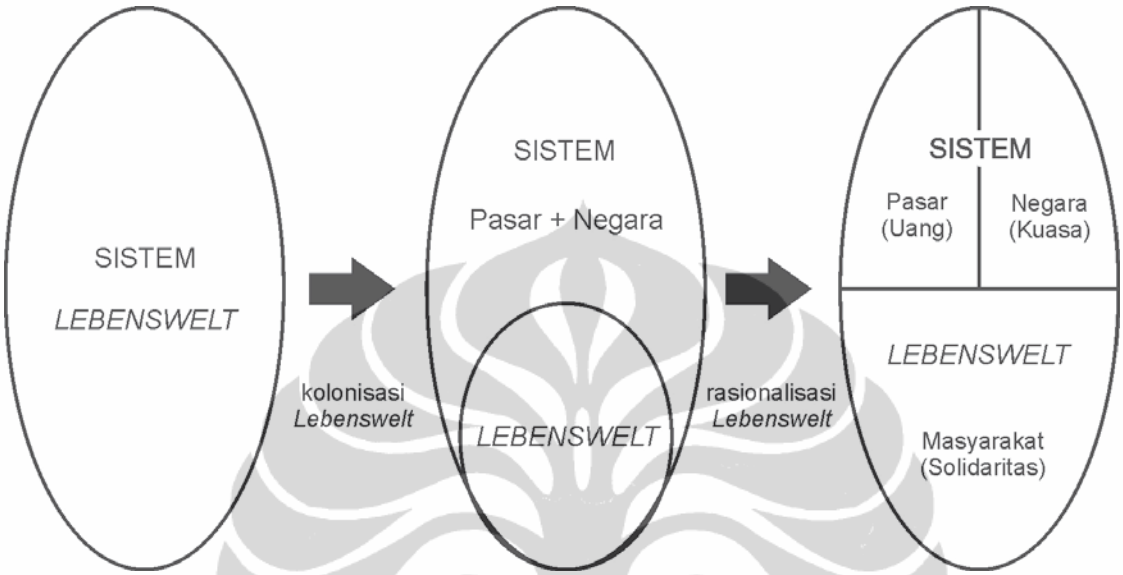

*Gambar 4.1. Dalam komunikasi diambil tiga macam sikap performatif terhadap dunia. Konsensus dapat tercapai hanya jika ketiga klaim kesahihan itu serentak dipenuhi.*

Dalam memahami mekanisme terciptanya konsensus yang dengan tindakan komunikatif kita tidak dapat mengandaikan klaim-klaim kesahihan itu begitu saja. Bagi dunia objektif, subjektif, dan intersubjektif terdapat klaim yang bersama-sama diandaikan kebenarannya secara kultural dan tidak terbantahkan. Untuk komunikasi yang sedang berlangsung hal-hal tersebut membentuk suatu pengetahuan bersama yang bersifat pra-reflektif, tak dipersoalkan dan implisit. Pengetahuan-latar-belakang yang membentuk konteks komunikasi ini dan beroperasi di belakang proses-proses komunikasi verbal ini disebut Habermas dengan istilah yang sudah lama dikembangkan dalam fenomenologi Edmund Husserl, yaitu: *Lebenswelt* (dunia-kehidupan).[374]

Di samping penjelasan tentang *Lebenswelt*, Habermas juga mengamati fungsionalitas serta tindakan masyarakat. Habermas dari sisi pengamat melihat adanya jaringan fungsional dari rentetan tindakan, dan

[374] *Ibid*., hal. 38.

dengan begitulah masyarakat muncul sebagai sistem. Dalam masyarakat modern ia menyebut sistem mencolok pada ekonomi dan kekuasaan negara.




*Gambar 4.2.* Perkembangan *Lebenswelt* terhadap sistem.[375]

Dengan memperhatikan hubungan antara sistem dengan *Lebenswelt,* Habermas mengandaikan bahwa idealnya sistem dan *Lebenswelt* berada dalam kesetimbangan. Namun pada awalnya keduanya tidak terpisahkan dan menyatu, kemudian dengan tekanan sistem, *Lebenswelt* mengkolonisasikan diri. Dan dengan rasionalisasi yang memungkinkan terbentuknya komunikasi maka keduanya dapat membentuk ruang yang sepadan satu sama lain.

Dengan ditempuhnya diskursus antara polisi dan jaksa sebagai penegak hukum dengan komunitas *cyber* dengan baik, maka akan ditemukan cara pula untuk menjadikan saling pemahaman dan memberikan kemungkinan kesepahaman antara kedua belah pihak. Sehingga, nilai-nilai yang meneguhkan moralitas tiap mereka yang berada dalam komunitas dapat didialogkan dengan kekuatan politis untuk mengatur sistem. Dan selanjutnya akan terjadi upaya kuat untuk menegaskan hukum sebagai

[375] *Ibid*., hal. 41.

proses untuk mencapai kesahihan tentang kebaikan dan keburukan bersama, dalam hal ini moralitas dalam suatu komunitas akan berusaha dijadikan formula bagi kekuatan penegakan hukum.

### 4.3.2 Hukum dan Proseduralisme

Yang kita temukan dalam perspektif sistem tampaknya semakin ditegaskan dari prespektif internal ini: semakin kompleks sebuah sistem sosial, semakin terpecah-pecah dunia-kehidupan. Dalam sistem sosial yang telah terdiferensiasi, dunia-kehidupan tampaknya tenggelam di bawah subsistem. Tidak boleh dibaca secara kausal, seolah-olah struktur dunia-kehidupan berubah tergantung pada peningkatan kompleksitas sistemik. Yang berlaku justru sebaliknya: meningkatnya kompleksitas tergantung pada diferensiasi struktural dunia-kehidupan. Bagaimanapun kita menjelaskan dinamika transformasi struktural ini, namun dia tetap mengikuti logika internal rasionalisasi komunikatif.[376]

Hukum pidana mayantara memerlukan peran aktor-aktor sosial untuk menciptakan komunikasi yang rasional dengan hukum itu sendiri. Rasionalitas sebagaimana dijelaskan sebelumnya adalah pembentuk ruang komunikasi yang terbuka antara negara dengan komunitas. Negara mesti menjaga legitimasi hukum, dan legitimasi hukum memerlukan suatu mekanisme yang baik, terlebih saat wilayah hukum yang dituju belum sepenuhnya terpahami dengan baik oleh pemilik otoritas politis dari hukum.

Mengamati semakin besarnya diferensiasi yang ada di ruang publik mayantara, Habermas memberi arahan bahwa level peningkatan kompleksitas hanya dapat dinaikkan dengan memperkenalkan mekanisme sistem baru. Setiap mekanisme baru diferensiasi sistem mesti ditempatkan

---

[376] Jurgen Habermas, *Teori Tindakan Komunikatif Buku Kedua: Kritik atas Rasio Fungsionalisasi* (*Theories des Kommunikativen Handelns, Band II: Zur Kritik der funktionalistischen Vernunft*), diterjemahkan oleh Nurhadi, cetakan pertama, (Yogyakarta: Kreasi Wacana, 2007), hal 235-236.

pada dunia-kehidupan; dia harus diinstitusionalisasikan di sana lewat status keluarga, otoritas jabatan atau hukum privat borjuis.[377] Sebagaimana pihak-pihak *hacker* dan komunitasnya maupun pemerintah sebagai pemegang otoritas semestinya mampu memisahkan dengan jelas sisi sosialnya dengan inti institusionalnya, dan dengan terbuka menjadi sosial dalam ruang publik, dalam *Lebenswelt*. Karena hanya dengan cara demikianlah tindakan komunikatif untuk mencapai kesepakatan konsesual yang deliberatif dapat tercapai, inilah rasionalisasi dari kemungkinan. Habermas menjelaskan bahwa Institusionalisasi level baru diferensiasi sistem memerlukan rekonstruksi inti wilayah institusional regulasi moral-legal konflik (artinya, bersifat konsesual).[378]

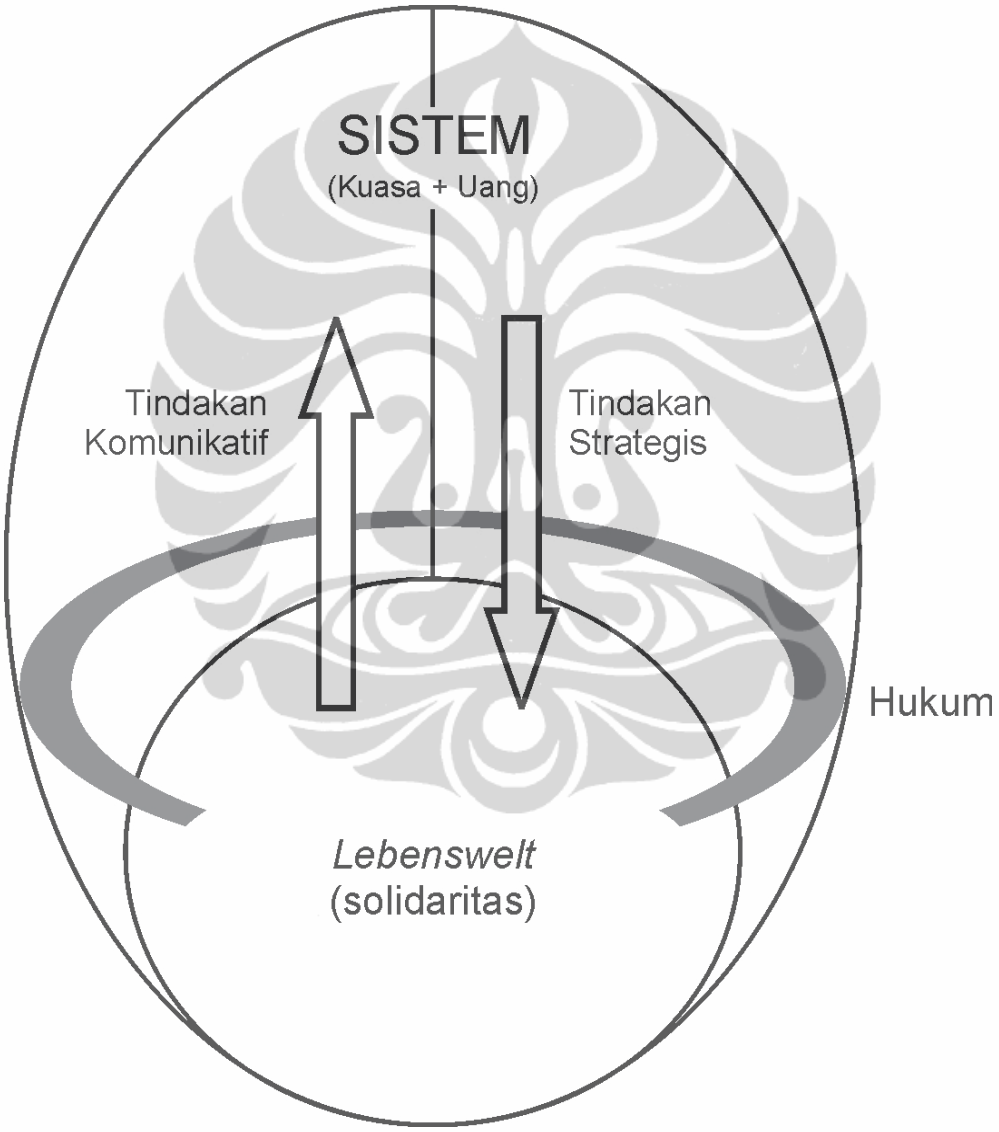
Dengan demikian maka perlulah komunitas mayantara dan pihak penegak hukum memerlukan perbaikan sistem mereka masing-masing, setiap pihak perlu menciptakan pemilahan antara peran institusional masing-masing dan sekaligus harus menjaga kemampuannya untuk senantiasa membuka ruang-ruang komunikatif satu sama lain, agar terciptak kesalingpengertian. Jika ruang-ruang ini terbentuk maka akan menciptakan kemungkinan konsesual dan ruang bagi penyelesaian konflik.

| Tahap-tahap kesadaran moral | Konsep sosiokognitif dasar | Etika | Jenis Hukum |
|---|---|---|---|
| Prakonvensional | Harapan perilaku tertentu | Etika magis | Hukum suci |
| Konvensional | Norma | Etika Hukum | Hukum tradisional |
| Pascakonvensional | Prinsip | Etika keyakinan dan tanggung jawab | Hukum formal |

[377] *Ibid*., hal 236.
[378] *Ibid*.

*Tabel 4.4. Tahap-tahap perkembangan hukum.*[379]

Dalam Teori Tindakan Komunikatif II Habermas menjelaskan tentang perkembangan hukum menurut perkembangan kesadaran moral dan sosiokognitif dasar, pada awalnya etika dan hukum dalam sosial ada dalam satu kesatuan, kemudian dengan kian munculnya norma-norma sekat antara keduanya mulai samar.




*Gambar 4.3. Dalam negara hukum demokratis hukum menjadi "poros proses pertukaran antara sistem dan Lebenswelt.*[380]

[379] *Ibid*., hal 237.

F. Budi Hardiman membuat penjelasan bagaimana hukum mempunyai peran dalam menjaga agar tindakan komunikatif antara *Lebenswelt* terjaga, sebagai penjaga integrasi yang baik. Akan tetapi perkembangan hukum sebagaimana yang telah dijelaskan Habermas dalam tabel sebelumnya, perlu adanya ketegasan posisi hukum yang berdiri sendiri terlebih dahulu. Gambar yang diberikan oleh F. Budi Hardiman tersebut menjelaskan peran hukum terhadap proseduralisme. Proseduralistis perlu diingat adalah merupakan rasio komunikatif dalam konsep Habermas. Gambar tersebut hendak menjelaskan bagaimana hukum memiliki poros pertukaran dan sekaligus menjaga mekanisme/ mengontrol pertukaran atau tindakan komunikatif untuk memberikan ruang bagi masing-masing pihak untuk mendapatkan posisi menjelaskan kesahihannya.

Dalam permasalahan hukum pidana dalam ruang publik mayantara Indonesia, perlu diciptakan kemungkinan bagi hukum untuk mencapai bentuk otonomnya. Pemahaman proses sejak memilah hukum tradisional dari etika hukum, yang kemudian akan membentuk hukum formal yang otonom di satu sisi dan etika keyakinan dan tanggung jawab di sisi lain dan keduanya berdiri sama tegak. Pada permasalahan minimnya pengakuan publik terhadap legitimasi hukum mayantara, harapannya adalah hukum pidana formal dapat berdampingan dengan etika yang selama ini berjalan baik dalam berbagai komunitas cyber dan melaluinyalah tanggung jawab tiap personal diemban.

Tindakan komunikatif yang timbal balik tersebut juga merupakan dukungan hukum, sebagai porosnya, terhadap kemungkinan terjaganya kepercayaan publik terhadap legitimasi hukum dan penegakan hukum yang baik dan membawa kesepakatan konsesualnya bersama publik mayantara akan memberikan jaminan kepercayaan publik. Dengan demikian publik

[380] Budi Hardiman, *op.cit.*, hal. 63.

dan pemilik kekuasaan dan pengelola sistem menjalin hubungan saling koreksi.

### 4.3.3 Demokrasi Deliberatif dan Legitimasi Hukum

Habermas menjelaskan bagaimana penyusutan legitimasi terjadi. Ia berpendapat bahwa penyusutan yang menimpa legitimasi harus diimbangi dengan penghargaan terhadap sistem. Krisis legitimasi muncul ketika tuntutan terhadap penghargaan-penghargaan semacam itu muncul lebih cepat daripada kuantitas nilai yang tersedia, atau ketika harapan-harapan yang muncul tidak bisa dipenuhi oleh penghargaan-penghargaan semacam itu.[381]

Peningkatan harapan publik terhadap perhatian kepada wilayah pidana hukum publik mayantara selama ini tidak diimbangi dengan peningkatan kemampuan sumber daya para penegak hukum. Dalam masyarakat informasi jaminan keselamatan bertransaksi dan jaminan karya intelektual di dalamnya adalah hal-hal yang sangat diinginkan sebagai bentuk jaminan mereka menciptakan ruang mayantara yang lebih apresiatif dan membuka peluang positif terhadap kinerja efektif masyarakat, yang bersamaan akan mendukung produktifitas.

Indonesia sebagai negara hukum memberikan jaminan konstitutif terhadap berbagai tindakan yang tidak bertentangan dengan konstitusi, dan berbagai undang-undang yang berakar pada konstitusi. Tindakan komunikatif yang timbal balik tersebut juga merupakan dukungan hukum, sebagai porosnya, terhadap kemungkinan terjaganya kepercayaan publik terhadap legitimasi hukum dan penegakan hukum yang baik dan membawa kesepakatan konsesualnya bersama publik mayantara akan memberikan jaminan kepercayaan publik. Dengan demikian publik dan pemilik kekuasaan dan pengelola sistem menjalin hubungan saling koreksi.

---

[381] Jurgen Habermas, *Krisis Legitimasi* (*Legitimation Crisis*), diterjemahkan oleh Yudi Santoso, (Yogyakarta: Qalam, cet. Pertama, 2004), hal 232-233.

F. Budi Hardiman menjelaskan bahwa legitimasi tidak terletak pada hasil komunikasi politik, melainkan pada prosesnya. Semakin diskursif proses itu, yakni semakin rasional dan terbuka terhadap pengujian publik, semakin legitim pula hasilnya. Betapapun koheren, sistematis dan estetisnya sebuah kebijakan atau norma publik, jika tidak lebih dahulu diuji secara diskursif dalam terang publik atau ditetapkan begitu saja oleh otoritas, kebijakan atau norma itu tidak mendapat legitimitas. Karena itu keterbukaan terhadap revisi justru menambah legitimitas sebuah kebijakan atau norma.[382]

Perbaikan sistem komunikatif yang berciri demokrasi deliberatif akan memberikan manfaat berupa perbaikan kepada keseluruhan mekanisme komunikatif di dalam sistem dan *Lebenswelt* publik mayantara, atau singkat kata, akan memberikan dampak positif yang meluas dalam sistem negara dan terpenuhinya jaminan-jaminan konstitusional. Bagaimanapun penjelasan terhadap logika tindakan komunikatif antara publik dan negara akan selalu memberikan gambaran pengaruh timbal-balik, dengan hukum sebagai poros kontrolnya dan keterbukaan terhadap potensi kesahihan konsesual sebagai jaminan penegasan kebenaran dan keberlangsungan hukum yang legitimatif yang menjadi porosnya.

Jaminan konstitusional untuk ruang publik atau masyarakat warga yang otonom tersebut sudah melekat pada konstitusi demokratis negara hukum. Hak-hak dasar ini menstrukturisasi ruang publik dalam kaitannya dengan ruang tindakannya, dengan keamanan infrastruktur-infrastruktur medianya, dengan hubungannya dengan sistem politik, dan dengan pluralismenya.[383]

Nonet dan Selznick menjelaskan bahwa, barangsiapa berbagi ruang sosial, ia akan memperoleh jaminan legitimasi. Terhadap komitmen untuk memperkuat rasa memiliki dan menghindari sikap dan gaya yang

[382] Budi Hardiman, *op.cit.*, hal. 130.
[383] *Ibid*., hal. 139.

mengucilkan individu dari komunitasnya. Standar kesopanan menjangkau pula pelaksanaan otoritas dan juga partisipasi publik. Pada kedua hal tersebut, kesopanan menyerukan suatu semangat moderat dan terbuka.[384]

## 4.4 Bentuk Kerjasama Penegakan Hukum Pidana antara Agen Sosial Mayantara dan Lembaga Penegak Hukum

Penjelasan tentang 'Publik' dalam dunia maya masih memerlukan pemfokusan untuk mendapatkan kekhususan dalam tujuan penelitian, dan kebutuhan akan kemampuan kelompok yang diteliti dalam mengamati cakupan luas ruang mayantara dengan baik. Fokus pada pemerhati aktif dan sekaligus mereka yang mengerti sistem akan dapat memberikan penegasan yang lebih sesuai.

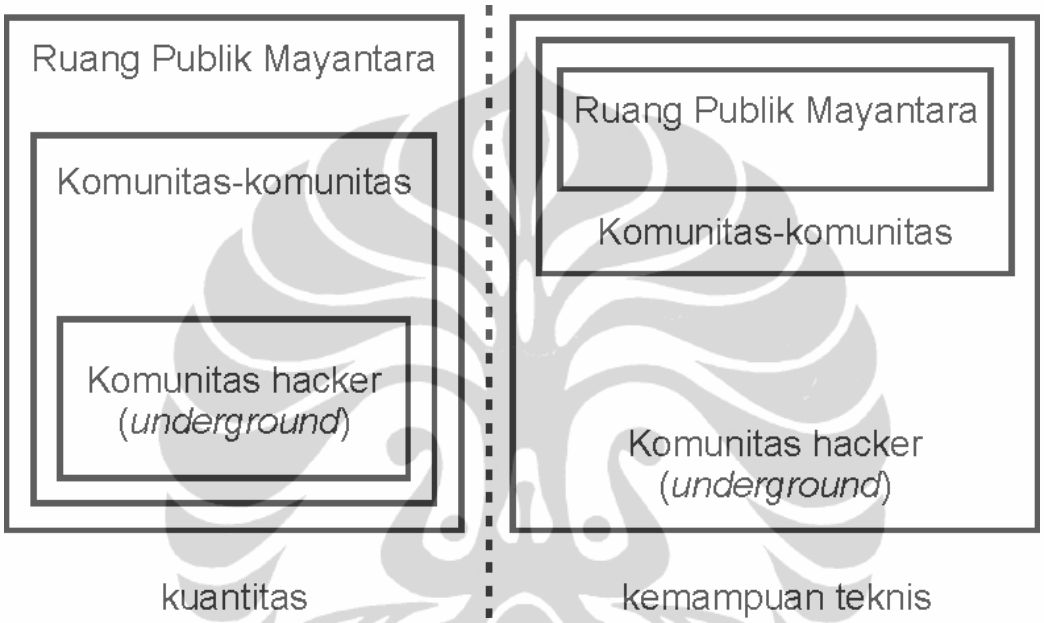
Tidak berpaling dari konsep strukturasi masyarakat, saya meminjam teori Anthony Giddens tentang dasar-dasar pembentukan struktur sosial masyarakat, bagaimana kemampuan pengawasan dan kontrol suatu komunitas *cyber* terhadap lingkungan komunikatifnya dan penguasaannya terhadap sumber kekuatan mayantara (pengetahuan). Perihal permasalahan *cybercrime* maka pertautan memfokuskan pada komunitas *hacker* yang memiliki relevansi luas terhadap berbagai bentuk mekanisme dalam ruang mayantara.

*Hacker* sebagai agen-agen sosial komunitas mayantara, baik terhadap setiap individu di bawah kemampuannya dan ruang-ruang dalam jangkauan pengamatannya, maupun terhadap kemampuan komunikatifnya dengan pertimbangan solidaritas komunitas, merupakan agen yang sesuai dan potensial untuk dikaji sebagai upaya pemulihan legitimasi hukum pidana mayantara. Sebagaimana pengamatan dan interaksi yang telah dilakukan terhadap komunitas serta *hacker* secara individu, optimisme terhadap penegakan hukum yang responsif di ruang mayantara Indonesia cukup kuat. Sekali lagi, pemberian asumsi optimisme tersebut hadir dari penilaian mereka terhadap berbagai

[384] Philippe Nonet dan Philip Selznick, *Hukum Responsif* (Law and Society in Transition: Toward Responsive Law), diterjemahkan oleh Raisul Muttaqien (Bandung: Nusamedia, 2010), hal. 101-102.

kemungkinan kontrol yang dapat diterapkan terhadap mayantara. Pengandaian di dalam benak mereka bukanlah utopis, lebih karena kemampuan mereka secara teknis dan pertimbangan-pertimbangan prosedural yang semestinya dilakukan dengan ukuran logika mayantara.

### 4.4.1 Tanggung Jawab Sosial




*Gambar 4.4. Perbandingan kuantitas dan kemampuan teknis yang melingkupi kemampuan pengawasan.*

Peran terpenting *hacker* sebagai anggota komunitas dan sebagai sosok sosial di dalam ruang publik mayantara dalam pemulihan legitimasi hukum yang terpuruk adalah peranan sosialnya di dalam komunitas dan sekaligus peranan sosialnya kepada publik luas sebagai individu yang memiliki kemampuan teknis yang lebih dari publik pada umumnya. Gambar tersebut memperlihatkan bahwa kuantitas minimal komunitas *hacker (underground)*, dengan kemampuan teknis penanganan permasalahan kejahatan mayantara yang lebih dari yang lain, bisa memberikan kemampuan pengawasan (kontrol) secara lebih luas.

Dalam penelitian beberapa *hacker* yang sekaligus founder komunitas *hacker* menjelaskan bahwa permasalahan UU ITE (UU Nomor 11 Tahun

2008), yang diterapkan sebagai undang-undang untuk merespon kebutuhan tentang kepastian hukum dalam ruang mayantara yang secara kategoris fokus pada tindakan transaksi elektronik (pertukaran informasi), adalah pada persoalan sosialisasi yang sangat minim. Sebagian besar mereka tidak mengetahui persis tentang UU ITE tersebut, dan memberikan pendapat cenderung dengan pengamatan atas penerapannya di lapangan.

PZ dan BD, terutama, dalam hasil wawancara mereka menyampaikan bahwa sosialisasi masih minim. Dan BD menjelaskan bagaimana mekanisme sosialisasi pemimpin komunitas terhadap komunitasnya dan berbagai komunitas yang memiliki solidaritas sebagai sesama komunitas *hacker*, yaitu dengan menyampaikan informasi kebijakan pemerintah ke dalam forum maupun kepada masing-masing individu di dalam komunitas.

Sebagai contoh adalah aktifitas Onno W. Purbo dalam beberapa komunitas *hacker* besar di Indonesia.[385] Ia senantiasa membagikan berbagai informasi dan makalah digital ke dalam komunitas yang sekiranya dapat membantu para anggota komunitas secara keseluruhan, dan tentunya tidak dapat disangkal bahwa komunitas besar tidak tertutup dalam berbagi informasi.[386] Kebebasan persebaran informasi dan luasnya jangkauan untuk berbagi pengetahuan adalah nilai tambah dalam mendukung peran sosial para penggiat mayantara kepada seluruh penghuni ruang publik mayantara.

Dengan mempertimbangkan kemampuan teknis dan aksesibilitas dalam berbagai ruang-ruang komunitas yang berarti adalah keleluasaan, maka seorang pemimpin komunitas memiliki peran informatif kepada anggota komunitasnya, dan tiap anggota komunitas (para pemimpin komunitas termasuk di dalamnya) memiliki peran kepada publik sebagai

[385] Sejauh pengamatan yang dapat diikuti, Onno W. Purbo adalah sosok pakar teknologi informasi yang sering membagi wawasannya tentang permasalahan *cyber* ke dalam komunitas besar seperti Yogyafree-Perjuangan dan Jasakom-Perjuangan.

[386] Ukuran keterbukaan informasi ini adalah dapat diaksesnya informasi mengenai suatu permasalahan di dalam mesin pencari (misalkan: Google, Yahoo, dlsb.) dengan cara sederhana (tanpa memerlukan kemampuan tingkat lanjut).

tanggung jawab sosialnya.[387] Pertimbangan tersebut tidak lepas dari bentuk tanggung jawab sosial yang mengusung nilai-nilai kesopanan dalam interaksi mayantaranya. Dalam etika pertanggungjawaban "setiap orang harus memperhatikan akibat-akibat yang dapat diperkirakan dalam perbuatan-perbuatannya."[388] Oleh karenanya pemupukan tanggung jawab yang sudah tertanam dalam komunitas semestinya dikembangkan oleh masing-masing anggota komunitas sebagai tanggung jawab terhadap publik yang lebih luas dengan penanaman etika-etika sosial dalam komunitas.

Peran tanggung jawab sosial (*social responsibility*) komunitas serta merta muncul seiring dengan kemampuan anggota komunitas dalam memecahkan masalah sosial mayantara. Dan dalam hukum pidana yang merupakan bagian dari hukum publik. Yang mengemban tugas melaksanakan *jus puniendi* adalah OM, yang mewakili kepentingan masyarakat atau persekutuan hukum. Adalah tugas dari hukum pidana untuk memungkinkan terselenggaranya kehidupan bersama antar manusia.[389] Dalam kondisi tidak memungkinkannya hukum pidana ditegakkan sepenuhnya oleh Kepolisian dan Kejaksaan, dikarenakan keterbatasan teknis, baik keterampilan maupun pemahaman konsep dan kontekstual, yang berimbas pada keterbatasan kemampuan menjangkau ruang-ruang publik yang lebih luas. Maka diperlukan keterlibatan publik dalam mensosialisasikan berbagai kebijakan pemerintah secara lebih baik dan terpahami.

### 4.4.2 Peran Teknis

Dari penelitian terhadap tindak pidana mayantara, telah didapatkan berbagai data statistik terhadap peningkatan tehnik kejahatan, jumlah

---

[387] Seringkali para *hacker* memiliki peran konsultatif dalam berbagai permasalahan kejahatan mayantara yang dihadapi oleh individu-individu dalam ruang maya.

[388] Nonet, *op.cit.*, hal. 102.

[389] Jan Remmelink, *Hukum Pidana* (*Inleiding tot de Studie van het Nederlanse Strafrecht*), diterjemahkan oleh Tristam Pascal Moeliono, (Jakarta: Gramedia, 2003), hal. 5. Remmelink menjelaskan 'OM' adalah Kejaksaan.

tindak pidana, dan pertumbuhan aktifis komunitas *hacker*.[390] Yang kesemuanya memiliki relefansi terhadap perkembangan kriminalitas dalam *cyberspace*, dengan beberapa perbandingan data global (dunia) serta Amerika Serikat sebagai contoh dalam penerapan teknologi dan teknis penegakan hukum yang efektif dan kompetitif dengan pertumbuhan jumlah kejahatan *cyber*.

Data tersebut memperlihatkan bahwa perkembangan jumlah *cybercriminals* dan *potential offenders* beriring dengan perkembangan teknologi, dan dengan semakin tingginya kemampuan individu dalam menghadapi perkembangan teknologi maka akan menuntut kemajuan dalam hal kemampuan teknis untuk melakukan tindak kejahatan. Karena perkembangan teknologi yang pesat juga mendukung tingkat keamanan yang lebih baik, oleh karenanya untuk dapat meretas dan melakukan tindak kriminal dengan baik pun memerlukan kemampuan yang lebih baik dengan mengoreksi dan mencari kelemahan sistem yang akan diserang. Kemampuan teknis para *hacker* tidak dapat disamaratakan, akan tetapi keterampilan dalam melakukan aktifitasnya bisa terus diperluas. Terlebih mereka yang memiliki keingintahuan lebih terhadap sistem dan keamanannya, hal ini didorong oleh dorongan kuat untuk menguji keamanan dan keterampilan teknis mereka.

Seorang *hacker* memiliki kemampuan untuk melakukan peretasan dan kemampuan yang sama dengan teknis perunutan (*tracing*) yang dilakukan untuk melacak jejak digital para *cybercriminals*. Keterampilan *tracing* seringkali dilakukan untuk menyelesaikan permasalahan yang menimpa teman kantor, tetangga, maupun anggota komunitas. Dalam hal teknis yang terlalu lambat (dalam mengikuti perkembangan kemuslihatan

[390] Pertumbuhan aktifis komunitas *hacker* yang sangat signifikan kini, dengan perbandingan data yang dipublikasikan Onno W. Purbo, memperlihatkan bahwa pengetahuan tentang tehnik-tehnik hacking juga berkembang dan tersebar lebih luas dengan lebih cepat dari sebelumnya. Hal ini memberikan pertimbangan tentang lebih tingginya kemungkinan seseorang untuk terlibat dalam kejahatan mayantara.

yang pesat di dunia maya) dan rutin yang dilakukan oleh pihak Depkominfo, seorang *hacker* dengan komunitasnya mempunyai solusi untuk menghindarinya.[391] Hal tersebut hanya sebuah contoh, dan bisa jadi masih terdapat banyak contoh bagaimana rutinitas yang ajeg bisa diatasi dengan memperbaiki tehnik.

Selama ini peran teknis komunitas *hacker* dan *hacker* secara pribadi dalam lingkungan sosial mayantara didominasi peran edukatif dalam menghadapi permasalahan teknis mayantara, selain itu *hacker* dalam komunitas juga mempunyai peran penyelesaian kasus-kasus tindak pidana mayantara (dominasi tindak pidana), yang karena belum memadainya perangkat hukum yang ada, lebih cenderug diselesaikan di luar pengadilan. *Hacker* secara personal dengan pertimbangan solidaritas komunitas dan pertemanan berusaha memperkuat basis pertahanan dalam lingkarannya dan dalam lingkaran itulah terbentuk sistem pengawasan. Selain dalam komunitas, secara acak tiap-tiap *hacker* adalah pengawas terhadap aktifitas mayantara yang berlalu-lalang secara bebas dan terdeteksi oleh kemampuan teknis mereka.

Dalam penegakan hukum pidana mayantara, sekiranya dengan memahami kinerja dan kemampuan individu *hacker* dapat memunculkan dua peran yang berkaitan dengan hal teknis:

a. Peran advisorial bagi penanganan kasus tindak pidana mayantara. Seorang penegak hukum, baik dari Kepolisian maupun Kejaksaan, dapat mengambil peran *hacker* dalam menganalisa suatu peristiwa kejahatan mayantara dengan lebih baik. Dengan memanfaatkan keahliannya, seorang *hacker* dapat memberikan saran terbaik untuk melakukan pencegahan, perbaikan, atau pelacakan.[392]

[391] Wawancara dengan BD, 11 April 2011.

[392] Peran advisorial inilah yang banyak diberikan oleh para *hacker* kepada para anggotanya yang memiliki masalah. Akan tetapi advisori bagi penegak hukum semestinya tidak seluas yang terdapat di dalam komunitas antara seorang *hacker* dan anggota yang berkonsultasi, karena teknis *cyber* teramat luas yang dibagi di dunia maya termasuk di dalamnya tutorial yang sangat luas. advisori

b. Peran pelacakan dan rekam jejak bagi penanganan kasus tindak pidana mayantara. *Tracing* merupakan keterampilan lanjut para *hacker* yang masuk dalam kategori *cyberforensics*, terutama untuk membantu permasalahan kejahatan yang dialami oleh anggota komunitas atau seseorang maupun institusi yang meminta bantuan teknis untuk mengetahui pelaku kejahatan terhadap sistem yang mereka miliki. Kemudian dalam istilah teknis, *tracing* akan berlanjut pada upaya mendapatkan *digital finger prints* untuk dijadikan *proof*.[393] Berkaitan dengan hukum pidana (formal) maka perlu ke validitas cara mendapatkan *proof* yang baik untuk bisa membawanya ke proses persidangan, dimana *proof* akan dijadikan *evidence*.

Peranan *hacker* dan komunitasnya dalam teknis penanganan perkara pidana dapat berupa dua hal tersebut di atas, dengan pertimbangan bahwa kemampuan teknis tersebutlah yang biasa mereka lakukan dalam ruang lingkup komunitas. Pemberian peranan yang baik dan adaptif terhadap kemampuan teknis para *hacker* merupakan pembentukan ruang komunikasi antara pihak kepolisian serta kejaksaan dengan aktor-aktor mayantara dalam melakukan penegakan hukum secara aktual.

### 4.4.3 Peran Politis

Sebagaimana dijelaskan oleh Habermas dalam Ruang Publik, setiap agen sosial memiliki peran politis terhadap transformasi publik. Hal ini terjadi selama antara legislatif mampu secara terbuka dan demokratis menyerap aspirasi publik dengan baik. Pembahasan tentang bagaimana opini publik di bentuk dalam ruang-ruang publik berkaitan erat dengan

---

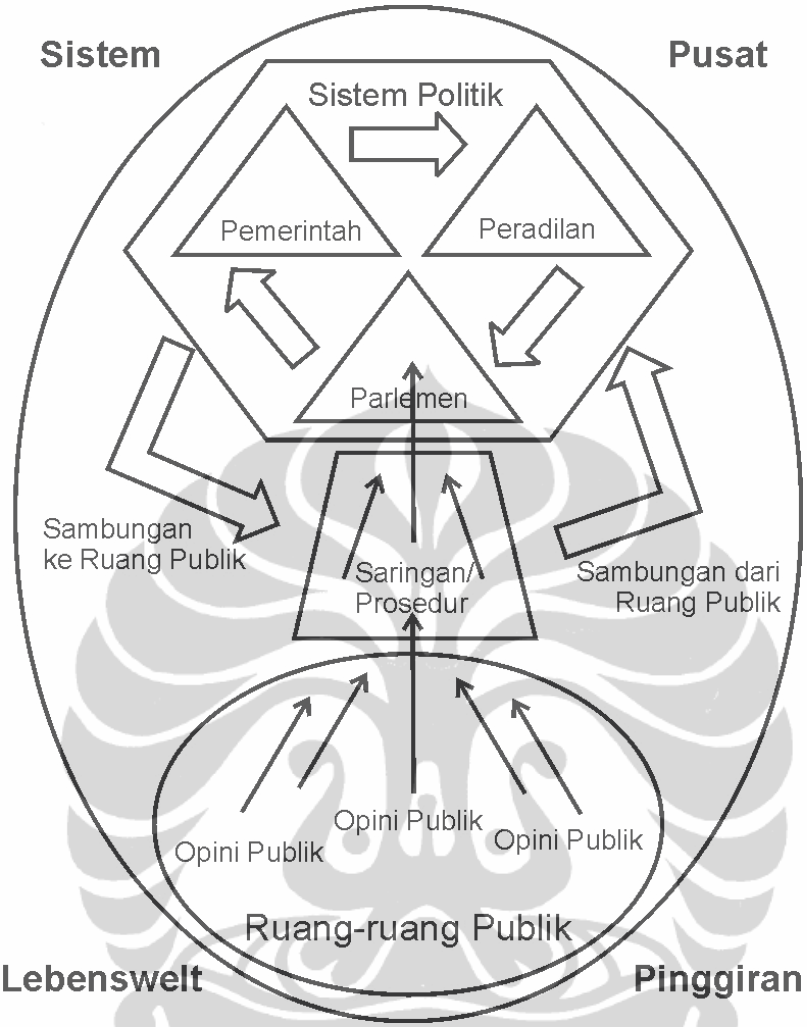
yang diberikan hendaknya adalah petunjuk teknis yang terarah dan praktis dalam memecahkan masalah.

[393] Dalam wawancara dengan BD, 11 April 2011. Dalam komunitas, penyelesaian permasalahan tindak pidana mayantara biasanya tidak melalui jalur hukum. Dalam jaringan komunitas satu dengan yang lainnya terdapat hubungan khusus untuk memberitahukan pelaku jika pelaku merupakan salah satu anggota dari komunitas lain. Jika komunitas tersebut memiliki ikatan emosional yang baik maka dapat menunjukkan siapa pelaku, jika *tracing* telah berhasil. Tetapi pada kasus komunitas yang besar dan sulit mengenali dan tidak adanya kedekatan emosional (hanya keakraban mayantara), hal ini sulit dilakukan.

tindakan komunikatif Habermas, seiring dengan konsistensinya terhadap sosiologi kritis dan modernisme.

Dalam penjelasan mengenai diskursus dan bagaimana cara masing-masing pihak yang terlibat di dalam diskursus untuk bisa mendapatkan kesahihan. Peran politis ini seiring dengan pendapat PZ saat menjelaskan tentang bagaimana sebaiknya undang-undang khusus *cybercrime* disusun. Ia mengusulkan agar pemerintah tidak sepihak menyusun suatu peraturan, terlebih yang menyangkut aktifitas mayantara secara luas dan tanpa wawasan yang cukup. PZ mengusulkan jika masing-masing pemimpin dari komunitas *hacker* dilibatkan secara aktif dalam penyusunan undang-undang tersebut.[394]

[394] Wawancara dengan PZ, 16 April 2011.




*Gambar 4.5. Opini publik yang berasal dari ruang publik masuk ke dalam sistem politik melalui saringan atau prosedur yang dapat dibayangkan sebagai bendungan.*[395]

Mula-mula 'publik', memang subjek opini publik, dipersamakan dengan 'massa', lalu dengan 'kelompok', kemudian sebagai substratum sosial-psikologis bagi proses komunikasi dan interaksi antara dua individu atau lebih. 'kelompok' diabstraksikan dari serangkaian kondisi sosial dan historis, serta alat-alat institusional, dan tentunya dari jaringan-jaringan fungsi sosial yang dulu pernah jadi penentu strata masyarakat privat yang bergabung membentuk publik yang berdebat kritis di wilayah politis. Opini

[395] Budi Hardiman, *op.cit.*, hal. 149. Habermas memberikan 'model bendungan' (*Schleusenmodel*) dengan meminjam teori demokrasi rancangan B. Peters.

bukan hanya mencakup kebiasaan yang terekspresikan di dalam konsep-konsep tertentu, namun juga segala mode tingkah laku.[396]

F. Budi Hardiman menjelaskan pemikiran Habermas yang mengacu pada Talcott Parsons, menjelaskan "pengaruh" sebagai bentuk komunikasi yang digeneralisasi secara simbolis...yang mengontrol interaksi-interaksi berkat persuasi-persuasi atau bujukan-bujukan." Dalam arti ini ruang publik mengandung potensi kekuasaan yang tidak mengecualikan kekuasaan sosial, yakni pemaksaan kehendak sendiri di hadapan orang-orang lain. Dalam pandangan Habermas sebuah politik boleh menyatakan dirinya sebagai deliberatif hanya jika tersedia sebuah prosedur diskursif yang mentransformasikan pengaruh-pengaruh ruang publik—termasuk kekuasaan sosial—menjadi kekuasaan politis yang dihasilkan secara komunikatif.[397]

Dengan demikian, sebagai fiksi hukum konstitusional, opini publik tidak lagi diidentikkan dengan tingkah laku aktual publik. Namun begitu, kendati opini dilekatkan kepada lembaga-lembaga politik pun (yang diabstraksikan bersama-sama dengan tingkah laku publik) tidak juga menghilangkan karakter fiktifnya. Penelitian sosial empiris akan menemui jalan buntunya kaum positivis ketika hendak menyusun definisi 'opini publik' yang tepat. Mengapa? Karena penelitian tersebut akan mengabstraksikan definisi 'opini publik' dari aspek-aspek institusionalnya, padahal tindakan yang demikian akan segera melikuidasi karakter sosio-psikologisnya.[398]

Demikianlah keutamaan pembentukan peran publik mayantara dengan melakukan penelitian sosiologis terhadap komunitas, pengambilan fokus terhadap komunitas *hacker* bukan hanya menjadi pertimbangan atas

---

[396] Jurgen Habermas, *Ruang Publik: Sebuah Kajian tentang Kategori Masyarakat Borjuis* (*Public Sphere: An Inquiry into a Category of Borgeois Society*), diterjemahkan oleh Yudi Santoso, (Yogyakarta: Kreasi Wacana, 2010), hal. 334.

[397] Budi Hardiman, *op.cit.*, hal. 148.

[398] Habermas, *op.cit.*, hal. 332.

kemampuan (*skill*) semata, akan tetapi sebagaimana dijelaskan Habermas, komunitas merupakan perluasan dari individu dan juga merupakan ruang dimana opini publik dibentuk dengan 'pengaruh'. Dan memang komunitas *hacker* dengan berbagai pertimbangan, memang memiliki pengaruh terhadap berbagai aktifitas *cyber* mayantara.

Pengaruh dan pembentukan opini publik mayantara sekiranya tidak memerlukan wadah partai politik untuk menampung aspirasi politisnya. Pada kenyataannya, UU ITE yang diusung oleh parlemen dengan pertimbangan 'pengaruh' mereka, tidak berlaku pada ruang mayantara di mana terdapat konsep lain tentang 'pengaruh'. Pengaruh mereka dalam memperjuangkan perundangan hukum pidana yang lebih responsif terhadap keadaan, semestinya melalui jalur yang terbuka dan bebas dari kepentingan politis berbagai partai politik, karena peran yang mereka ambil adalah bukan peran dalam ruang pertarungan pengaruh politis partai politik, akan tetapi lebih karena ruang publik mayantara adalah *Lebenswelt* bagi siapa saja. Maka jika perjuangan menciptakan perundangan yang lebih responsif terhadap keadaan, parlemen mesti membuka ruang yang netral yang memungkinkan bagi konsensus pencapaian kesahihan antara parlemen dan semua setiap wakil komunitas *hacker* di Nusantara, yang memiliki peran sosial terhadap 'lingkungannya'.

Selanjutnya, ketiga pertimbangan terhadap kemungkinan pelibatan *hacker* dan komunitasnya dalam penegakan hukum pidana mayantara tersebut di atas merupakan tiga aspek tindakan komunikatif yang semestinya tidak dilakukan secara bebas, karena dengan mengambil aktifis mayantara secara sembarangan untuk membantu kerja kepolisian serta kejaksaan dalam penanganan perkara, justru bisa menimbulkan keresahan lain. Oleh karenanya perlu dibentuk suatu undang-undang yang mengatur mekanisme tersebut dengan elegan.

Dengan tidak mempertimbangkan solidaritas antar-komunitas dan profesionalitas dari individu-individu yang diperbantukan dalam

penanganan perkara justru akan menimbulkan sentimen negatif terhadap pemerintah dari komunitas-komunitas lain. Perlunya komunikasi terbuka dari kedua pihak dengan deliberatif, pihak komunitas dengan pihak pemerintah yang diwakili penegak hukum maupun parlemen dalam tujuan pembentukan undang-undang yang mengajak peran serta komunitas *hacker* untuk memberikan pandangan-pandangan dan sumbang sarannya.

Sekiranya dapat didefinisikan kerjasama antara penegak hukum dengan komunitas *hacker (underground)* adalah merupakan kerjasama yang dapat memulihkan kekuatan sistem peradilan pidana untuk menjadi lebih solid dalam menangani berbagai kasus-kasus tindak pidana mayantara. Sebagaimana dijelaskan oleh M. Yahya Harahap, bahwa kegiatan "sistem peradilan pidana" didukung dan dilaksanakan "empat fungsi utama".[399]

- Fungsi Pembuatan Undang-undang (*Law Making Function*). Fungsi ini dilaksanakan oleh DPR dan Pemerintah atau badan lain berdasarkan *dlegated legislation.*
- Fungsi Penegakan Hukum (*Law Enforcement Function*). Tujuan objektif fungsi ini ditinjau dari pendekatan "tata tertib sosial" (*social order*):
  *1)* Penegakan hukum secara aktual. Meliputi: *investigation, arrest—detention, trial, punishment.*
  2) Efek "preventif" (*prefentive effect*).
- Fungsi Pemeriksaan Persidangan Pengadilan (*Function of Adjudication*). Merupakan subfungsi dari kerangka penegakan hukum yang dilaksanakan oleh Jaksa PU dan Hakim serta pejabat pengadilan terkait.
- Fungsi Memperbaiki Terpidana (*The function of correction*). Meliputi aktivitas Lembaga Pemasyarakatan, Pelayanan Sosial terkait, dan Lembaga Kesehatan Mental.

[399] M. Yahya Harahap, *Pembahasan Permasalahan dan Penerapan KUHAP: Penyidikan dan Penuntutan*, cetakan kesebelas, (Jakarta: Sinar Grafika, 2009), hal. 90-91.

Dengan mengingat kegiatan "sistem peradilan pidana" tersebut di atas, maka: *pertama*, penjelasan tanggung jawab sosial *hacker* terhadap komunitas dan ruang publik yang lebih luas dalam jangkauannya dalam melakukan sosialisasi serta menjaga solidaritas bisa jadi memberikan efek prefentif tindak pidana, setidaknya mulai dari penanaman *hacker ethics* yang lebih berpihak kepada kepentingan masyarakat luas. Maka dalam pada itu diperlukan pendekatan yang baik dari pihak-pihak penegak hukum untuk melakukan komunikasi yang baik, sehingga lebih mengutamakan kepentingan publik dan memberikan sudut pandang positif di kedua belah pihak secara timbal balik. Hal ini hanya akan terjadi saat adanya jaminan hukum yang berperan sebagai poros dan kontrol terhadap tindakan komunikatif tersebut.

*Kedua,* fungsi teknis dalam penanganan kasus-kasus tindak pidana oleh para *hacker* adalah peran dalam turut mendukung penegakan hukum "secara aktual". Setidaknya kemampuan dalam melakukan pelacakan dan pengumpulan jejak serta bukti merupakan kemampuan teknis yang lazim dipraktikkan dalam ruang lingkup komunitas dan pihak-pihak terkait yang memerlukan bantuan, potensi ini dapat dimanfaatkan. Sekiranya perlu adanya standar penanganan perkara *cybercrime* yang diatur dengan baik.

*Ketiga,* fungsi politis *hacker* dalam penyusunan undang-undang khusus cybercrime merupakan bagian dari *Law Making Function*. Dengan mempertimbangkan bahwa *hacker* tidak seutuhnya berperan politis, akan tetapi sebagaimana dukungan penjelasan Habermas pada peran ini, *hacker* memiliki 'pengaruh' dalam ruang publik sebagaimana partai-partai dalam ruang-ruang demokratis. 'Pengaruh' terhadap ruang sosial sekiranya dapat mendukung 'pengaruh' terhadap legitimasi hukum.

Di samping pihak Kepolisian secara khusus perlu memperbaiki mekanisme pelaporan atas berbagai tindak pidana mayantara demi

menjamin proses dan berjalan dengan baiknya sistem peradilan pidana,[400] yaitu dengan sistem pelaporan efektif yang mampu membantu dan mengarahkan korban kepada penanganan pertama pada insiden *cybercrime* untuk mencegak hilangnya jejak, yang tentunya diiringi dengan perunutan 'reaksi-cepat' dari kantor polisi terdekat yang sudah memiliki integrasi dengan teknisi *cyber* maupun anggota kepolisian yang berketerampilan khusus dalam hal tersebut. Terlebih lagi dan terutama dalam peran penegakan hukum aktual dalam sistem peradilan pidana, dapat dipertimbangan tentang sertifikasi semacam CEH (*Certified Ethical Hacker*), CHFI (*Computer Hacking Forensics Investigator*), dan sebagainya sebagai standarisasi kemampuan teknis *hacker* etis dan standarisasi kemampuan *cyberforensics* untuk pengumpulan alat bukti dalam proses persidangan. Dan kemudian pelatihan intern oleh pihak Kepolisian dan Kejaksaan perlu terus ditingkatkan demi meningkatkan jaminan kepastian hukum yang mendukung berbagai kegiatan ekonomis di dunia maya.[401]

Akan tetapi dari semua itu Onno W. Purbo mengingatkan bahwa, pelatihan dan sertifikasi merupakan satu hal, yang lebih penting adalah akhlak, attitude, dan perilaku. Dan beliau menambahkan bahwa semua hal itu hanya akan terlihat jika kita bergaul lebih dekat.[402] Pertimbangan untuk mengenal lebih dekat dunia *hacker* dan mengenal dengan baik personal-personalnya ada baiknya disusun suatu *"Profiling Hackers"*. Karena kritik demi perubahan sosiologis, dalam hal ini ruang sosial mayantara, perlu mendapatkan masukan tentang informasi tiap-tiap subjek pelaku sosial dan *hacker* dalam hal ini merupakan aktor sosial.

---

[400] Dalam dorongan untuk perbaikan sistem pelaporan berbagai kasus tindak pidana terdapat pertimbangan tentang dapat dihapusnya jejak oleh pelaku pidana mayantara—selama serangan serupa itu dilakukan dengan kemampuan mengakses web server, penghapusan itu dapat dilakukan dengan cepat, terlebih lagi permasalahan pemalsuan identitas yang bisa menjadikan proses pelaporan tradisional tidak lagi maksimal. Disarikan dari wawancara dengan BD, 11 April 2011.

[401] DM dalam wawancara mengingatkan tentang pentingnya pertimbangan ekonomis dalam prioritas penegakan hukum pidana mayantara. Wawancara dengan DM, 9 April 2011.

[402] Wawancara dengan Onno W. Purbo, 20 Mei 2011.

> "Logika being tidak dapat digunakan untuk memahami manusia sebab manusia terus-menerus 'menjadi' (becoming) sehingga sulit ditemukan ujung-pangkalnya. Diperlukan 'logika' lain untuk memahaminya, logika yang memungkinkan identitas dipahami sebagai sesuatu yang tetap sekaligus berubah atau berkembang."[403]

*Profiling hacker* merupakan hal penting dalam proses kritik sosial, terutama pengaruhnya terhadap penegakan hukum, *profiling* merupakan kegiatan untuk menjelaskan sosok *hacker* dalam pertimbangan psikologi naratif, dan dalam sosiologi kritis Mazhab Frankfurt peran psikoanalisa adalah penting dalam memahami ruang publik psikis. Tentang psikologi naratif juga terdapat pertimbangan filosofis yang bermanfaat dalam mengantisipasi perkembangan psikologis *hacker* secara umum, dan tentunya tindakan-tindakan potensialnya di kemudian hari. Hal ini akan memberikan langkah antisipatif yang efektif.

[403] Bagus Takwin, *Psikologi Naratif*, cet. Pertama, (Yogyakarta: Jalasutra, 2007), hal. 9.

# BAB V
# PENUTUP

## 5.1 Simpulan

1. Struktur sosial masyarakat mayantara terbentuk oleh arus informasi dan pengetahuan yang berlalu-lalang di dalam mayantara. Posisi dan peran tiap-tiap bagiannya ditentukan oleh penguasaan teknologi informasi dan kemampuannya melakukan kontrol terhadap ruang-ruang mayantara. Dalam gambaran umum adalah terdapat ruang publik mayantara sebagai bentuk utuh interaksi sosial di dalamnya, di dalam ruang publik tersebut terdapat berbagai organisasi-organisasi sosial yang menciptakan ruang-ruang komunikasi yang berupa komunitas-komunitas. Komunitas-komunitas tersebut terbentuk oleh kesamaan selera tentang informasi maupun pengetahuan secara umum, dan melaluinya tercipta interaksi secara khusus. Dalam komunitas terdapat pemimpin yang mengorganisasikan dan menengahi komunikasi setiap anggotanya, peran koordinator inilah yang menjadi agen (wakil) dari kelompoknya dalam berkomunikasi dengan ruang di luar komunitas, dikarenanya kelebihannya dalam mengelola dan melakukan kontrol terhadap komunitas. Dan dalam berbagai bentuk komunitas, komunitas *hacker* merupakan komunitas dengan kemampuan dan penguasaan atas teknologi informasi yang lebih baik daripada komunitas lain, meskipun di samping itu terdapat berbagai komunitas searah dengan penguasaan TI, akan tetapi keseriusan dan kemampuannya melakukan organisasi diri secara adaptif terhadap berbagai ancaman kejahatan maupun melakukan berbagai bentuk bantuan terhadap publik dalam permasalahan kejahatan internetlah yang menjadikannya lebih dari komunitas lain. Sebagaimana komunitas-komunitas lain, dalam komunitas *hacker* terdapat pula pemimpin komunitas yang juga berperan sebagai kontrol terhadap komunitasnya.

   Dengan memperhatikan demikian pentingnya posisi komunitas dalam penegakan hukum dengan pertimbangan organisasi diri dan sistem di

dalamnya, terutama komunitas TI yang menguasai ruang komunikasi dengan lebih baik, maka kerjasama antara agen-agen (pemimpin komunitas) sosial mayantara, terutama dari komunitas yang memiliki kemampuan teknis lebih baik dalam menghadapi permasalahan pidana di mayantara, sangat penting. Dan hal ini untuk efektifnya penegakan hukum pidana mayantara, diperlukan juga pemahaman terhadap struktur sosial masyarakat mayantara oleh penegak hukum.

Ruang publik mayantara, saat hukum tidak berjalan efektif, memiliki cara mengatasi berbagai kasus, yang keterkaitannya dengan kriminal publik yang menjadikannya masuk dalam definisi tindak pidana mayantara. Kekuatan informasi dan pengetahuan memunculkan cara-cara interaktif menyelesaikan kasus-kasus tindak kejahatan mayantara, dengan memanfaatkan keahlian teknis permasalahan diselesaikan dengan landasan solidaritas, dan pengetahuan tehnik di dalam mayantara mengalami pemurnian terus-menerus. Dengan pengetahuan dan penguasaan tehnik *cyber* pulalah keamanan dan kontrol untuk kenyamanan publik dalam beraktifitas dalam mayantara terus dikembangkan. Dalam komunitaslah mekanisme yang sedemikian rupa terjadi dan berlangsung dengan baik secara berkelanjutan seiring dengan perkembangan teknologi, pengetahuan, dan kemuslihatan ancaman kejahatan. Penelitian terhadap aktifitas *cybercommunity* yang memberikan gambaran yang baik terhadap peran agen-agen (aktor) sosial dalam mempertahankan stabilitas ruang mayantara, dan dalam komunitas *hacker* maupun *hacker underground*-lah teori sosiologi hukum dengan panduan diskursus Habermas menemui gambaran yang jelas.

2. Keutamaan penelitian sosial dalam memahami permasalahan penegakan hukum pidana mayantara adalah kemampuannya dalam mengamati lebih jauh aspek-aspek sosio-psikologis ruang dan individu-individu mayantara. Dan peran sosiologi kritis Habermas juga mendukung pemahaman sosio-psikologis, dan tidak terbentur atau terhenti pada aspek-aspek institusional pembentukan opini publik saja. Opini publik dengan penelitian sosiologis

mampu mengurai tingkatan-tingkatan sosial dan karakter psikologisnya terhadap ruang publik. Pembentukan opini publik juga ditentukan oleh pengaruh-pengaruh sosial, dan pengaruh-pengaruh tersebut di dalam mayantara, yang menjadikan pengetahuan dan keahlian sebagai kekuatan, memosisikan para profesional TI (*hacker*) sebagai pihak yang berpengaruh dalam menentukan kebijakan, oleh karenanya pendekatan dan pemanfaatan peran para profesional tersebut adalah utama. Dan dengan demikianlah upaya-upaya yang selalu bersinggungan dengan masyarakat, terutama hukum pidana, semestinya memperhatikan kajian sosiologi hukum agar kebijakan-kebijakan hukum yang dijalankan dapat berjalan dengan baik dan senantiasa berada dalam jalur historis perubahan sosial.

Peraturan perundang-undangan di Indonesia terlihat masih kurang menyerap perubahan sosial di dalam mayantara, dikarenakan masih terbatasnya pemahaman terhadap mayantara dan dinamika sosialnya. Penerapan delik-delik yang limitatif dan masih sempit lingkupnya dalam UU ITE yang dimaksudkan untuk menjamin kepastian hukum dalam mayantara dinilai masih tidak memadai. Pembatasan dalam beberapa pasal tentang rumusan delik terasa masih kurang untuk dapat menjangkau luasnya aktivitas mayantara dan berbagai kemungkinan tindak pidana yang mungkin terjadi di dalamnya. Di samping itu, tidak tersosialisasikannya dengan baik suatu peraturan perundang-undangan dalam mayantara sedangkan hal itu berkaitan erat dengan hajat hidup orang banyak dalam mayantara, justru menjadikannya tidak efektif, bahkan sama sekali tidak dikenali oleh para aktivis mayantara.

Ruang publik mengalami perubahan dan perkembangan dalam mayantara dengan cepat. Seiring dengan makin kompleksnya ruang publik maka akan semakin banyak kotak-kotak dalam ruang mayantara yang semakin melemahkan sistem otoritas. Di samping itu penegakan hukum tidak diiringi dengan pemahaman karakter ruang publik mayantara dengan baik, hal ini berimbas pada surutnya legitimasi hukum. Di lain pihak, komunitas-komunitas *hacker* (*underground*) menjadi ruang diskusi dan pertukaran

pengetahuan tentang teknis keahlian mayantara, pengetahuan dalam hal ini selalu memiliki potensi positif (konstruktif) maupun negatif (destruktif) terhadap tertib-hidup ruang mayantara. Hal inilah yang semestinya dapat diserap negara dalam menetapkan suatu perundang-undangan yang terkait erat dengan tindak pidana mayantara, dengan senantiasa memperbaiki hubungan dengan publik mayantara dan menciptakan ruang komunikasi aktif untuk saling koreksi dan memberi kritik yang membangun, sehingga sosialisasi dan konsensus tentang bentuk hukum pidana mayantara yang legitim dapat menemukan kesahihannya.

3. Dalam menanggulangi kejahatan di setiap negara memerlukan kerjasama antara para penegak hukum dengan masyarakat. Tanpa adanya kerjasama yang baik bisa mengakibatkan kegagalan penegakan hukum. Dalam pikiran Hobessian memandang bahwa demi ketertiban di dalam masyarakat semua orang di dalam negara harus tunduk pada negara, masyarakat tenggelam dalam negara, dan tidak ada lagi ruang publik. Akan tetapi kenyataannya ruang publik mayantara memberikan kisah yang berbeda di Indonesia, tidak ada kekuatan hukum yang absolut di dalam masyarakat, dan saat hukum tidak berjalan efektif masyarakat dengan mekanisme di dalamnyalah yang mengarahkan ruang-ruang publik menjadi tertib. Minimnya kemampuan hukum secara riil menyentuh sudut-sudut permasalahan *cybercrime* yang terus berkembang menjadikan surutnya legitimasi hukum dalam mayantara. Legitimasi merupakan akar kepercayaan masyarakat kepada hukum dan penyelesaian permasalahan hukum pidana (terutama) yang mereka hadapi di dalam mayantara. Akan tetapi minimnya kemampuan penegak hukum dalam melaksanakan perannya dalam mayantara menjadikan merosotnya kepercayaan publik, bukan semata karena kurangnya penanganan terhadap kasus-kasus *cybercrime* yang dapat dilihat dari besarnya jumlah korban jika dibandingkan dengan kasus yang diproses di pengadilan, akan tetapi sistem pelaporan, yang merupakan titik awal sebuah kasus diproses secara hukum, yang kurang memadai secara teknis dapat memunculkan keraguan. Dengan

demikian banyaknya kekurangan maka semakin banyak peranan berbagai pihak dalam ruang mayantara yang dibutuhkan untuk menciptakan legitimasi hukum pidana dalam ruang publik mayantara.

Optimisme para aktivis teknologi informatika terhadap tegaknya hukum yang efektif merupakan pertimbangan objektif dengan kemampuan mereka dalam mengamati mekanisme mayantara yang tidak selamanya tak mungkin diatur. Dengan pemahaman dan kemampuan teknis yang baik, serta ruang lingkupnya dalam melakukan tindakan komunikatif yang luas, maka *hacker* dan profesional merupakan aktor-aktor sosial yang dapat diajak bekerjasama dalam melakukan upaya-upaya pemulihan legitimasi hukum, dan secara khusus membantu dalam mengefektifkan ruang-ruang komunikatif antara penegak hukum dengan publik mayantara.

Untuk menciptakan legitimasi hukum perlu melalu beberapa tahap. Perlu dibuka ruang-ruang komunikasi sehingga antara pihak aktifis mayantara dengan pemerintah sebagai pihak penentu kebijakan, komunikasi ini harus dibuat sedemikian rupa sehingga masing-masing pihak dapat menyampaikan klaim-klaim kesahihan tentang pandangan masing-masing. Kemudian akan menuntun kepada konsensus yang membimbing kepada pembentukan kebijakan-kebijakan penegakan hukum pidana yang sesuai dengan pemahaman dan pengamatan teknis para profesional komunitas *cyber* (*hacker*). Dan terbukanya kemungkinan konsensus tidaklah mungkin tanpa adanya pemahaman yang baik oleh satu pihak terhadap pihak lainnya dan sebaliknya. Karena pengaruh media yang memberitakan dengan tidak selamanya benar tentang komunitas hacker, oleh karenanya perlu adanya kajian terhadap komunitas *hacker* dengan lebih baik, agar proses komunikasi yang berkelanjutan dengan tujuan pemulihan ketertiban bersama dapat terwujud dengan baik.

Untuk membangkitkan legitimasi hukum, maka komunikasi dan koreksi antara kedua belah pihak perlu dijaga stabilitasnya dan perlu dijaga batasan-batasannya. Dalam hal ini, seharusnya mekanisme tindakan komunikatif

antara para agen sosial mayantara dengan pemegang kekuasaan (otoritas) mengambil peran hukum sebagai poros yang sekaligus memiliki peran kontrol demi lancarnya arus pertukaran tindakan komunikatif dan tindakan strategis antara profesional TI mayantara (*hacker*) dengan pemerintah. Yang selanjutnya dalam upaya kontrol yang berkelanjutan hal ini harus senantiasa dijaga dan dilanjutkan antara para *hacker* sebagai agen publik mayantara dengan penegak hukum sebagai wakil pemegang otoritas hukum, dalam melakukan penegakan hukum yang berkelanjutan.

Pemanfaatan peran agen sosial mayantara maupun komunitas-komunitas mayantara secara luas, sebagai simpul-simpul 'pengaruh' sosial mayantara, tidak hanya sebatas pada pembentukan saling pemahaman dan pembentukan kebijakan-kebijakan yang berpengaruh terhadap ruang publik mayantara. Akan tetapi peran mereka juga dapat meliputi wilayah aktual penegakan hukum pidana mayantara. Peranan aktual berarti adalah peranan yang meliputi ruang lingkup kerja kepolisian, kejaksaan, atau hingga pengadilan, peranan ini berkaitan erat dengan hal-hal teknis seperti pelacakan pelaku tindak pidana, penanganan barang bukti, hingga verifikasi *digital proof* kepada *evidence* dalam persidangan. Sedangkan disamping peran aktual terdapat pula peran preventif, peran preventif ini harus senantiasa diterapkan ke dalam ruang-ruang komunitas mereka masing-masing. Sehingga peningkatan jumlah tindak pidana dapat ditekan, dan dengan ditanganinya kasus-kasus tindak pidana mayantara oleh ahlinya (para *hacker*)—terutama ketika para penegak hukum belum memiliki kemampuan baik kuantitas dan kualitas dalam menangani dengan baik bentuk-bentuk permasalahan tindak pidana mayantara—maka tingkat resiko dalam melakukan tindak pidana mayantara akan meningkat, dan juga maningkatkan pertimbangan pelaku kejahatan terhadap kemungkinan tertangkap dan dipidana.

4. Mayantara merupakan ruang global yang memungkinkan kejahatan tidak hanya hadir di satu wilayah dan dalam satu waktu tertentu, kemudahan seorang pelaku kejahatan dalam melakukan tindak pidana tergantung pada

keahliannya dan juga pada kelemahan sistem yang diserang. Aneka macam tindak kejahatan mayantara dilakukan dengan keahlian, sedangkan penegak hukum masih minim keahlian dan hanya segelintir dari mereka yang mampu melakukan dengan baik tindakan-tindakan yang tepat untuk mencegah dan memproses tindak pidana mayantara. Para pelaku potensial terhadap tindak pidana mayantara tersebar di setiap penjuru dunia, dan dengan semakin meningkatnya komunitas *hacker* di dunia maya menjadikan pertumbuhan jumlah *potential offender* semakin meningkat. Dari hasil penelitian terlihat bahwa: *pertama*, tingkat kriminalitas mayantara di Indonesia sangat tinggi, dengan keluasan ruang untuk mempelajari berbagai bentuk *cybercrime; kedua*, dengan mempertimbangkan minimnya peran kontrol hukum, serta dukungan kajian kriminologi terhadap keadaan tersebut, maka potensi peningkatan masih sangat besar. Kedua hal tersebutlah yang menonjol sebagai tantangan besar dalam penegakan hukum selama ini.

Ketika penegakan hukum masih minim tingginya ancaman keselamatan dalam ruang mayantara menjadi tanggung jawab para profesional yang ada dalam komunitas-komunitas, dan dalam komunitaslah para korban mendapatkan ruang komunikasi untuk menyelesaikan masalah kejahatan yang ia alami. Dalam komunitas para profesional yang memiliki keahlian dalam teknologi informatika melakukan regenerasi dan menanamkan etika-etika. Saat hukum belum berakar kuat di dalam masyarakat mayantara, saat itulah norma-norma yang ditanamkan akan menciptakan para profesional yang beretika, dan para profesional ini memiliki kecenderungan mampu menghargai milik orang lain saat solidaritas dan penanam etika di dalam komunitas juga berjalan dengan kuat. Maka pada saat yang sama komunitas membantu lingkungannya untuk semakin aman dan nyaman dalam beraktifitas di mayantara, saat itu pula pencegahan dari dalam terus-menerus dilakukan.

Dan salah satu cara terbaik untuk mengatasinya adalah dengan membuka ruang komunikasi yang memungkinkan pihak penegak hukum serta para agen sosial mayantara yang memiliki kompetensi terhadap penanganan

berbagai kemungkinan tindak pidana mayantara. Sehingga hukum dapat menyerap perubahan sosial dan beradaptasi, dan publik mendapatkan perlindungan hukum yang sesuai dan pasti.

## 5.2 Saran-saran

1. Dalam pembentukan undang-undang yang berkaitan dengan perlu ditingkatkannya pemahaman para pembentuk kebijakan dalam memandang ruang mayantara dan segala resikonya, sehingga dapat dilahirkan berbagai kebijakan yang sesuai tujuan dan tepat sasaran. Hal ini untuk menghindari kesalahpahaman dan tidak efektifnya penerapan kebijakan hukum pidana mayantara, dan menghindari permasalahan penegakan hukum pidana. Sebab tidak legitimnya hukum bergantung pada objektifitas hukum tersebut, jika permasalahan definisi masih menjadi kendala maka penerapannya akan menjadi lebih sulit lagi. Oleh karenanya dalam penyusunan kebijakan-kebijakan terkait perlu melibatkan para aktor sosial ruang publik mayantara.
2. Dalam membuat sistem pelaporan atas peristiwa pidana hendaknya pemerintah melalui situs-situs Kepolisian membuat sistem pelaporan yang lebih aman dan terarah, hal ini mempertimbangkan tiga hal: a) kemudahan masyarakat untuk melaporkan permasalahan pidana mayantara yang ia alami, hal ini seringkali membutuhkan tindakan cepat-tanggap karena dalam pidana mayantara terkadang pelaku mampu menghapus jejaknya. Oleh karenanya perlu kerjasama dengan aktifis *cyber* dan terus melatih anggota institusi penegak hukum untuk mampu menanganinya; b) kemudahan dan keterarahan laporan yang tidak hanya sekedar mengisi form kosong sederhana, tetapi dengan memfokuskan permasalahan pidana yang dihadapi oleh korban, akan membantu korban dalam memahami situasinya karena tindak pidana mayantara bukanlah situasi alamiah yang bisa diantasipasi secara manusiawi akan tetapi butuh kemampuan teknis yang tidak biasa. Dan dengan bantuan pemilahan itulah semestinya mekanisme pelaporan juga memberikan saran untuk menghadapi situasi tertentu demi menghindari resiko yang lebih besar

dan bisa jadi untuk menghindari hilangnya barang bukti; c) dengan pelaporan yang aman dan terarah maka akan terdapat jaminan proses dilanjutkan kepada alur peradilan (penyelidikan, penyidikan, persidangan, pemidanaan). Dan dari kejelasan proses tersebut maka kepolisian bisa mendapatkan data pasti tentang banyaknya kasus perkara pidana yang dilaporkan, perkara yang cukup bukti untuk diajukan di persidangan, dan perkara yang diputus pengadilan.

3. Untuk menciptakan pemahaman dengan para *hacker*, demi terbukanya segala kemungkinan terciptanya penegakan hukum pidana yang lebih baik dan demi meningkatnya legitimasi hukum di dalam ruang publik, maka diperlukan studi/kajian yang lebih dalam dan lebih baik terhadap para *hacker*. Sekaligus hal ini bertujuan untuk mendefinisikan *hacker* dalam hukum, atau untuk mengelompokkannya secara spesifik dalam stratifikasi yang jelas. Sehingga peran 'pengaruh' dan peran sebagai aktor sosial sekaligus agen perubahan dalam ruang publik mayantara dapat diterapkan dengan lebih baik dan lebih berkesesuaian. Dalam terminologi yang lebih khas, perlu diadakannya riset untuk melakukan *"Profiling Hackers"*, profiling ini bermanfaat untuk mengenali hacker sebagai individu maupun sebagai bagian dari komunitasnya dan masyarakat, sehingga pemahaman yang lebih baik terhadap dapat memberikan cara pandang serta penanganan permasalahan di dalamnya dengan lebih baik pula. Dan dengan saling memahami antara dua belah pihak, penegak hukum dan komunitas hacker, akan membuka ruang-ruang dialog yang lebih positif untuk menciptakan konsensus dalam penanganan permasalahan tindak pidana mayantara.

# DAFTAR PUSTAKA

**Buku:**


Adler, Freda; Gerhard O.W. Mueller; dan William S. Laufer. *Criminology*. New York: McGraw-Hill, 1991.

Akers, Ronald L. *Criminological Theories*. Chicago: Fitzroy Dearborn Publisher, 1999.

Anggara; Supriyadi W.E; dan Ririn Sjafriani. *Kontroversi Undang-undang ITE: Menggugat Pencemaran Nama Baik di Ranah Maya*. Jakarta: Degraf, 2010.

Arif, Barda Nawawi, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*. Jakarta: Raja Grafindo Perkasa, 2007.

----------, *Kebijakan Legislatif dalam Penanggulangan Kejahatan dengan Pidana Penjara*. Yogyakarta: Genta Publishing, 2010.

----------, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta: Rajawali Press, 2006.

Bailei, James, *Hume on Morality*, London: Routledge, 2000.

Burke, Peter. *Sejarah dan Teori Sosial*. Jakarta: Yayasan Obor Indonesia, 2001.

Camus, Albert. *The Rebel*. Middlesex: Penguin Books, 1974.

Chiesa, Raoul, *Profiling Hackers: The Science of Criminal Profiling as Applied to The World of Hacking*, New York: Auerbach, 2009.

Creswell, John W., *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, second edition, London: Sage Publication, 2003.

Freud, Sigmund. *Memperkenalkan Psikoanalisa: lima ceramah (Ueber Psychoanalyse, Funf Vorlesungen)*, diterjemahkan oleh K. Bertens, Jakarta: Gramedia, 1987.

Fromm, Erich. *Memilik dan Menjadi: Tentang Dua Modus Eksistensi*. Jakarta: LP3ES, 1988.

Friedman, Lawrence M. *Sistem Hukum: Perspektif Ilmu Sosial*, Bandung: Nusamedia, 2009.

Mudiardjo, Rapin. "Kajian Aspek Pidana", dalam *Pengantar Hukum Telematika: Suatu Kajian Kompilasi*, Editor Edmon Makarim. Jakarta: Rajagrafindo Persada, 2005, hal. 417-446.

Garner, Bryan A. *et al*. *Black's Law Dictionary*, 9th ed. Minnesota: Thomson Reuters, 2009.

Ghosh, Sumit, ed. *Cybercrime: A Multidisciplinary Analysis*. Heidelberg: Springer, 2010.

Gibson, William, *Neuromancer* (*Neuromancer*), diterjemahkan oleh Eman Prihatmo, Yogyakarta: Jalasutra, 2010.

Giddens, Anthony, *Teori Strukturasi: Dasar-Dasar Pembentukan Struktur Sosial Masyarakat* (*The Constitution of Society: Outline of the Theory of Structuration*), diterjemahkan oleh Maufur dan Daryatno,Yogyakarta: Pustaka Pelajar, 2010.

----------, *Konsekuensi-Konsekuensi Modernitas (The Consequences of Modernity)*, diterjemahkan oleh Nurhadi, Cet. Kedua. Yogyakarta: Kreasi Wacana, 2009.

Goldstein, Emmanuel. *The Best of 2600: A Hacker Oddyssey*. Indianapolis: Willey Publishing, 2008.

Habermas, Jurgen, *Krisis Legitimasi*, Yogyakarta: Qalam, 2004.

----------, *The Structural Transformation of The Public Sphere: An Inquiry into a Category of Bourgeois Society*. Cambridge: MIT Press, 1993.

----------, *Teori Tindakan Komunikatif (Buku Satu): Rasio dan Rasionalisasi Masyarakat*. Yogyakarta: Kreasi Wacana, 2009.

----------, *Ruang Publik: Sebuah Kajian tentang Kategori Masyarakat Borjuis*, Cet. Ketiga. Yogyakarta: Keasi Wacana, 2010.

----------, *Teori Tindakan Komunikatif, (Buku Kedua): Kritik atas Rasio Fungsionalisasi*, Cet. Pertama. Yogyakarta: Kreasi Wacana, 2007.

Hardiman, F. Budi. *Filsafat Fragmentaris*. Yogyakarta: Kanisius, 2007.

----------, *Filsafat Modern*. Jakarta: Gramedia, 2007.

----------, *Kritik Ideologi: Menyingkap Kepentingan Pengetahuan Bersama Jurgen Habermas*, Yogyakarta: Buku Baik, 2003.

----------, *Demokrasi Deliberatif: Menimbang 'Negara Hukum' dan 'Ruang Publik' dalam Teori Diskursus Jurgen Habermas*, Yogyakarta: Kanisius, 2009.

----------, *Menuju Masyarakat Komunikatif: Ilmu, Masyarakat, Politik dan Postmodernisme Menurut Jurgen Habermas*, Yogyakarta: Kanisius, 2009.

----------, *Heidegger dan Mistik Keseharian.* Jakarta: Kepustakaan Populer Gramedia (KPG), 2008.

----------, ed., *Ruang Publik*, Yogyakarta: Kanisius, 2010.

----------, *Memahami Negativitas: Diskursus tentang Massa, Teror, dan Trauma.* Jakarta: Kompas, 2005.

Hart, H.L.A., *Konsep Hukum*, Bandung: Nusa Media, 2009.

Harahap, M. Yahya. *Pembahasan Permasalahan dan Penerapan KUHAP: Penyidikan dan Penuntutan*, Cet. Kesebelas. Jakarta: Sinar Grafika, 2009.

Hazlitt, Henry. *Dasar-dasar Moralitas*. Yogyakarta: Pustaka Pelajar, 2003.

Hebdige, Dick. *Subculture: The Meaning of Style*. London: Routledge, 1979.

Hegel, G.W.F. *Filsafat Sejarah*. Yogyakarta: Pustaka Pelajar, 2001.

Holten, N. Gary dan Lawson L. Lamar, *The Criminal Courts*. New York: McGraw-Hill, 1991.

Hornby, AS. *Oxford Advanced Learner's Dictionary of Current English*, Oxford: Oxford University Press, 1987.

Ibrahim, Johnny, *Teori dan Metode Penelitian Hukum Normatif*, Malang: Bayumedia Publishing, 2006.

Irianto, Sulistyowati & Shidarta, *Metode Penelitian Hukum: Konstelasi dan Refleksi*, Jakarta: Yayasan Obor Indonesia-JHMP FHUI, 2009.

Jay, Martin. *The Dialectical Imagination* (A History of Frankfurt School and The Institute of Social Research 1923-1950). London: Heinemann Educational Book Ltd, 1973.

Kipper, Gregory, *Wireless Crime and Forensic Investigation*, New York: Auerbach, 2007.

Levy, Steven. *Hackers: Heroes of The Computer Revolution.* New York: Delta Publishing, 1994.

Makarim, Edmon, *Himpunan Peraturan Perundang-Undangan Telematika*, Jakarta: Rajawali Press-Badan Penerbit FHUI, 2005.

Milovanovic, Dragan. *A Primer in the Sociology of Law*. New York: Harrow and Heston, 1994.

Mohay, George M. *Computer and Intrusion Forensics*. Massachusett: Artech, 2003.

Nonet, Philippe dan Philip Selznick, *Hukum Responsif* (*Law and Society in Transition: Toward Responsive Law*), diterjemahkan oleh Raisul Muttaqien, Cet. Kelima. Bandung: Nusamedia, 2010.

Packer, Herbert L., *The Limit of* Criminal *Sanction*, Stanford: Stanford University Press, 1968.

Pangaribuan, Luhut M. P. *Lay Judges & Hakim Ad Hoc*, Jakarta: Program Pascasarjana Fakultas Hukum Universitas Indonesia, 2009.

Piliang, Yasraf Amir. *Post-Realitas: Realitas Kebudayaan dalam Era Post-Metafisika.* Yogyakarta: Jalasutra, 2010.

Purbo, Onno W. *Filosofi Naif Kehidupan Dunia Cyber*. Jakarta: Republika, 2003.

Rawls, John, *Teori Keadilan* (*A Theory of Justice*), diterjemahkan oleh Uzair Fauzan dan Heru Prasetyo, cet. Pertama, Yogyakarta: Pustaka Pelajar, 2006.

Reyes, Anthony, *et al*. *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors*. Massachusett: Syngress Publising, 2007.

----------, *et al*. *The Best Damn Cybercrime and Digital Forensics Book Period*. Massachusett: Syngress Publising, 2007.

Rahardjo, Satjipto, *Hukum Progesif*. Yogyakarta: Genta, 2009.

----------, *Hukum dan Perubahan Sosial*. Yogyakarta: Genta, 2009.

----------, *Penegakan Hukum Progresif*. Jakarta: Kompas, 2010.

----------, *Penegakan Hukum: Suatu Tinjauan Sosiologis*, Yogyakarta: Genta Publishing, 2009.

Reksodiputro, Mardjono. *Kriminologi dan Sistem Peradilan Pidana, Kumpulan Karangan Buku Kedua*. Jakarta: Pusat Pelayanan Keadilan dan Pengabdian Hukum Universitas Indonesia, 2007.

Remmelink, Jan, *Hukum Pidana* (*Inleiding tot de Studie van het Nederlanse Strafrecht*), diterjemahkan oleh Tristam Pascal Moeliono, Jakarta: Gramedia, 2003.

Ritzer, George & Goodman, Douglas J., *Teori Sosiologi Modern* (*Modern Sociological Theory*), diterjemahkan oleh Alimandan, Cet. Keenam, Jakarta: Kencana, 2010.

Rogers, Marcus K. "The Psyche of Cybercriminals: A Psychosocial Perspective", dalam *Cybercrime: A Multidisciplinary Analysis*, edited by Sumit Ghosh, Elliot Turrini. Heidelberg: Springer, 2010, hal. 217-235.

Schell, Bernadette. *Webster's New World Hacker Dictionary*. Indianapolis Willey Publishing, 2006.

Shariff, Shaheen. *Confronting Cyber-Bullying*. Cambridge: Cambridge University Press, 2009.

Shinder, Debra Littlejohn, *Scene of the Cybercrime: Computer Forensics Handbook*. Massachusett: Syngress Publishing, 2002.

Sindhunata. *Dilema Usaha Manusia Rasional*. Jakarta: Gramedia, 1982.

Soekanto, Soerjono, *Faktor-faktor yang Mempengaruhi Penegakan Hukum*, Jakarta: Rajawali Press, 2010.

Strauss, Anselm & Corbin, Juliet, *Dasar-Dasar Penelitian Kualitatif*, Yogyakarta: Pustaka Pelajar, 2003.

Supelli, Karlina. "Ruang Publik Dunia Maya" dalam *Ruang Publik*, diedit oleh F. Budi Hardiman, Yogyakarta: Kanisius, 2010.

Suseno, Franz Magnis, *Pemikiran Karl Marx*. Jakarta: Gramedia, 2001.

----------, *Filsafat Sebagai Ilmu Kritis*. Yogyakarta: Kanisius, 2001.

Takwin, Bagus. *Psikologi Naratif*, Yogyakarta: Jalasutra, 2007.

Taryadi, Alfons. *Epistemologi Pemecahan Masalah*. Jakarta: Gramedia, 1991.

Thomas, Douglas. *Hacker Culture*. Minneapolis: University of Minnesota Press, 2002.

Vago, Steven. *Law and Society*. New Jersey: Prentice Hall, 1991.

Wall, David S., ed. *Crime and The Internet*. New York: Routledge, 2001.

Yar, Majid. *Cybercrime and Society*. London: Sage Publication, 2006.

**Tesis, Disertasi, Makalah dan Sumber yang Tidak Diterbitkan:**

Golose, Petrus Reinhard, "Manajemen Penyidikan Tindak Pidana *Hacking*. Studi Kasus: Penyidikan Tindak Pidana Hacking website Partai Golkar Oleh Unit V IT & *Cybercrime* Bareskrim Polri", Disertasi Kajian Ilmu Kepolisian, Jakarta: Universitas Indonesia, 2008.

**Artikel, Koran, dan Majalah:**

Suseno, Franz Magnis. *"75 Tahun Jurgen Habermas"*, dalam Basis (Edisi 75 tahun Jurgen Habermas), No. 11-12, tahun ke-53, November-Desember 2004.

McAfee North America Criminology Report; Organized Crime and the Internet 2007.

Juliawan, B. Hari, *Ruang Publik Habermas: Solidaritas Tanpa Intimitas*, dalam Basis (Edisi 75 tahun Jurgen Habermas), No. 11-12, tahun ke-53, November-Desember 2004, hal. 38-39.

**Jurnal:**

Northwestern University Law Review, Vol. 83, Northwest University, School of Law, 1989.

Jentera, Ruang dan Hukum, Edisi 21-Tahun VI, Januari-April, Jentera: Jakarta 2011.

Jurnal Filsafat Driyarkara, Kebaruan Teori Sistem Niklas Luhmann, Driyarkara: Jakarta, Th. XXIX No. 3, 2008.

**Peraturan Perundang-undangan:**

Indonesia, *Wetboek van Strafrecht* (WvS), Kitab Undang-Undang Hukum Pidana (KUHP), *staatsblad* Tahun 1915, 15 Oktober 1915, No. 732.

Indonesia, Undang-Undang Tentang Hukum Acara Pidana (*KUHAP*). UU No. 8 Tahun 1981, LN. No. 76 Tahun 1981, TLN. 3209.

Indonesia, Undang-Undang tentang Informasi dan Transaksi Elektronik, UU No. 11 Tahun 2008, LN No. 58 Tahun 2008, TLN No. 4843.

**Internet:**

http://Zone-H.org/

http://www.isoc.org/internet/history/brief.shtml#Commercialization.

http://teknologi.vivanews.com/news/read/168958-2009-jadi-tonggak-sejarah-internet-indonesia

http://www.computerhistory.org/internet_history/

http://www.isoc.org/internet/history/brief.shtml#Community

http://www.isoc.org/internet/history/brief.shtml#Commercialization

http://opensource.telkomspeedy.com/wiki/index.php/Hacker

http://www.newworldencyclopedia.org/entry/Jean_Genet

http://opensource.telkomspeedy.com/wiki/index.php/Filosofy:_Etika_Hacker

http://www.eccouncil.org/about_us.aspx

http://www.guardian.co.uk/uk/2011/may/30/military-cyberwar-offensive

http://www.eccouncil.org/training/professional_series/ceh_course_outline.aspx

http://www.eccouncil.org/training/professional_series/chfi_course_outline.aspx

http://opensource.telkomspeedy.com/wiki/index.php/Komunitas_Underground_Indonesia_2006

http://www.detikinet.com/read/2010/10/14/163749/1465203/404/forum-hacker-cisadane-nama-seram-dengan-kegiatan-positif

http://teknologi.vivanews.com/news/read/168958-2009-jadi-tonggak-sejarah-internet-indonesia

http://www.takedown.com/

http://www.takedown.com/evidence/index.html

http://www.imdb.com/title/tt0159784/

http://www.imdb.com/title/tt0309614/

http://www.2600.com/news/view/article/2038

http://opensource.telkomspeedy.com/wiki/index.php/Phising

http://www.gartner.com/technology/home.jsp

http://www.antiphishing.org/

http://opensource.telkomspeedy.com/wiki/index.php/Surat_Steven_Haryanto_ke_BCA_6_Juni_2001

http://kambing.ui.ac.id/bebas/v09/onno-ind-1/network/network-security/ppt-situs-klikbca-palsu-06-2001.ppt

http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism/

http://www.research.ibm.com/antivirus/SciPapers/Gordon/GenericVirusWriter.html

http://zone-h.org

http://zone-ar.com

http://www.antiphishing.org/

http://www.internetidentity.com

http://www.internetidentity.com/images/stories/docs/phishing_trends_report_q2-2009_by_internet_identity.pdf

http://apwg.org/reports/APWG_GlobalPhishingSurvey_2H2010.pdf

http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html

http://zone-h.org/news/id/4737. 6 Januari 2011.

http://www.guardchild.com/statistics/

http://www.zone-h.org/stats/notifier

http://www.oversecurity.net/2010/12/01/web-hacking-statistiche-2010-1%C2%B0-puntata-da-dove-originano-gli-attacchi-globali/

http://www.ic3.gov/media/annualreports.aspx

http://www.pandi.or.id/

http://www.polri.go.id/laporan-all/lpm/adu/

http://www.interpol.go.id/id/kejahatan-transnasional/kejahatan-dunia-maya

http://www.kominfo.go.id/

http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf.

http://nasional.kompas.com/read/2009/03/25/18505497/Cyber.Crime..Indonesia.Tertinggi.di.Dunia