

**TINJAUAN YURIDIS TINDAK PIDANA *CYBER CRIME*  
DI INDONESIA**

*Skripsi*

*Diajukan untuk Memenuhi Syarat Guna Memperoleh Gelar Sarjana Hukum (S.H)  
Pada Program Studi Hukum Tata Negara Fakultas Syariah  
Institut Agama Islam Negeri Palopo.*



**IAIN PALOPO**

Oleh:

**SRIWULAN**

19 0302 0080

**PROGRAM STUDI HUKUM TATA NEGARA  
FAKULTAS SYARIAH  
INSTITUT AGAMA ISLAM NEGERI PALOPO  
2023**

**TINJAUAN YURIDIS TINDAK PIDANA *CYBER CRIME*  
DI INDONESIA**

*Skripsi*

*Diajukan untuk Memenuhi Syarat Guna Memperoleh Gelar Sarjana Hukum (S.H)  
Pada Program Studi Hukum Tata Negara Fakultas Syariah  
Institut Agama Islam Negeri Palopo.*



**IAIN PALOPO**

Oleh:

**SRIWULAN**

19 0302 0080

Pembimbing :

**1. Dr. Abdain, S.Ag.,M.HI.**

**2. Firmansyah,S.Pd., S.H.,M.H.**

**PROGRAM STUDI HUKUM TATA NEGARA  
FAKULTAS SYARIAH  
INSTITUT AGAMA ISLAM NEGERI PALOPO**

**2023**

## HALAMAN PERNYATAAN KEASLIAN

Saya yang bertandatangan di bawah ini:

Nama : Sriwulan  
NIM : 19 0302 0080  
Fakultas : Syariah  
Program Studi : Hukum Tata Negara (*Siyasah*)

menyatakan dengan sebenarnya bahwa:

1. Skripsi ini merupakan hasil karya saya sendiri, bukan plagiasi atau duplikasi dari tulisan/karya orang lain yang saya akui sebagai tulisan atau pikiran saya sendiri,
2. Seluruh bagian dari Skripsi ini adalah karya saya sendiri selain kutipan yang ditunjukkan sumbernya. Segala kekeliruan atau kesalahan yang ada di dalamnya adalah tanggungjawab saya.

Bilamana di kemudian hari pernyataan ini tidak benar, maka saya bersedia menerima sanksi administratif atas perbuatan tersebut dan gelar akademik yang saya peroleh karenanya dibatalkan.

Demikian pernyataan ini dibuat untuk dipergunakan sebagaimana mestinya.

Palopo, 4 September 2023

Yang membuat pernyataan,



  
Sriwulan  
NIM 19 0302 0080

## HALAMAN PENGESAHAN

Skripsi berjudul **Tinjauan Yuridis Tindak Pidana Cyber Crime di Indonesia** yang ditulis oleh Sriwulan Nomor Induk Mahasiswa (NIM) 1903020080, Mahasiswa Program Studi Hukum Tata Negara (*Siyasah*) Fakultas Syariah Institut Agama Islam Negeri Palopo, yang telah dimunaqasyahkan pada hari Selasa, Tanggal 05 September 2023 M, bertepatan dengan 19 Shafar 1445 H, telah diperbaiki sesuai catatan dan permintaan Tim Penguji, dan diterima sebagai syarat meraih gelar Sarjana Hukum (S.H).

Palopo, 05 September 2023

### TIM PENGUJI

1. Dr. Muhammad Tahmid Nur, M.Ag. Ketua Sidang (.....)
2. Dr. H. Haris Kulle, Lc., M.Ag. Sekretaris Sidang (.....)
3. Dr. Rahmawati, M.Ag. Penguji I (.....)
4. Wawan Haryanto, S.H., M.H. Penguji II (.....)
5. Dr. Abdain, S.Ag., M.HI. Pembimbing I (.....)
6. Firmansyah, S.Pd., S.H., M.H. Pembimbing II (.....)

### Mengetahui:

a.n Rektor IAIN Palopo  
Dekan Fakultas Syariah



Dr. Muhammad Tahmid Nur, M.Ag.  
NIP 19740630 200501 1 004

Ketua Program Studi  
Hukum Tata Negara (*Siyasah*)



Nirwana Malide, S.HI., M.H.  
NIP 19880106 201903 2 007

## PRAKATA

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ  
الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ وَالصَّلَاةُ وَالسَّلَامُ عَلَى سَيِّدِنَا مُحَمَّدٍ وَعَلَى آلِهِ وَاصْحَابِهِ  
أَجْمَعِينَ. أَمَّا بَعْدُ

Puji syukur penulis panjatkan kepada Allah Swt yang telah menganugerahkan rahmat, hidayah serta kekuatan lahir batin, sehingga penulis dapat menyelesaikan penulisan Skripsi ini dengan judul “Tinjauan Yuridis Tindak Pidana *Cyber Crime* di Indonesia” setelah melalui proses panjang.

Sholawat serta salam tak lupa tercurahkan kepada Nabi Muhammad Saw, para sahabat, keluarga, dan pengikutnya yang menyebarkan dan memperjuangkan ajaran agama islam sehingga membawa peradaban seperti saat ini. Skripsi ini menjadi salah satu syarat wajib memperoleh gelas strata satu (SI), untuk memperoleh gelar sarjana hukum bidang Program Studi Hukum Tata Negara di Institut Agama Islam Negeri Palopo. Penelitian ini dapat diselesaikan berkat dorongan, bantuan, serta bimbingan dari banyak pihak. Meskipun Skripsi ini masih jauh dari kesempurnaan.

Teristimewa dan yang utama penulis sampaikan terima kasih yang tulus kepada kedua orang tua saya yang begitu luar biasa, Ayahanda Nurdin, Ibunda Rahmiati, yang merupakan sumber inspirasi dan motivasi melalui perhatian dan kasih sayang, nasehat, dukungan moril serta materil terutama doa restu demi keberhasilan penulis dalam menuntut ilmu. Semoga penulis dapat menjadi kebanggaan bagi kedua orang tua, dan semoga apa yang telah mereka korbakan selama ini menjadi mahkota keselamatan di dunia dan di akhirat. Selama mengisi

hari-hari kuliah dan penyusunan Skripsi ini, penulis telah banyak mendapat bantuan, motivasi dan bimbingan dari berbagai pihak. Oleh karena itu penulis menghaturkan terima kasih yang tak terhingga kepada yang telah memberikan sumbangsih baik berupa bimbingan, dorongan, dan bantuan yang diberikan kepada penulis, untuk itu penulis ucapkan terima kasih yang tulus kepada :

1. Rektor IAIN Palopo, Dr. Abbas Langaji, M.Ag. beserta Wakil Rektor I Bidang Akademik dan Pengembangan Kelembagaan, Dr. Munir Yusuf, M.Pd. Wakil Rektor II Bidang Administrasi Umum, Perencanaan dan Keuangan, Dr. Masruddin, S.S.,M.Hum, dan Wakil Rektor III Bidang Kemahasiswaan dan Kerjasama, Dr. Mustaming,S.Ag.,M.HI.
2. Dekan Fakultas Syariah IAIN Palopo, Dr. Muhammad Tahmid Nur, M.Ag. beserta Bapak Wakil Dekan I Bidang Akademik, Dr. H. Haris Kulle, Lc.,M.Ag., Wakil Dekan II Bidang Administrasi Umum, Perencanaan, dan Keuangan, Ilham S.Ag.,M.A. dan Wakil Dekan III Bidang Kemahasiswaan dan Kerjasama, Muh. Darwis, S.Ag.,M.Ag.
3. Ketua Program Studi Hukum Tata Negara di IAIN Palopo, Nirwana Halide, S.HI.,M.H, Sekretaris Program Studi Hukum Tata Negara, Syamsuddin, S.H.I.,M.H beserta staf yang telah memberikan bimbingan, masukan dan membantu mengarahkan dalam penyelesaian Skripsi.
4. Pembimbing I dan Pembimbing II, Dr. Abdain, S.Ag., M.HI. dan Firmansyah, S.Pd.,S.H.,M.H. yang telah memberikan bimbingan, masukan dan mengarahkan dalam rangka penyelesaian Skripsi.

5. Penguji I dan Penguji II, Dr. Rahmawati, M.Ag. dan Wawan Haryanto, S.H., M.H yang telah banyak memberikan arahan untuk menyelesaikan Skripsi ini.
6. Penasehat Akademik Dr. H. Muammar Arafat Yusmad, S.H.,M.H
7. Seluruh Dosen beserta seluruh staf pegawai IAIN Palopo yang telah mendidik penulis selama berada di IAIN Palopo dan memberikan bantuan dalam penyusunan Skripsi ini.
8. Kepala Unit Perpustakaan, Abu Bakar, S.Pd.I.,M.Pd beserta Karyawan dan Karyawati dalam lingkup IAIN Palopo, yang telah banyak membantu, khususnya dalam mengumpulkan literatur yang berkaitan dengan pembahasan Skripsi ini.
9. Kepada semua teman seperjuangan penulis, Mahasiswa Program Studi Hukum Tata Negara angkatan 2019 terkhusus kepada sahabat penulis, Malyana Tantri, S.H., Vira Yunia, S.H., Isna Mawar Sari, S.H, Nurlia, S.H., Sumiati, S.H, Rahmi Indah Sulfiani, S.H., Nur Hijrah Dahlan, S.H., Nirwana, S.H., Lis Hidayah, S.H., Rani Pratiwi, S.H., Ramlah, S.H. yang selama ini membantu dan selalu memberikan semangat dalam penyusunan Skripsi ini.
10. Semua pihak yang tak bisa penulis sebutkan satu persatu Terima kasih telah banyak memberikan kontribusinya selama proses penyelesaian Skripsi ini.  
Tiada balasan yang dapat diberikan penyusun, kecuali kepada Allah Swt penulis harapkan balasan dan semoga kerja keras ini bernilai pahala disisi-Nya.

*Aamiin Ya Rabbal Alamin*

Palopo, 17 Mei 2023

Sriwulan

## PEDOMAN TRANSLITERASI ARAB-LATIN DAN SINGKATAN

### A. Transliterasi Arab-Latin

Daftar huruf bahasa Arab dan transliterasinya ke dalam huruf Latin dapat dilihat pada tabel berikut:

#### 1. Konsonan

Huruf Arab	Nama	Huruf Latin	Nama
ا	Alif	Tidak dilambangkan	Tidak dilambangkan
ب	Ba'	B	Be
ت	Ta'	T	Te
ث	Ša'	Š	Es dengan titik di atas
ج	Jim	J	Je
ح	Ha'	h	Ha dengan titik di bawah
خ	Kha	KH	Ka dan ha
د	Dal	D	De
ذ	Žal	Ž	Zet dengan titik di atas
ر	Ra'	R	Er
ز	Zai	Z	Zet
س	Sin	S	Es
ش	Syin	Sy	Es dan ye
ص	Šad	Š	Es dengan titik di bawah
ض	Đađ	Đ	De dengan titik di bawah
ط	Ṭa	Ṭ	Te dengan titik di bawah
ظ	Ža	Ž	Zet dengan titik di bawah
ع	'Ain	'	Koma terbalik di atas
غ	Gain	G	Ge
ف	Fa	F	Fa
ق	Qaf	Q	Qi
ك	Kaf	K	Ka
ل	Lam	L	El
م	Mim	M	Em
ن	Nun	N	En
و	Wau	W	We
ه	Ha'	H	Ha

ء	Hamzah	'	Apostrof
ي	Ya'	Y	Ye

Hamzah (ء) yang terletak di awal kata mengikuti vokalnya tanpa diberi tanda apa pun. Jika ia terletak di tengah atau di akhir, maka ditulis dengan tanda(').

## 2. Vokal

Vokal bahasa Arab, seperti vokal bahasa Indonesia, terdiri atas vokal tunggal atau monoftong dan vokal rangkap atau diftong.

Vokal tunggal bahasa Arab yang lambangnya berupa tanda atau harakat, transliterasinya sebagai berikut:

Tanda	Nama	Huruf Latin	Nama
اَ	<i>fathah</i>	a	a
اِ	<i>kasrah</i>	i	i
اُ	<i>dammah</i>	u	u

Vokal rangkap bahasa Arab yang lambangnya berupa gabungan antara harakat dan huruf, transliterasinya berupa gabungan huruf, yaitu:

Tanda	Nama	Huruf Latin	Nama
اِي	<i>fathah dan ya'</i>	ai	a dan i
اُو	<i>fathah dan wau</i>	au	a dan u

Contoh:

كَيْفَ : *kaifa*  
 هَوَّلَ : *haulā*

## 3. Maddah

*Maddah* atau vokal panjang yang lambangnya berupa harakat dan huruf, transliterasinya berupa huruf dan tanda, yaitu:

Harakat dan Huruf	Nama	Huruf dan Tanda	Nama
اَ ...   اِ ...	<i>fathah</i> dan <i>alif</i> atau <i>yā'</i>	ā	a dan garis di atas
اِ ...	<i>kasrah</i> dan <i>yā'</i>	ī	i dan garis di atas
اُ ...	<i>ḍammah</i> dan <i>wau</i>	ū	u dan garis di atas

مَاتَ : *māta*

رَمَى : *rāmā*

قِيلَ : *qīla*

يَمُوتُ : *yamūtu*

#### 4. *Tā marbūtah*

Transliterasi untuk *tā' marbūtah* ada dua, yaitu *tā' marbūtah* yang hidup atau mendapat harakat *fathah*, *kasrah* dan *ḍammah*, transliterasinya adalah [t], sedangkan *tā' marbūtah* yang mati atau mendapat harakat sukun, transliterasinya adalah [h].

Kalau pada kata yang berakhir dengan *tā' marbūtah* diikuti oleh kata yang menggunakan kata sandang *al-* serta bacaan kedua kata itu terpisah, maka *tā' marbūtah* itu ditransliterasikan dengan ha (h).

Contoh:

رَوْضَةُ الْأَطْفَالِ : *raudah al-atfāl*

الْمَدِينَةُ الْفَاضِلَةُ : *al-madīnah al-fādilah*

الْحِكْمَةُ : *al-hikmah*

## 5. Syaddah (*Tasydīd*)

Syaddah atau *tasydīd* yang dalam sistem tulisan Arab dilambangkan dengan sebuah tanda *tasydīd* ( ّ ), dalam transliterasi ini dilambangkan dengan perulangan huruf (konsonan ganda) yang diberi tanda *syaddah*.

*syaddah*.

## 6. Hamzah

Aturan transliterasi huruf hamzah menjadi apostrof (') hanya berlaku bagi hamzah yang terletak di tengah dan akhir kata. Namun, bila hamzah terletak di awal kata, ia tidak dilambangkan, karena dalam tulisan Arab ia berupa alif.

Contoh:

تَأْمُرُونَ	: ta'murūna
النَّوْعُ	: al-nau'
شَيْءٌ	: syai'un
أُمِرْتُ	: umirtu

## 7. Penulisan Kata Arab yang Lazim Digunakan dalam Bahasa Indonesia

Kata, istilah atau kalimat Arab yang ditransliterasi adalah kata, istilah atau kalimat yang belum dibakukan dalam bahasa Indonesia. Kata, istilah atau kalimat yang sudah lazim dan menjadi bagian dari perbendaharaan bahasa Indonesia, atau sering ditulis dalam tulisan bahasa Indonesia, atau lazim digunakan dalam dunia akademik tertentu, tidak lagi ditulis menurut cara transliterasi di atas. Misalnya, kata al-Qur'an (dari *al-Qur'ān*), alhamdulillah, dan munaqasyah. Namun, bila kata-kata tersebut menjadi bagian dari satu rangkaian teks Arab, maka harus ditransliterasi secara utuh.

Contoh:

*Syarh al-Arbaʿīn al-Nawāwī*

*Risālah fī Riʾāyah al-Maslahah*

#### 8. *Lafz al-Jalālah*

Kata “Allah” yang didahului partikel seperti huruf jarr dan huruf lainnya atau berkedudukan sebagai *mudāfilaih* (frasa nominal), ditransliterasi tanpa huruf hamzah.

Contoh: *dānullāh billāh*

Adapun *بِاللَّهِ* *arbūtah* *دِينُ اللَّهِ* di akhir kata yang disandarkan kepada *lafz al-jalālah*, diteransliterasi dengan huruf [t]. Contoh:

*m fī rahmatillāh* *مُ فِي رَحْمَةِ اللَّهِ*

#### 9. Huruf Kapital

Walau sistem tulisan Arab tidak mengenal huruf kapital (*All Caps*), dalam transliterasinya huruf-huruf tersebut dikenai ketentuan tentang penggunaan huruf kapital berdasarkan pedoman ejaan Bahasa Indonesia yang berlaku (EYD). Huruf kapital, misalnya, digunakan untuk menuliskan huruf awal nama diri (orang, tempat, bulan) dan huruf pertama pada permulaan kalimat. Bila nama diri didahului oleh kata sandang (al-), maka yang ditulis dengan huruf kapital tetap huruf awal nama diri tersebut, bukan huruf awal kata sandangnya. Jika terletak pada awal kalimat, maka huruf A dari kata sandang tersebut menggunakan huruf kapital (al-). Ketentuan yang sama juga berlaku untuk huruf awal dari judul referensi yang didahului oleh kata sandang al-, baik ketika ia ditulis dalam teks maupun dalam catatan rujukan (CK, DP, CDK, dan DR). Contoh:

*Wa mā Muhammadun illā rasūl*

*Inna awwala baitin wudi'a linnāsi lallazī bi Bakkata mubārakan*

*Syahru Ramadān al-lazī unzila fīhi al-Qurān*

*Nasīr al-Dīn al-Tūsī*

*Nasr Hāmid Abū Zayd*

*Al-Tūft*

*Al-Maslahah fī al-Tasyrī' al-Islāmī*

Jika nama resmi seseorang menggunakan kata Ibnu (anak dari) dan Abū (bapak dari) sebagai nama kedua terakhirnya, maka kedua nama terakhir itu harus disebutkan sebagai nama akhir dalam daftar pustaka atau daftar referensi.

Contoh:

Abū al-Walīd Muhammad ibn Rusyd, ditulis menjadi: Ibnu Rusyd, Abū al-Walīd Muhammad (bukan: Rusyd, Abū al-Walīd Muhammad Ibnu)  
Nasr Hāmid Abū Zaīd, ditulis menjadi: Abū Zaīd, Nasr Hāmid (bukan, Zaīd Nasr Hāmid Abū)

## **B. Daftar Singkatan**

Beberapa singkatan yang dibakukan adalah:

Sw. : *Subhanahu wa ta'ala*

Saw. : *Sallallahu 'alaihi wa sallam*

as : *'alaihi al-salam*

H : Hijrah

M : Masehi

SM : Sebelum Masehi

I : Lahir Tahun (untuk orang yang masih hidup saja)

w : Wafat tahun

QS .../...:4 :

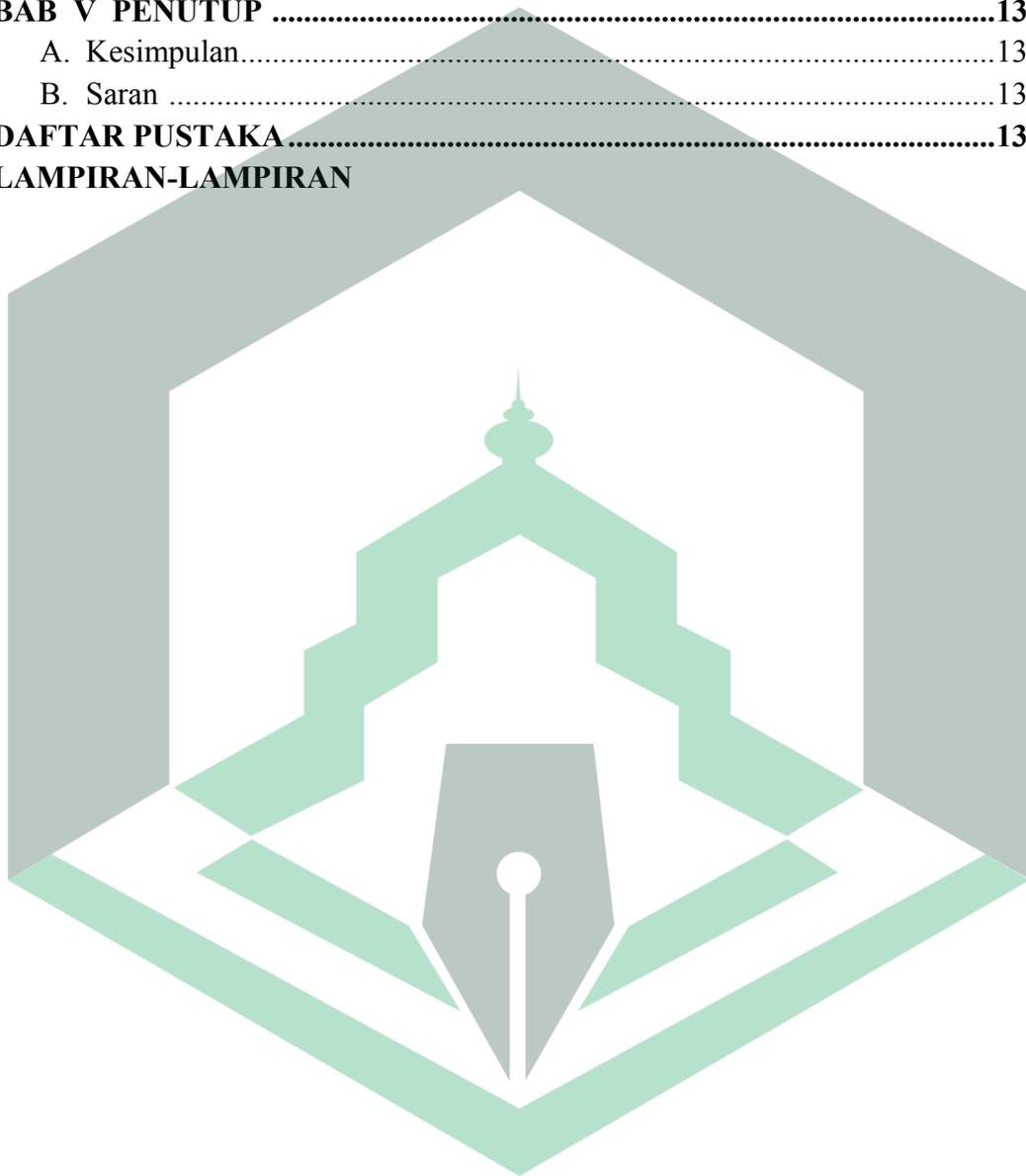
HR : Hadits Riwayat



## DAFTAR ISI

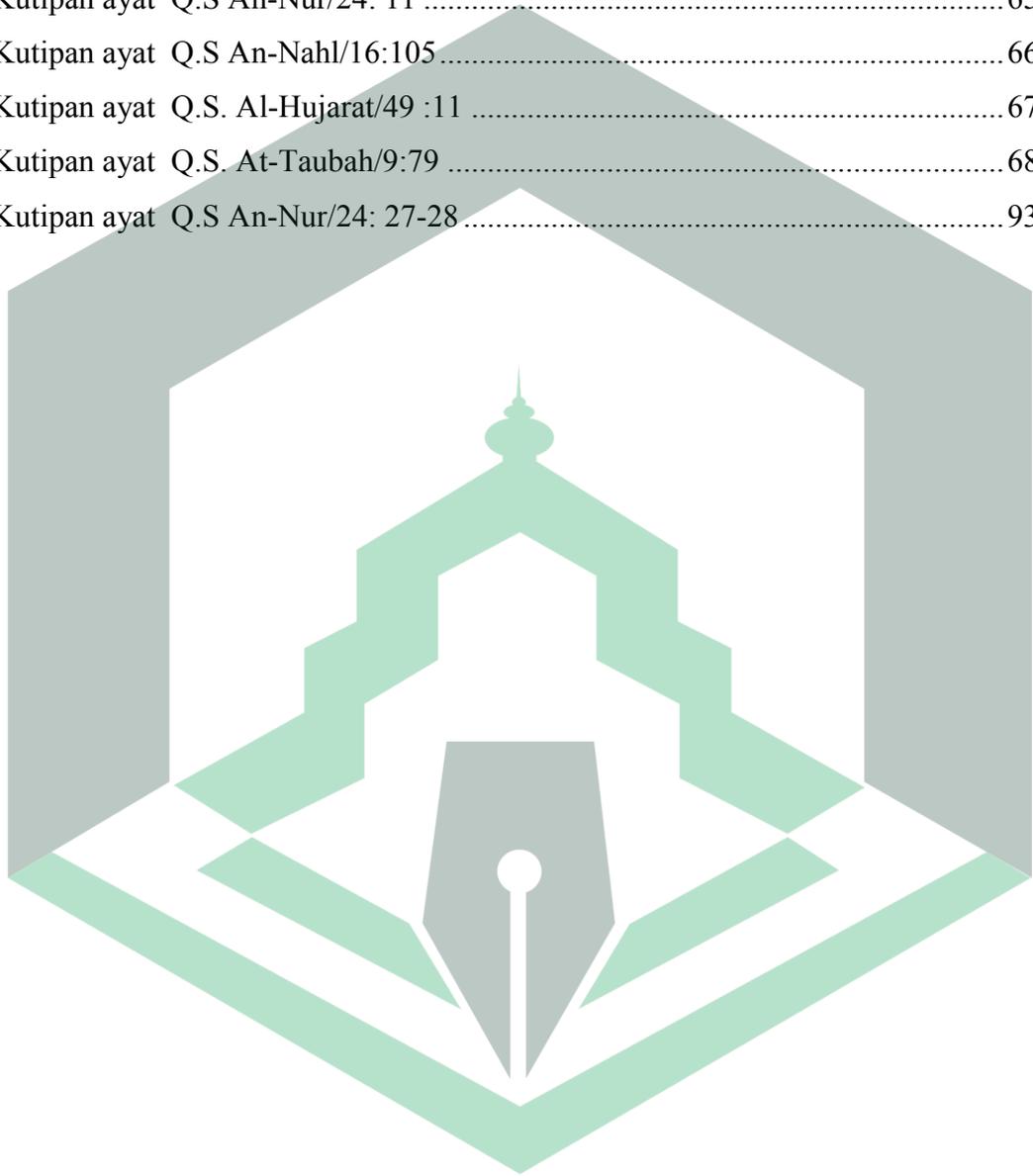
HALAMAN SAMPUL.....	i
HALAMAN JUDUL .....	ii
HALAMAN PERNYATAAN KEASLIAN.....	
HALAMAN PENGESAHAN.....	
PRAKATA.....	iii
PEDOMAN DAN TRANSLITERASI .....	vi
DAFTAR ISI.....	xi
DAFTAR AYAT.....	xii
DAFTAR ISTILAH .....	xiii
ABSTRAK .....	xvii
ABSTRACT.....	xviii
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
A. Latar Belakang .....	1
B. Rumusan Masalah .....	11
C. Tujuan Penelitian.....	11
D. Manfaat Penelitian.....	12
E. Penelitian Terdahulu Yang Relevan.....	13
F. Deskripsi Teori .....	17
G. Metode Penelitian.....	28
H. Kerangka Pikir.....	32
I. Definisi Istilah.....	33
<b>BAB II KETENTUAN PENGATURAN TINDAK PIDANA CYBER CRIME DI INDONESIA .....</b>	<b>35</b>
A. Konsep Tindak Pidana .....	35
B. Konsep <i>Cyber Crime</i> .....	54
C. Ketentuan Pengaturan Tindak Pidana <i>Cyber Crime</i> di Indonesia.....	74
<b>BAB III KENDALA DALAM PENANGANAN TINDAK PIDANA CYBER CRIME DI INDONESIA .....</b>	<b>90</b>
A. Faktor Yang Mempengaruhi Terjadinya <i>Cyber Crime</i> .....	90
B. Kendala dalam Penanganan Tindak Pidana <i>Cyber Crime</i> di Indonesia .....	103

<b>BAB IV PENANGANAN TINDAK PIDANA <i>CYBER CRIME</i></b>	
<b>DI INDONESIA .....</b>	<b>112</b>
A. Kebijakan Formulasi Hukum Pidana dalam Penanggulangan <i>Cyber Crime</i> di Indonesia .....	112
B. Penanganan Tindak Pidana <i>Cyber Crime</i> di Indonesia.....	118
<b>BAB V PENUTUP .....</b>	<b>136</b>
A. Kesimpulan.....	136
B. Saran .....	137
<b>DAFTAR PUSTAKA.....</b>	<b>139</b>
<b>LAMPIRAN-LAMPIRAN</b>	



## DAFTAR AYAT

Kutipan ayat Q.S Al-Maidah/5: 64 .....	6
Kutipan ayat Q.S. Al-Baqarah/2:9 .....	64
Kutipan ayat Q.S An-Nur/24: 11 .....	65
Kutipan ayat Q.S An-Nahl/16:105 .....	66
Kutipan ayat Q.S. Al-Hujarat/49 :11 .....	67
Kutipan ayat Q.S. At-Taubah/9:79 .....	68
Kutipan ayat Q.S An-Nur/24: 27-28 .....	93



## DAFTAR ISTILAH



UU ITE	: Undang-Undang Informasi dan Transaksi Elektronik
KUHP	: Kitab Undang-Undang Hukum Pidana
UUD	: Undang-Undang Dasar
EDI	: Elektronik Data Interchange
APJII	: Asosiasi Penyelenggara Jasa Internet Indonesia
ASEAN	: Association Of South-East Asia Nation
NCSI	: National Cyber Security Index
BSSN	: Badan Siber dan Sandi Negara
IT	: Informasi Teknologi
IPTEK	: Ilmu Pengetahuan dan Teknologi
NKRI	: Negara Kesatuan Republik Indonesia
TP	: Tindak Pidana
BPJS	: Badan Penyelenggara Jaminan Sosial
BRI	: Bank Rakyat Indonesia
E-HAC	: Elektronik Health Aleart
SARA	: Suku, Agama, Ras, dan Antargolongan
PBB	: Perserikatan Bangsa-Bangsa

## ABSTRAK

**Sriwulan, 2023.** “*Tinjauan Yuridis Tindak Pidana Cyber Crime di Indonesia*”. Skripsi Program Studi Hukum Tata Negara Fakultas Syariah Institut Agama Islam Negeri Palopo dibimbing oleh Abdain dan Firmansyah.

Skripsi ini membahas tentang Tinjauan Yuridis Tindak Pidana *Cyber Crimi*di Indonesia. Penelitian ini bertujuan untuk: mengetahui ketentuan Pengaturan tindak pidana *cyber crime* di Indonesia; untuk mengetahui kendala yang dihadapi dalam penanganan tindak pidana *cyber crime* di Indonesia; untuk mengetahui penanganan tindak pidana *cyber crime* di Indonesia. Jenis penelitian ini adalah penelitian hukum normatif dengan pendekatan penelitian yang digunakan adalah pendekatan perundang-undangan. Teknik pengumpulan data yang digunakan adalah studi kepustakaan(*library research*) dengan Teknik analisis data yang digunakan adalah deskriptif kualitatif. Hasil penelitian ini menunjukkan bahwa ketentuan pengaturan tindak pidana *cyber crime* di Indonesia terdapat dalam pasal 332, 333, 334, 407, 426, 433, 483 KUHP, Undang-Undang No 19 tahun 2016 perubahan atas Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang No. 28 Tahun 2014 tentang Hak Cipta, Undang-Undang No. 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme, Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi dan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Meskipun sudah ada beberapa peraturan yang dapat menjerat pelaku *cyber crime* ke penjara masih dijumpai adanya Kendala yang dihadapi dalam penanganan tindak pidana *cyber crimi*di Indonesia yakni faktor hukum, faktor penegak hukum, Alat bukti, Faktor sarana dan fasilitas pendukung, faktor masyarakat, serta keterbatasan anggaran oprasional yang kurang menjadi faktor signifikan dalam mengungkap kasus *cyber crime*. Sebagai salah satu bentuk dari kejahatan berteknologi tinggi(*hi-tech crime*)Adapun berbagai upaya dalam penanganan tindak pidana *cyber crime* yang bisa ditempuh yaitu melalui upaya non hukum seperti pendekatan teknologi, pendekatan budaya,/*cultural*, pendekatan edukatif/moral/moral religius, hingga pendekatan global seperti kerja sama internasional, dan upaya hukum yaitu melakukan pendekatan penegakan hukum terhadap tiga unsur sistem hukum, yakni struktur hukum (*legal structure*) substansi hukum (*legal substance*) dan budaya hukum (*legal culture*).

**Kata Kunci :** Cyber Crime, Tindak Pidana

## ABSTRACT

**Sriwulan, 2023.** *"Judicial Review of Cyber Crime Crimes in Indonesia"*. Thesis of the Constitutional Law Study Program, Faculty of Sharia, Palopo State Islamic Institute, supervised by Abdain and Firmansyah.

This thesis discusses the Juridical Review of Cyber Crime in Indonesia. This research aims to: determine the provisions governing cyber crime in Indonesia; to find out the obstacles faced in handling cyber crime in Indonesia; to find out how to handle cyber crime in Indonesia. This type of research is normative legal research with the research approach used is a statutory approach. The data collection technique used was library research with the data analysis technique used was descriptive qualitative. The results of this study indicate that the provisions governing cyber crime in Indonesia are contained in articles 332, 333, 334, 407, 426, 433, 483 of the Criminal Code, Law No. 19 of 2016 amendment to Law no. 11 of 2008 concerning Information and Electronic Transactions, Law no. 28 of 2014 concerning Copyright, Law no. 5 of 2018 concerning Eradication of Criminal Acts of Terrorism, Law no. 36 of 1999 concerning Telecommunications and Law no. 27 of 2022 concerning Personal Data Protection. Even though there have been several regulations that can ensnare cybercrime perpetrators in prison, there are still obstacles encountered in handling cybercrime in Indonesia, namely legal factors, law enforcement factors, evidence, supporting facilities and facilities, community factors, and budget constraints. Insufficient operations are a significant factor in uncovering cyber crime cases. As a form of high-tech crime (hi-tech crime), there are various efforts in handling cyber crime that can be taken, namely through non-legal efforts such as technological approaches, cultural/cultural approaches, educative/moral/religious approaches, to global approaches such as international cooperation, and legal remedies, namely taking a law enforcement approach to three elements of the legal system, namely legal structure, legal substance and legal culture.

**Keywords:** Cyber Crime, Criminal Acts

# BAB I

## PENDAHULUAN

### A. Latar Belakang

Undang-Undang Informasi dan transaksi elektronik yang disahkan DPR pada 25 maret 2008 menjadi bukti bahwa Indonesia tidak lagi ketinggalan dari negara lain dalam membuat peranti hukum di bidang *cyber space law*. UU ini merupakan *cyberlaw* di Indonesia, karena muatan dan cakupannya yang luas dalam membahas peraturan dunia maya.<sup>1</sup>

Undang-Undang Nomor 19 Tahun 2016 atas perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ini mengatur berbagai perlindungan hukum atas kegiatan yang memanfaatkan internet sebagai medianya, baik transaksi maupun pemanfaatan informasinya. Pada Undang-Undang ITE ini juga diatur berbagai macam hukuman bagi kejahatan yang dilakukan melalui internet. Undang-Undang ITE ini juga mengakomodir kebutuhan para pelaku bisnis di internet dan masyarakat pada umumnya guna mendapat kepastian hukum, dengan diakuinya bukti elektronik dan tanda tangan digital sebagai bukti yang sah dipengadilan. Undang-Undang ITE ini berlaku untuk setiap orang yang melakukan perbuatan hukum, baik di wilayah Indonesia maupun diluar wilayah Indonesia, yang memiliki keterkaitan hukum di Indonesia.<sup>2</sup>

---

<sup>1</sup> Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cyber crime) Urgensi Pengaturan dan Celah Hukumnya*, (Depok: PT. Raja Grafindo Persada, 2013), 102

<sup>2</sup> RikoNugraha, "Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber di Indonesia." *Jurnal ilmiah hukum dirgantara*, 11, No.2, (Maret 2021), 20.

Berdasarkan Undang-Undang Nomor 19 Tahun 2016 atas perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, informasi elektronik merupakan satu atau sekumpulan data elektronik termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *Elektronik Data Interchange* (EDI), surat elektronik (*electronic mail*), telegram, atau sejenisnya, huruf, tanda, angka, kode akses, symbol, atau yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Banyak teknologi informasi maupun teknologi telekomunikasi yang semakin terkemuka, hampir banyak teknologi maupun alat dan elektronik yang setiap saat bermunculan dan berganti model (*type*). Berbagai macam barang teknologi seperti HP, Laptop, Komputer dan sebagainya.<sup>3</sup>

Transaksi elektronik merupakan suatu kegiatan pada dunia siber yang menjadi inspirasi untuk lahirnya alternatif baru pada penyelenggaraan suatu kegiatan, mulai kegiatan bisnis, pendidikan, pendaftaran, pembelian, pembayaran, jasa perbankan hingga seluruh kegiatan yang dilakukan secara elektronik dalam pemenuhan kebutuhan sehari-hari. Manfaat transaksi elektronik ini telah diakui oleh kementerian komunikasi dan informatika (Kemenkominfo) Republik Indonesia yang secara tegas berpendapat bahwa dengan masuknya teknologi, informasi dan komunikasi melalui suatu kegiatan yang berbasis elektronik, maka kedepannya dapat membuka peluang yang baik bagi pertumbuhan penduduk di Indonesia, baik dari segi ilmu pengetahuan maupun ekonomi.<sup>4</sup>

---

<sup>3</sup> Riko Nugraha, "Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber di Indonesia." *Jurnal ilmiah hukum dirgantara*, 11, No.2, (Maret 2021), 22.

<sup>4</sup> Soerjono Soekanto, *Pengantar Penelitian Hukum*, (Jakarta: Universitas Indonesia Press, 1984), 10

Teknologi informasi dan transaksi elektronik di era globalisasi telah menempatkan posisi yang sangat strategis karena menghadirkan suatu dunia tanpa batas, jarak, ruang dan waktu yang berdampak pada peningkatan produktivitas dan efisiensi. Pengaruh globalisasi juga telah mengubah pola hidup masyarakat dan berkembang menjadi tatanan kehidupan baru yang mendorong terjadinya perubahan social, ekonomi, budaya bahkan penegakan hukum.<sup>5</sup>

Kebutuhan akan teknologi jaringan komputer semakin meningkat. Selain sebagai media penyedia informasi, melalui internet pula kegiatan komunitas komersial menjadi bagian terbesar dan pesat pertumbuhannya serta menembus berbagai batas negara. Bahkan melalui jaringan ini, segala macam informasi di dunia bisa diketahui selama 24 jam. Melalui dunia internet atau bisa disebut *cyber space*, apapun dapat dilakukan.

Teknologi informasi dan transaksi elektronik telah dimanfaatkan dalam kehidupan sosial masyarakat dan telah memasuki berbagai sektor kehidupan baik sektor pemerintah, sektor bisnis, dan lain sebagainya selain bisa memberikan dampak positif, teknologi informasi dan transaksi elektronik juga memberikan dampak negatif seperti menjadikan sarana untuk melakukan tindak pidana baru (*Cyber crime*).<sup>6</sup>

Keberadaan teknologi informasi dalam suatu kehidupan manusia di dunia sangatlah penting, baik dimasa sekarang maupun dimasa yang akan datang, karena dengan memanfaatkan kecanggihan teknologi dan informasi, sudah barang

---

<sup>5</sup> Heru Soeprapto, "Peranan Komputer dalam Industry dan Pengaruhnya Terhadap Bidang Hukum", *Skripsi* (Bandung: Universitas Diponegoro, 2000).

<sup>6</sup> Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cyber crime) Urgensi Pengaturan dan Celah Hukumnya*, (Depok: PT. Raja Grafindo Persada, 2013), 108.

tentu akan dapat membuka cakrawala baru dalam suatu kehidupan manusia di dunia yang menjanjikan dapat menembus batas antar negara dan dapat mempercepat penyebaran informasi maupun pertukaran ilmu pengetahuan dan gagasan di kalangan ilmuwan serta cendekiawan di seluruh dunia. Seiring dengan kebutuhan masyarakat di dunia dan kemajuan teknologi informasi sudah barang tentu akan dapat memacu pertumbuhan ekonomi dunia berkembang dengan pesat, baik dimasa sekarang maupun dimasa yang akan datang. Hal ini disebabkan oleh karena: 1). Adanya kemajuan teknologi informasi dan komunikasi dapat mendorong permintaan atas produk-produk teknologi informasi dan komunikasi itu sendiri, seperti komputer, modem, sarana untuk membangun jaringan internet dan lain sebagainya. 2). Memudahkan transaksi bisnis terutama bisnis keuangan disamping bisnis lainnya. Kemajuan teknologi informasi dan komunikasi yang pesat juga dapat memberikan kemudahan bagi setiap orang di dunia untuk itu Teknologi informasi ini yakini membawa keuntungan yang besar bagi negara-negara di dunia.<sup>7</sup>

Perkembangan teknologi informasi dan komunikasi yang pesat dapat menjadikan pedang bermata dua, karena selain memberikan kontribusi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus dapat menjadi sarana yang efektif kejahatan/perbuatan melawan hukum. Perbuatan melawan hukum yang dilakukan melalui dunia maya merupakan kejahatan baru, yang dikenal dengan istilah *cyber crime*. Kejahatan yang dilakukan melalui jaringan internet yang berbasis komputer dinamakan *cyber crime*, yang modus

---

<sup>7</sup> Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cyber crime) Urgensi Pengaturan dan Celah Hukumnya*, (Depok: PT. Raja Grafindo Persada, 2013), 1

operandinya dilakukan melalui jaringan sistem komputer dan sistem komunikasi dijadikan sebagai sarana atau alat untuk memperoleh keuntungan diri sendiri dengan merugikan pihak lain. *Cyber crime* merupakan satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif yang sangat luas bagi seluruh bidang kehidupan modern saat ini.<sup>8</sup>

Teknologi informasi (*information technology*) membawa dampak bagi masyarakat secara luas, baik dampak positif maupun negatif. Dampak positifnya adalah dapat memperoleh berbagai informasi, baik dari dalam maupun luar negeri, transaksi jarak jauh. Sedangkan dampak negatifnya adalah memberikan peluang untuk melakukan berbagai kejahatan. Seiring dengan perkembangannya teknologi internet, menyebabkan munculnya beberapa kasus *cyber crime* seperti penipuan, *hacking* beberapa situs, pencurian, pencemaran nama baik, keasusilaan, perjudian, pengancaman, perusakan dan teror, menyadap transmisi data orang lain misalnya email dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki kedalam program komputer. Sehingga dalam kejahatan komputer dimungkinkan adanya delik formil dan delik materil. Delik formil adalah delik yang perumusannya menitik beratkan pada perbuatan yang dilarang dan diancam dengan pidana oleh Undang-Undang.<sup>9</sup> Misalnya perbuatan seseorang yang memasuki komputer orang lain tanpa ijin, sedangkan delik materil adalah delik yang perumusannya menitik beratkan pada akibat yang dilarang dan diancam dengan pidana oleh Undang-Undang yang berlaku. Misalnya perbuatan yang menimbulkan akibat kerugian bagi orang lain.

---

<sup>8</sup> Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, (Jakarta: Rajawali Pres, 2006), 1.

<sup>9</sup> Leden Marpaung, *Asas Teori Praktik Hukum Pidana*, (Jakarta: Sinar Grafika, 2008), 8.

Konteks islam *cyber crime* adalah tindakan yang dilarang oleh Allah Swt, karena Allah swt, tidak menyukai orang-orang yang membuat kerusakan yang memudharatkan orang lain. Perusakan dalam bentuk apapun tidak dibenarkan, karena perusakan merupakan tindakan yang bertentangan dengan nilai-nilai universal. Allah Swt berfirman dalam Q.S. Al-Maidah/5:64 sebagai berikut:

وَقَالَتِ الْيَهُودُ يَدُ اللَّهِ مَغْلُولَةٌ غُلَّتْ أَيْدِيهِمْ وَلُعِنُوا بِمَا قَالُوا بَلْ يَدَاهُ مَبْسُوطَتَانِ يُنفِقُ كَيْفَ يَشَاءُ  
وَلَيَزِيدَنَّ كَثِيرًا مِّنْهُمْ مَا أَنْزَلْنَا إِلَيْكَ مِنَ رَبِّكَ طُغْيَانًا وَكُفْرًا وَالْفَيْنَا بَيْنَهُمُ الْعَدَاوَةَ وَالْبَغْضَاءَ إِلَى  
يَوْمِ الْقِيَامَةِ كُلَّمَا أَوْقَدُوا نَارًا لِلْحَرْبِ أَطْفَأَهَا اللَّهُ وَيَسْعَوْنَ فِي الْأَرْضِ فَسَادًا وَاللَّهُ لَا يُحِبُّ  
الْمُفْسِدِينَ

Terjemahnya: “Orang-orang Yahudi berkata: “Tangan Allah terbelenggu”. Tangan merekalah yang dibelenggu dan merekalah yang dilaknat disebabkan apa yang telah mereka katakan itu. (Tidak demikian), tetapi kedua-dua tangan Allah terbuka; Dia menafkahkan sebagaimana dia kehendaki. Dan pasti apa yang diturunkan (Al-Quran) kepadamu dari tuhanmu akan menambah pelampauan batas dan kekufuran oleh banyak diantara mereka. Dan kami telah campakkan permusuhan dan kebencian di antara mereka sampai hari kiamat. Setiap mereka menyalakan api peperangan, Allah memadamkannya dan mereka berbuat kerusakan dimuka bumi dan Allah tidak menyukai orang-orang yang membuat kerusakan”.<sup>10</sup>

Ayat tersebut menegaskan bahwa tindakan perusakan merupakan sesuatu yang dilarang oleh Allah Swt, dan Allah tidak menyukai dan tidak merestui

<sup>10</sup> M. Quraish Shihab. *Tafsir Al-Mishbah, Surah Al-Ma'idah* (jakarta : Lentera Hati, 2002 ), 134.

dengan memberi ganjaran atau rahmat, baik dalam bentuk apapun dan dimanapun, tetap tidak dibenarkan. Tindakan para *hacker* menjadi bagian dari perbuatan dan tindakan yang sangat dominan dilakukan oleh para pelaku kejahatan *cyber crime* yang dilarang sebagaimana ayat tersebut. Landasan pada larangan tersebut mengarah pada hal-hal yang merugikan dan meresahkan bagi orang lain.

Kasus-kasus *Cyber crime* dapat dikatakan suatu bentuk kejahatan canggih yang dilakukan dengan teknik tinggi atau intelektual, sehingga sangat sulit untuk dimengerti oleh orang awam yang tidak menguasai teknik teknologi informasi dan komunikasi. Semua orang rentan menjadi korban dari kejahatan *cyber* karena sudah terpengaruh oleh pesatnya kemajuan teknologi. Tingginya pengaruh negatif dari teknologi khususnya internet akan memperbesar timbulnya suatu kejahatan *cyber*.<sup>11</sup>

Kasus-kasus yang muncul dipermukaan dan diketahui oleh public umumnya berdasarkan adanya laporan dari korban *cyber crime* akan kerugian yang dialaminya. Contoh Pada kasus korban penipuan dalam transaksi jual beli di *online shop*, dimana pelaku seolah-olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu produk atau di salah satu *website* sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan, tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesan tidak datang sehingga pembeli tersebut merasa tertipu. Selanjutnya kasus pengancaman dan pemerasan melalui *e-mail*, pencemaran nama baik dengan menggunakan media internet e-

---

<sup>11</sup> Andi Hamzah, *Aspek-aspek Pidana dibidang Komputer*, (Jakarta: Sinar Grafika, 1987), 26.

mail, mailing list, penyebaran pornografi di *website*, kasus perjudian secara online di internet, dan kasus kejahatan *cyber crime* lainnya yang membuat sistem milik orang tidak berfungsi.<sup>12</sup>

Berdasarkan hasil survey Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2021-2022 tersebut, bahwasanya pengguna internet di Indonesia dari tahun ketahun telah mengalami peningkatan yang cukup signifikan. Peningkatan mulai dari tahun 2018 ketahun 2019-2020 yaitu sebesar 8,90%, peningkatan dari tahun 2019-2020 ketahun 2021-2022 yaitu sebesar 3,32%. Kemudahan akses perangkat elektronik ke jaringan internet dan banyaknya jumlah perangkat elektronik yang dapat tersambung internet dapat menjadi salah satu faktor pertumbuhan pengguna internet di Indonesia akan terus meningkat.<sup>13</sup>

Kasus pencemaran nama baik masih mendominasi laporan di kepolisian terkait UU ITE, pada 2020 menjadi 1.794 laporan polisi yang menyangkut pencemaran nama baik. Urutan kedua ditempati ujaran kebencian sebanyak 223 laporan polisi pada 2020. Selanjutnya terkait informasi hoaks atau kabar bohong pada tahun 2020 menjadi 197 kasus yang menyangkut hoaks.<sup>14</sup>

Menurut data ASEAN Cyberthreat 2021, Indonesia menempati urutan pertama diantara negara-negara ASEAN, Perihal serangan *malware*. Indonesia berada di urutan pertama dengan 1,3 juta kasus. Jumlah tersebut hampir setengah

<sup>12</sup> Asril Sitompul, *Hukum Internet Pengenalan Mengenai Masalah Hukum Cyber Crime* (Bandung: Citra Aditya Bakti, 2001),114.

<sup>13</sup> Asrarina Oktaviani, "Alternative Pidana Bagi Pelaku Tindak Pidana Peretasan di Indonesia dalam Undang-Undang Informasi dan Transaksi Elektronik." *Jurnal Hukum*, 1, no.1 (januari ,9,2023): 250, <https://doi.org/10.2674/novum.v0i0.50394>

<sup>14</sup> Riko Nugraha, "Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber di Indonesia." *Jurnal ilmiah hukum dirgantara*, 11, No.2, (Maret 2021),<https://doi.org/10.35968/jihd.v11i2.767>

dari total keseluruhan ancaman *ransomware* di antara negara-negara ASEAN. Vietnam berada di urutan kedua dengan 886.874 kasus. Sementara Brunei menjadi yang terendah dengan 257 kasus. Sebuah laporan terbaru oleh National Cyber Security Index (NCSI) menunjukkan keamanan siber Indonesia beradadi peringkat ke-6 diantara negara-negara ASEAN lainnya dan urutan 83 dari 160 negara secara global. Sementara itu, dalam tiga tahun terakhir ancaman-ancaman siber pada umumnya menyasar perusahaan besar dan institusi pemerintahan. Indonesia menduduki peringkat ketiga mengenai jumlah kasus kebocoran data terbanyak di dunia pada tahun 2022 yaitu dengan jumlah 13,8 juta akun yang telah bocor. Data tersebut semakin memperkuat bukti bahwa Indonesia masih sangat rentan terkena serangan siber.<sup>15</sup> Berdasarkan kajian dan analisis yang dilakukan melalui DAKA Advisor pada tahun 2022, kerugian yang diperkirakan akibat *cyber crime* di Indonesia adalah USD 895 miliar, yang berarti mencapai 1,20% dari total kerugian yang diperkirakan akibat *cyber crime* global, yaitu USD 71,620 miliar.<sup>16</sup>

Badan Siber dan Sandi Negara (BSSN) melaporkan bahwa lebih dari 700 juta serangan siber terjadi di Indonesia pada tahun 2022, sehingga menimbulkan sejumlah masalah terkait perlindungan data pribadi. *Ransomware*, atau perangkat lunak dengan mode permintaan tebusan, adalah jenis serangan siber yang paling umum. Menurut data BSSN, ada 714.170.967 lintas atau serangan siber sepanjang

---

<sup>15</sup> Asrarina Oktaviani, Emmilia Rusdiana “Alternative Pidana Bagi Pelaku Tindak Pidana Peretasan di Indonesia dalam Undang-Undang Informasi dan Transaksi Elektronik.” *Jurnal Hukum*, 1, no.1 (januari ,9,2023),250, <https://doi.org/10.2674/novum.v0i0.50394>

<sup>16</sup> Febyola Indah, ” Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia ” *Jurnal Bidang Penelitian Informatika*, 1, No. 1, (22 Oktober 2022).1-8, <https://ejournal.Kreatifcemerlang.id/index.php/jbpi/article/view/78>

tahun 2022, bulan januari mengalami serangan terbanyak dengan 272. 962.734 lebih dari sepertiga dari semua serangan selama paruh pertama tahun ini. Serangan *Ransomware*, juga dikenal sebagai serangan *malware* yang menuntut tebusan dari pemilik data, adalah jenis serangan siber paling umum yang sering di temukan BSSN.<sup>17</sup>

Kejahatan yang dilakukan melalui dunia maya atau melalui jaringan sistem elektronik yang berbasis komputer adalah komputer itu sendiri dan dokumen elektronik yang tersimpan di dalamnya secara komputerisasi, karena kejahatannya dilakukan dengan menggunakan komputer sebagai sarana atau alat dan komputer dijadikan sebagai sasaran untuk melakukan kejahatan dengan cara masuk atau mengakses jaringan komputer tanpa izin.

Aspek pokok aktivitasnya, *cyber crime* dilakukan lebih menitik beratkan pada penyerangan kontent, komputer system dan *communication system* milik orang lain, baik secara personal maupun umum di dalam *cyber space*. Untuk itu, diperlukan pengamanan sebuah sistem untuk mencegah terjadinya perusakan. Penanggulangan *cyber crime* dilakukan dengan pencegahan dan penegakan hukum, demi tercapainya supremasi hukum. Apabila dibiarkan terus menerus, dapat mengganggu keamanan baik secara nasional maupun internasional. Sesungguhnya *cyber crime* sudah mengganggu keamanan dalam negeri maupun

---

<sup>17</sup> Denda Ginanjar, "Urgensi Perlindungan Data Pribadi dalam Menjamin Keamanan Data", *Jurnal Hukum dan HAM West Science*, 1, No. 1,(November,14,2022). 22, <https://wnj.westsciencepress.com/index.php/jhhws/article/view/7>

luar negeri, sehingga diperlukan langkah-langkah strategis aparat penegak hukum untuk menanggulangnya.<sup>18</sup>

Lahirnya Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) telah dinilai mampu mengakomodir jenis kejahatan yang merupakan pengembangan terhadap kejahatan melalui media internet. Selain itu, Undang-Undang tersebut diharapkan menjadi jawaban konkrit terhadap masalah yang dihadapi oleh aparat penegak hukum.<sup>19</sup>

Berdasarkan latar belakang masalah yang telah diuraikan diatas mendorong penulis untuk melakukan penelitian dengan judul “TINJAUAN YURIDIS TINDAK PIDANA *CYBER CRIME* DI INDONESIA”.

## **B. Rumusan Masalah**

Berdasarkan latar belakang masalah yang telah dikemukakan diatas maka rumusan masalah yang ada dalam penelitian ini yaitu:

- a. Bagaimana ketentuan pengaturan Tindak Pidana *Cyber crime* di Indonesia?
- b. Apa Kendala yang dihadapi dalam Penanganan Tindak Pidana *Cyber crime* di Indonesia?
- c. Bagaimana Penanganan Tindak Pidana *Cyber crime* di Indonesia?

---

<sup>18</sup> Muhammad Muis. “Kebijakan Hukum Pidana dalam Penanggulangan *Cyber Crime* di Indonesia”, *skripsi*, (medan: 2019) .

<sup>19</sup> Undang-Undang Republik Indonesia No. 19 Tahun 2016 atas perubahan Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).

### **C. Tujuan Penelitian**

Tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

- a. Untuk mengetahui ketentuan pengaturan tindak pidana *Cyber crime* di Indonesia
- b. Untuk mengetahui Kendala yang dihadapi dalam Penanganan Tindak Pidana *Cyber crime* di Indonesia
- c. Untuk mengetahui Penanganan tindak pidana *Cyber crime* di Indonesia

### **D. Manfaat Penelitian**

Merujuk pada rumusan masalah yang akan diteliti yang sebagaimana di sebutkan diatas, penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

#### **1. Manfaat Teoritis**

Hasil penelitian ini diharapkan dapat menambah literatur dan sumber informasi di lingkungan Program Studi Hukum Tata Negara (*Siyasah*) Fakultas Syariah Institut Agama Islam Negeri Palopo. Serta penelitian ini diharapkan dapat memberikan pemahaman, pengetahuan, dan gambaran utuh tentang tinjauan yuridis tindak pidana *cyber crime* di Indonesia. Selain itu dapat memperkuat dan menyempurnakan teori-teori sebelumnya, dan dapat dijadikan sebagai bahan referensi bagi para pihak peneliti selanjutnya, yang ingin mengetahui tentang pandangan hukum mengenai tindak pidana kasus *Cyber crime* di Indonesia.

## 2. Manfaat Praktis

### a. Bagi Penulis

Sebagai bahan acuan untuk menambah ilmu pengetahuan dan membentuk pola pikir kritis yang berkaitan dengan masalah tindak pidana *Cyber crime* di Indonesia, sebagai salah satu pemenuhan persyaratan dalam penyelesaian Studi di Fakultas Syariah Program Studi Hukum Tata Negara.

### b. Bagi Masyarakat

Penelitian ini diharapkan dapat menjadi salah satu sumber atau bahan pembelajaran terhadap masalah-masalah dalam kemajuan perkembangan ilmu hukum dan pengetahuan kedepannya bagi masyarakat terkait tindakan hukum pidana mengenai *Cyber crime*.

## E. Penelitian Terdahulu Yang Relevan

Berdasarkan hasil penelusuran dapat diidentifikasi beberapa penelitian yang dilakukan sebelumnya dan dianggap mirip dengan masalah yang akan diteliti tetapi memiliki beberapa perbedaan terhadap masalah yang akan dikaji dalam penelitian ini. Dari beberapa penelitian yang dimaksud adalah:

1. Ruddy R. Watulinggas dengan judul “Tinjauan Yuridis tentang alat bukti digital dalam tindak pidana kejahatan mayantara (*Cyber Crime*)”. Penelitian ini mengkaji tentang kedudukan alat bukti dalam perkara kasus *cyber crime* dan faktor yang mempengaruhi kejahatan mayantara. Dengan hasil penelitian menyatakan bahwa belum ada pemrosesan alat bukti yang sesuai prosedur, alat bukti digital yang dihadirkan di persidangan telah di explore oleh saksi sebelumnya, sehingga mengurangi keaslian dari sebuah alat bukti itu sendiri,

padahal dalam Undang-undang no. 11 tahun 2008 pada pasal 43 ayat (2) telah dijelaskan tentang pelaksanaan prosedur penyidikan dalam bidang teknologi informasi dan transaksi elektronik, sistem pembuktian dalam perkara dalam perkara tindak pidana *cyber crime* dengan cara memperluas alat bukti dalam KUHAP sebenarnya sudah diatur dalam berbagai Perundang-Undangan secara tersebar. Dengan demikian email, suara, gambar, kode akses, simbol, dan berbagai dokumen elektronik lainnya mempunyai kekuatan pembuktian yang setara dengan alat bukti lainnya yang diatur dalam KUHAP dan digunakan sebagai alat bukti yang sah.<sup>20</sup>

Berdasarkan hasil penelitian ini terdapat persamaan dan perbedaan penelitian yang akan dilakukan oleh penulis yaitu keduanya mengkaji satu variable penelitian yang sama yaitu *cyber crime* sedangkan perbedaannya adalah peneliti diatas membahas tentang kedudukan alat bukti dalam perkara kasus *cyber crime* dan faktor yang mempengaruhi kejahatan mayantara. Sedangkan penelitian yang dilakukan oleh penulis mengkaji tentang ketentuan yang mengatur tindak pidana *cyber crime* di Indonesia, serta penanganan yang bisa dilakukan.

2. Jhodi Shofian dengan judul “ Tinjauan Siyasah Dusturiyah Terhadap Pelaksanaan Kewenangan *Cyber Crime* Polda Bengkulu dalam Pembentukan Virtual Police. ”Penelitian yang dilakukan pada tahun 2022, dengan hasil penelitian menyatakan bahwa perspektif Siyasah Dusturiyah terhadap Pelaksanaan Kewenangan *Cyber Crime* Polda Bengkulu dalam Pembentukan

---

<sup>20</sup> Ruddy R. Watulinggas dengan judul “Tinjauan Yuridis Tentang Alat Bukti Digital Dalam Tindak Pidana Kejahatan Mayantara (*Cyber Crime*)”. *jurnal unsrat* , 10 No. 5 (22 agustus 2022).

Virtual Police bahwa ada 3 kajian pokok dalam fikih Siyasah Dusturiyah yaitu diantaranya *Siyasah Tasyri'iyah*, *Siyasah Tandfidziah*, dan *Siyasah Qoda'iyah*. Dan yang menjadi latar belakang pada pembahasan adalah *Siyasah Tandfidziah*. Karena dalam setiap kegiatan kepolisian yang telah diberikan oleh Undang-Undang harus menjalankan tugas dan kewenangannya sesuai dengan Undang-Undang dan dapat memberikan kemaslahatan bagi manusia.<sup>21</sup>

Berdasarkan hasil penelitian yang dilakukan oleh Jhodi Shofian terdapat persamaan dan perbedaan, penelitian yang akan dilakukan oleh penulis yaitu keduanya mengkaji satu variable penelitian yang sama yaitu *cyber crime* sedangkan perbedaannya dalam penelitian ini adalah peneliti diatas membahas tentang kasus *cyber crime* ini ditinjau dari siyasah dusturiyah, sedangkan penelitian yang akan dilakukan penulis ditinjau berdasarkan tinjauan yuridis.

3. Bonanda Japatani Siregar dengan judul "Problem dan Pengaturan *Cyber Crime* Melalui Aktifitas Internet dalam Kasus Sara di Pilkada Serentak 2018". Dengan hasil penelitian menunjukkan bahwa problem dan pengaturan *cyber crime* melalui aktivitas internet dalam kasus sara di pilkada serentak 2018 dalam penerapannya lebih tepat menggunakan pasal 28 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dengan ketentuan sanksi pidana pasal 28 ayat (2) diatur dalam pasal 45 ayat (2).<sup>22</sup>

<sup>21</sup> Jhodi Shofian. "*Tinjauan Siyasah Dusturiyah Terhadap Pelaksanaan Kewenangan Cyber Crime Polda Bengkulu dalam Pembentukan Virtual Police.*" Thesis, (UIN Fatmawati Sukarno Bengkulu, 2022)

<sup>22</sup> Bonanda Japatani Siregar. "Problem dan Pengaturan Cyber Crime Melalui Aktifitas Internet dalam Kasus Sara Di Pilkada Serentak 2018." *Jurnal Penelitian Pendidikan Sosial Humaniora* , 3, No.1, (Mei, 24, 2018), 330-336. <https://doi.org/10.32696/jp2sh.v3i1.96>.

Berdasarkan hasil penelitian ini terdapat persamaan dan perbedaan penelitian yang akan dilakukan oleh penulis yaitu keduanya mengkaji satu variable penelitian yang sama yaitu *cyber crime* sedangkan perbedaannya dalam penelitian ini adalah peneliti diatas membahas tentang problem dan pengaturan *cyber crime* dalam kasus sara dipilkada serentak. Sedangkan penelitian yang dilakukan oleh penulis yaitu mengkaji persoalan dalam penanganan Tindak Pidana *Cyber crime* di Indonesia.

4. Agilia Maya Asia Wardani dengan judul “Perlindungan Hukum Terhadap Korban Tindak Pidana Siber (*Cyber Crime*) (Studi Ditreskrimsus Polda Jateng). ”Dengan hasil penelitian ini menyatakan bahwa perlindungan hukum terhadap korban kejahatan siber dapat mengajukan gugatan ganti rugi kerugian berdasarkan pasal 26 ayat (2) UU ITE. Penelitian ini menggunakan metode penelitian kualitatif dengan pendekatan yuridis empiris dan spesifikasi penelitian deskriptif analitis. Penelitian ini mengambil lokasi Direktorat Reserse Kriminal Khusus Kepolisian Daerah Jawa Tengah.<sup>23</sup>

Berdasarkan hasil penelitian yang dilakukan oleh Agilia Maya Asia Wardani terdapat persamaan dan perbedaan penelitian yang akan dilakukan oleh penulis yaitu keduanya mengkaji satu variable penelitian yang sama yaitu *cyber crime* sedangkan perbedaannya dalam penelitian ini adalah peneliti diatas membahas tentang perlindungan hukum terhadap korban kejahatan siber, sedangkan penulis membahas tentang upaya dalam penanganan *cyber crime* di Indonesia.

---

<sup>23</sup>Agilia Maya Asia Wardani. “*Perlindungan Hukum Terhadap Korban Tindak Pidana Siber (Cyber Crime) (Studi Ditreskrimsus Polda Jateng)*. ” Doctoral Dissertation, (Purwokerto: Universitas Jenderal Soedirman, 2021)

5. Indraswari Rahajeng dengan judul “Yurisdiksi Kriminal Berlakunya Hukum Pidana Nasional Terhadap *Cyber Crime* di Luar Yurisdiksi Indonesia”. Dengan hasil penelitian menyatakan bahwa mengenai penerapan yurisdiksi kriminal berlakunya hukum pidana nasional terhadap orang yang melakukan *cyber crime* di luar yurisdiksi Indonesia, sebelum adanya UU ITE telah diatur beberapa peraturan untuk menangani *cyber crime*. Mengenai upaya yang efektif pemberlakuan yurisdiksi yang diperluas untuk menangani *cyber crime* yang terjadi dilintas batas negara, maka digunakan prinsip-prinsip yurisdiksi yaitu prinsip *territorial subjektif*, *territorial objektif*, prinsip nasional aktif maupun nasional pasif, dan prinsip universal. Selain menggunakan prinsip diatas, upaya yang bisa dilakukan untuk menanggulangi kejahatan transnasional yaitu berupa perjanjian *ekstradisi*, *Mutual Legal Assistance* (MLA), dan *transfer for proceeding*. Upaya tersebut hanya bisa dilakukan berdasarkan hubungan baik timbal balik antar negara.<sup>24</sup>

Berdasarkan hasil penelitian diatas terdapat persamaan dan perbedaan penelitian yang akan dilakukan oleh penulis yaitu keduanya mengkaji satu variable penelitian yang sama yaitu *cyber crime* sedangkan perbedaannya dalam penelitian ini adalah peneliti diatas membahas tentang kasus *cyber crime* di luar yurisdiksi Indonesia, sedangkan penelitian yang akan dilakukan oleh penulis yaitu kasus *cyber crime* yang terjadi di wilayah hukum Republik Indonesia.

---

<sup>24</sup> Indraswari Rahajeng . “*Yurisdiksi Kriminal Berlakunya Hukum Pidana Nasional Terhadap Cyber Crime di Luar Yurisdiksi Indonesia*”. Thesis, (Padang: Universitas Andalas)

## F. Deskripsi Teori

### 1. Teori Pidanaan

Teori pidanaan adalah pandangan atau aliran yang berkaitan dengan tujuan pidanaan. Pidanaan kasus *cyber cyber* melibatkan penerapan hukuman pelaku kejahatan dunia maya. Teori-teori pidanaan yang digunakan dalam kasus-kasus *cyber crime* mencakup beberapa pendekatan yang umumnya digunakan dalam sistem hukum.<sup>25</sup>

#### a. Teori Pembalasan/Teori Absolut (*vergeldings theorieen*)

Teori ini diperkenalkan oleh Kent dan Hegel. Menurut teori ini, pidana dijatuhkan semata-mata karena orang telah melakukan kejahatan atau tindak pidana. Teori ini didasarkan pada pemikiran bahwa pidana tidak bertujuan untuk praktis, seperti memperbaiki penjahat tetapi pidana merupakan tuntutan mutlak, bukan hanya sesuatu yang perlu dijatuhkan tetapi menjadi keharusan.

Teori ini berfokus pada keadilan mutlak dan mengaggap bahwa pelaku *cyber crime* harus menerima hukuman yang setimpal dengan tingkat kejahatan yang mereka lakukan. Pidanaan absolut cenderung menerapkan hukuman yang keras sebagai bentuk pembalasan dan pencegahan terhadap kejahatan yang dilakukan. Teori berpandangan bahwa pidanaan berarti pembalasan atas kesalahan yang telah dilakukan. Jadi menurut teori pembalasan itu ditujukan untuk memberikan sebuah hukum kepada pelaku pidana yang mana nantinya akan

---

<sup>25</sup> Adami Chzawi, Pelajaran Hukum Pidana Bagian: Stelse Pidana Tindak Pidana, Teori Pidanaan, dan Batasan Berlakunya Hukum Pidana (Jakarta: PT. Raja Grafindo Persada , 2023), 31.

memberikan efek jera dan ketakutan untuk mengulangi perbuatan pidana tersebut, Pencetus teori ini adalah Imanuel Kant.<sup>26</sup>

b. Teori Tujuan/Teori Relatif (*Doeltheorieen*)

Teori ini berpandangan bahwa pemidanaan bukan sebagai pembalasan atas kesalahan si pelaku, namun sebagai sarana mencapai tujuan yang bermanfaat untuk melindungi masyarakat menuju kesejahteraan. Menurut teori ini, pemidanaan dilaksanakan untuk memberikan suatu maksud dan tujuan suatu pemidanaan, yakni dapat memperbaiki ketidakpuasan masyarakat sebagai akibat perbuatan kejahatan tersebut. Dalam hal ini, teori ini juga mempunyai maksud sebagai pencegahan terjadinya kejahatan dan sebagai perlindungan terhadap masyarakat. Pencetus teori ini yaitu Paul Anselm Van Feurbach yang mengatakan bahwa “hanya dengan mengadakan ancaman pidana saja tidak akan memadai, melainkan diperlukan penjatuhan pidana kepada si penjahat”. Menurut Zevenbergen “terdapat tiga macam memperbaiki si penjahat, yaitu perbaikan yuridis, perbaikan intelektual, dan perbaikan moral.” Perbaikan yuridis mengenai sikap si penjahat dalam menaati Undang-Undang. Perbaikan intelektual mengenai cara berfikir si penjahat agar ia insyaf akan jeleknya kejahatannya. Sedangkan perbaikan moral mengenai rasa kesusilaan si penjahat agar ia bisa menjadi orang yang bermoral tinggi.<sup>27</sup>

Menurut pandangan penulis pendekatan ini bertujuan untuk mencegah kejahatan dengan menghukum pelaku sebagai contoh atau peringatan bagi orang

---

<sup>26</sup> Adami Chzawi, *Pelajaran Hukum Pidana Bagian: Stelse Pidana Tindak Pidana, Teori Pemidanaan, dan Batasan Berlakunya Hukum Pidana* (Jakarta: PT. Raja Grafindo Persada, 2023), 31.

<sup>27</sup> Wirjono Prodjodikoro, *Asas-Asas Hukum Pidana di Indonesia*, (Bandung:Refika Aditama, 2003),26.

lain. Dalam kasus *cyber crime*, hukuman yang berat dapat dijatuhkan untuk memberikan efek jera dan mengurangi tindakan yang membuat orang lain untuk melakukan kejahatan serupa. Teori relatif ini melihat bahwa penjatuhan pidana bertujuan untuk memperbaiki si penjahat agar menjadi orang yang baik dan tidak akan melakukan kejahatan lagi.

c. Teori Gabungan (*veremigingstheorieen*)

Teori ini disatu sisi mengakui adanya unsur pembalasan dalam hukum pidana, tetapi di sisi lain mengakui pula unsur prevensi dan unsur memperbaiki penjahat. Teori gabungan ini lahir sebagai jalan keluar dari teori absolut dan teori relatif yang belum dapat member hasil memuaskan. Aliran ini didasarkan pada tujuan pembalasan namun tetap mempertahankan ketertiban masyarakat secara terpadu. Artinya penjatuhan pidana beralasan pada dua alasan yaitu sebagai suatu pembalasan dan sebagai ketertiban bagi masyarakat.<sup>28</sup> teori ini diperkenalkan oleh Prins, Van Hammel, Van List dengan pandangan sebagai berikut: **pertama** tujuan terpenting pidana adalah memberantas kejahatan sebagai suatu gejala masyarakat. **Dua** ilmu hukum pidana dan perundang-undangan pidana harus memperhatikan studi antropologi dan sosiologis. **Ketiga** pidana ialah suatu dari yang paling efektif yang dapat digunakan pemerintah untuk memberantas kejahatan. pidana bukanlah satu-satunya sarana, oleh karena itu pidana tidak boleh digunakan tersendiri akan tetapi harus digunakan dalam bentuk kombinasi dengan upaya sosialnya.<sup>29</sup>

---

<sup>28</sup> Wirjono Prodjodikoro, *Asas-Asas Hukum Pidana di Indonesia*, (Bandung:Refika Aditama, 2003),27.

<sup>29</sup> Djoko Prakoso, *Alat Bukti dan Kekuatan Pembuktian di dalam Proses Pidana*, (Yogyakarta: Liberty,1988), 47.

Menurut pandangan penulis teori ini berfokus pada rehabilitasi dan resosialisasi pelaku kejahatan dalam kasus *cyber crime*, pendekatan ini dapat melibatkan program-program pemulihan dan pelatihan untuk membantu pelaku memahami dan mengubah perilaku mereka. Tujuan utamanya adalah untuk mencegah pelaku melakukan kejahatan lagi di masa depan.

## 2. Teori Perubahan Hukum dan Perubahan Sosial Steven Vago

*Applied theory* (teori terapan) yang digunakan adalah teori perubahan hukum dan perubahan sosial dari Steven Vago. Menurutnya, perubahan sosial adalah suatu perubahan yang dapat mengubah cara hidup dalam masyarakat, seperti perubahan jenis pekerjaan, perubahan cara mengurus keluarga, perubahan cara mendidik anak, perubahan dalam mengurus hidup, serta perubahan tujuan hidup. Perubahan sosial dapat pula diartikan bahwa telah terjadi perubahan yang mendasar dalam bidang kehidupan yang berhubungan dengan pemerintahan, perekonomian, pendidikan, kepercayaan, kehidupan berkeluarga, hiburan, bahasa, dan kegiatan lainnya.<sup>30</sup>

Salah satu bidang kehidupan yang memberikan peran besar dalam perubahan sosial adalah bidang teknologi. Dikatakan demikian karena banyak sosiolog dan ahli hukum yang berpendapat bahwa perubahan teknologi dalam suatu masyarakat dapat memberikan dampak yang besar kepada perkembangan sistem hukum dalam masyarakat tersebut. misalnya saja dalam hal perkembangan teknologi komputer, dengan adanya perkembangan teknologi tersebut terjadi berbagai perubahan-perubahan dalam cara hidup masyarakat, seperti cara

---

<sup>30</sup> Steven Vago, *Law And Society: Third Edition*, (New Jersey; Prentice Hall, 1991), 215.

berbelanja, cara memproduksi barang, cara menyebarkan informasi dan hal lainnya yang dimana mempengaruhi berbagai bidang kehidupan sehingga diperlukan pembentukan hukum baru untuk mengatur perubahan cara hidup tersebut.<sup>31</sup>

Ketika berbicara mengenai pembentukan hukum, terdapat banyak teori yang dihasilkan oleh berbagai golongan dalam masyarakat. Salah satu teori tersebut adalah teori yang didasarkan pada pendapat golongan rasional. Steven Vago menjelaskan, bahwa menurut teori ini hukum diciptakan dengan serasional mungkin untuk memberikan perlindungan kepada anggota masyarakat dari bahaya. Dalam teori tersebut terdapat suatu masalah, yaitu bahwa batasan bahaya yang dapat berlaku dalam suatu masyarakat ditentukan oleh pembuat hukum dalam masyarakat tersebut. nilai-nilai, syarat, dan hal lain yang mendefinisikan suatu perbuatan dapat ditentukan oleh pembuat hukum sehingga perbuatan yang dilakukan dalam kasus *cyber crime* ini berupa suatu perbuatan melawan hukum. Apabila dapat digambarkan dengan contoh, maka hal tersebut dapat digambarkan dalam bentuk perjudian, pengerusakan, pencurian, tindakan anarkis, terhadap suatu sistem informasi dan komputer dan lain sebagainya, yang dapat dimasukkan dalam perbuatan kriminal.

Kriminalisasi dalam kriminologi dapat diartikan sebagai suatu proses dimana suatu perbuatan dan seseorang individu dijadikan sebagai suatu tindakan kejahatan dan pelaku kejahatan. dalam hal ini, suatu perbuatan yang sebelumnya merupakan perbuatan legal pun dapat dirubah menjadi suatu tindakan kejahatan

---

<sup>31</sup> Steven Vago, *law and society:third edition*, (new jersey;prentice hall, 1991),218.

melalui Peraturan Perundang-Undangan. Oleh karena kriminalisasi merupakan suatu kepastian mengenai perbuatan apa yang boleh dan tidak boleh dilakukan, maka hal tersebut disebarkan kepada masyarakat dalam bentuk hukum sehingga tidak ada seorang pun yang bisa memberikan alasan untuk tidak mengetahuinya dan dapat menghukum mereka yang tidak mematuhi.<sup>32</sup>

### 3. Teori Efektivitas Hukum Soerjono Soekanto

Efektivitas berasal dari kata efektif yang mengandung arti sebagai suatu proses pencapaian suatu tujuan yang telah ditetapkan sebelumnya. Efektivitas hukum berarti bahwa orang benar-benar berbuat sesuai dengan norma hukum sebagai mana mereka harus berbuat, bahwa norma itu benar-benar diterapkan dan dipatuhi<sup>33</sup>. Jadi efektivitas hukum menurut pengertian diatas mengartikan bahwa indikator efektivitas dalam arti tercapainya sasaran atau tujuan yang telah ditentukan sebelumnya merupakan sebuah pengukuran dimana suatu target telah tercapai sesuai dengan apa yang telah direncanakan.

Ketika berbicara sejauh mana efektivitas hukum maka kita pertama-tama harus dapat mengukur sejauh mana aturan hukum itu dimengerti atau tidak dimengerti dan ditaati atau tidak ditaati. Jika suatu aturan hukum dimengerti dan ditaati oleh sebagian besar target yang menjadi sasaran ketaatannya maka akan dikatakan aturan hukum yang bersangkutan efektif.

Teori efektivitas hukum menurut Soerjono Soekanto adalah bahwa efektif atau tidaknya suatu hukum ditentukan oleh 5 (lima) faktor yaitu diantaranya :

---

<sup>32</sup> Steven Vago, *Law And Society: Third Edition*, (New Jersey; Prentice Hall, 1991), 104.

<sup>33</sup> Sabian Usman, *Dasar-Dasar Sosiologi* (Yogyakarta: Pustaka Belajar, 2009), 12.

### 1) Faktor Hukum

Salah satu fungsi hukum adalah untuk menciptakan keadilan, kepastian dan kemanfaatan. Hukum berfungsi sebagai *rechtzekerheid* atau pemberi kepastian hukum, di mana apabila terjadi persoalan dan permasalahan ada kepastian hukum untuk dijadikan pegangan oleh seluruh masyarakat, menjadikan faktor hukum dalam pelaksanaan transaksi elektronik khususnya jika terjadi suatu kejahatan dunia maya (*cyber crime*) dapat menjadi pegangan oleh pihak yang merasa dirugikan. Sebagaimana arti dari kepastian hukum itu sendiri yaitu suatu interpretasi dari hukum tertulis yang dapat dijadikan pedoman kepada masyarakat, sebagai upaya penanggulangan terhadap suatu perbuatan yang dianggap melawan hukum<sup>34</sup>.

### 2) Faktor Penegak Hukum

Faktor kedua yang menentukan efektif atau tidaknya kinerja hukum yaitu adalah aparat penegak hukum. Dalam hubungan ini dikehendaki adanya aparatur yang handal sehingga aparat tersebut dapat melakukan tugasnya dengan baik. Kehandalan dalam kaitannya disini adalah meliputi keterampilan profesional dan mempunyai mental yang baik.

Namun Pengetahuan dan kemampuan penegak hukum dalam bidang teknologi informasi dan komunikasi masih sangat minim. Banyak faktor yang mempengaruhi hal tersebut yaitu diantaranya, kurangnya pengetahuan di bidang IT dan belum memahami teknik kejahatan dunia maya (*cyber crime*), sehingga pada saat pelaku tindak pidana tertangkap, aparat penegak hukum mengalami

---

<sup>34</sup> Arief Hidayat, *Kajian Kritis Hukum Lingkungan di Era Otonomi Daerah*, (Semarang : Universitas Diponegoro, 2007), 68.

kesulitan untuk menemukan alat bukti yang dapat dipakai untuk menjerat pelaku, terlebih apabila kejahatan yang dilakukan memiliki sistem pengoperasian yang sangat rumit. Penegak hukum tidak dapat berdiri sendiri dalam penanganan *cyber crime* di karenakan keterbatasan dalam beberapa hal seperti halnya pengetahuan dan pengalaman dalam menangani kasus *cyber crime* serta kemampuan teknis yang dibutuhkan dalam melakukan pelacakan (*tracking*) terhadap pelaku *cyber crime*.<sup>35</sup>

Untuk menangani kasus *cyber crime* diperlukan penyidik atau penegak hukum yang mempunyai cukup pengalaman, serta mempunyai dasar-dasar pengetahuan dan kemampuan di bidang IT untuk mengetahui modus operandi, profil dan metode penyerangan para *hacker*, diperlukan juga peralatan *Forensik Computing* yang canggih guna pembuktian kejahatan *cyber*, dan menyiapkan penyidik Polri untuk dididik agar mampu menyelidiki *cyber crime* serta meningkatkan upaya penyidikan dan membangun kerja sama internasional.<sup>36</sup>

### 3) Faktor Sarana dan Fasilitas Pendukung

Faktor ketiga yaitu faktor sarana atau fasilitas yang membantu penegak hukum, menurut Soerjono Soekanto sendiri menyatakan bahwa tidak mungkin penegak hukum akan berlangsung dengan lancar tanpa adanya sarana atau fasilitas yang mendukung. Sarana atau fasilitas tersebut antara lain, mencakup tenaga

---

<sup>35</sup> Soerjono Soekanto, *Faktor-Faktor Yang Mempengaruhi Penegak Hukum*, (Jakarta: UI Press, 1983).64

<sup>36</sup> Agus Raharjo, *Cyber Crime: Pemahaman dan Upaya Pencegahan Penyalahgunaan Komputer*, (Jakarta: Universitas Atma Jaya, 1999), 112.

manusia yang berpendidikan dan terampil, organisasi yang baik, peralatan yang memadai, dan sebagainya.<sup>37</sup>

Jika fasilitas pendukung tidak terpenuhi maka mustahil penegak hukum akan mencapai tujuannya. Kepastian dan kecepatan penyelesaian perkara tergantung pada fasilitas pendukung yang ada dalam bidang pencegahan dan pemberantasan kejahatan. Untuk itu Faktor sarana atau fasilitas khusus untuk kepentingan penyidikan tindak pidana *cyber crime* mutlak di perlukan, khususnya oleh penyidik Polri karena pada tahap penyelidikan dan/atau penyidikan.

#### 4) Faktor Masyarakat

Selain dari pihak yang berkaitan dengan hukum, penegak hukum juga berasal dari masyarakat dan bertujuan untuk mencapai kedamaian dalam masyarakat di negara itu sendiri khususnya Indonesia. Sebagaimana diketahui bahwa dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 dijelaskan bahwa Indonesia merupakan negara hukum, sehingga turut serta masyarakat dapat membantu mencapai kedamaian di dalam masyarakat itu sendiri. Setiap masyarakat sedikitnya dinilai wajib memiliki kesadaran atas hukum yang membuat mereka menjadi taat kepada hukum. Adanya derajat kepatuhan hukum masyarakat terhadap hukum, merupakan salah satu indikator berfungsinya hukum yang bersangkutan.<sup>38</sup>

Namun dalam hal ini perlu diketahui bahwa dalam berjalannya transaksi elektronik saat ini, masih beberapa orang saja yang memang memahami akan

---

<sup>37</sup> Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, (Jakarta: Rajawali Press,2006).

<sup>38</sup> Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, (Jakarta: Rajawali Press,2006).

konsekuensi tersebut, sehingga pemahaman tentang perbuatan yang boleh dan tidak boleh dilakukan sebagaimana diatur dalam Peraturan Perundang-Undangan terkait transaksi elektronik tidak dipahami olehnya. Begitu juga terhadap apa yang harus dilakukan sebagai langkah pencegahan dalam menghadapi perkembangan teknologi yang saat ini sedang banyak digunakan.

#### 5) Faktor Kebudayaan

Faktor lain yang banyak mempengaruhi berjalannya suatu kaidah hukum adalah nilai kebudayaan. Kebudayaan menurut Soerjono Soekanto, mempunyai fungsi yang sangat besar bagi masyarakat, yaitu mengatur agar masyarakat dapat mengerti bagaimana seharusnya bertindak, berbuat, dan menentukan sikapnya kalau mereka berhubungan dengan orang lain. Dengan demikian, kebudayaan adalah suatu garis pokok tentang perikelakuan yang menetapkan peraturan mengenai apa yang harus dilakukan, dan apa yang dilarang.

Kelima faktor tersebut diatas merupakan yang secara keseluruhan harus terpenuhi, di mana keterkaitan antar faktor tersebut berjalan dengan sangat erat, bahkan menjadi suatu hal pokok dalam penegakan hukum, serta sebagai tolak ukur efektivitas penegak hukum. Adapun penjelasan terkait teori efektivitas hukum oleh Soerjono Soekanto tersebut diatas relevan dengan teori yang dikemukakan oleh Romli Atma sasmita yaitu bahwa faktor-faktor yang menghambat efektivitas penegakan hukum tidak hanya terletak pada sikap mental aparatur penegak hukum saja, akan tetapi terletak juga pada faktor sosialisasi hukum yang sering diabaikannya itu biasa berupa faktor masyarakat, faktor

penunjang sarana dan fasilitas maupun dari faktor kebudayaan yang ada pada masyarakat<sup>39</sup>.

## **G. Metode Penelitian**

### **1. Jenis dan Pendekatan Penelitian**

#### **a. Jenis Penelitian**

Jenis penelitian yang digunakan adalah penelitian normatif. Normatif adalah kerangka Peraturan Perundang-Undangan, pembuktian melalui pasal, teori, pembuktian melalui masyarakat. penggunaan jenis penelitian normatif dalam penelitian ini dapat di lihat dari aspek normatif yakni mencoba menganalisis permasalahan yang ada pada norma dan teori tersebut. penelitian yang menggunakan bahan kepustakaan sebagai bahan utama yang mengkaji Peraturan Perundang-Undangan, bahan pustaka, dokumen, atau data sekunder yang ada<sup>40</sup>.

Penelitian ini berdasarkan data sekunder dengan menggunakan bahan penelitian berupa buku serta tulisan lain seperti jurnal, artikel, tesis, dan Skripsi yang berhubungan dengan objek penelitian yaitu Tinjauan Yuridis Tindak Pidana *Cyber Crime* di Indonesia.

#### **b. Pendekatan Penelitian**

Metode pendekatan yang digunakan dalam penelitian ini adalah:

##### **1. Pendekatan Perundang-Undangan (*Statute Approach*)**

Pendekatan Perundang-Undangan adalah melakukan penelitian melalui peraturan perundang-undangan, pendekatan ini digunakan untuk menganalisis

---

<sup>39</sup> Romli Atma Sasmita, *Reformasi Hukum Hak Asasi Manusia & Penegakan Hukum*, (Bandung : Mandar Maju, 2001), 55.

<sup>40</sup> Johnny Ibrahim, *Teori dan Metode Penelitian Hukum Normatif*, (Jakarta: Bayumedia Publishing, 2005), 241.

materi atau permasalahan yang bersangkutan paut dengan isu hukum tersebut atau yang sedang diteliti.

## 2. Pendekatan Konseptual (*Conceptual Approach*)

Pendekatan konseptual merupakan pendekatan yang beranjak dari pandangan-pandangan dan doktrin-doktrin yang berkembang didalam ilmu hukum, guna menemukan ide-ide yang melahirkan pengertian, konsep, dan asas hukum yang relevan, sebagai sandaran dalam membangun suatu argumentasi hukum dalam memecahkan isu hukum yang dihadapi.

## 2. Jenis dan Sumber Data

Jenis dan Sumber data dalam penelitian adalah subjek dari mana data tersebut diperoleh<sup>41</sup>. Sumber data yang diperoleh dalam penelitian ini adalah data yang berasal dari sumber kepustakaan. Data yang digunakan dalam penelitian ini terdiri dari bahan hukum primer, sekunder, dan tersier.

### 1. Bahan Hukum Primer

Bahan hukum primer yaitu bahan hukum yang mempunyai kekuatan hukum yang tetap dan mengikat yang terdiri dari norma-norma dasar atau kaidah dasar, peraturan dasar, Peraturan Perundang-Undangan dan sebagainya. Bahan hukum primer terkait penelitian yang dilakukan oleh penulis antara lain: Kitab Undang-Undang Hukum Pidana (KUHP), Kitab Undang-Undang Hukum Acara Pidana (KUHAP), Undang-Undang Nomor 19 Tahun 2016 atas perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

---

<sup>41</sup> Suharsimi Arikunto, *Prosedur Penelitian Suatu Pendekatan*, (Jakarta: Rineke Cipta, 2002), 107.

## 2. Bahan Hukum Sekunder

Sumber data sekunder adalah sumber data pokok berupa referensi yang membahas masalah yang berkaitan dengan judul penelitian, misalnya berupa buku-buku, rancangan Undang-Undang, hasil penelitian, hasil karya dari kalangan hukum.<sup>42</sup> Dapat pula berupa Al-Qur'an dan hadist, karya ilmiah dari akademisi, jurnal dan majalah terkait penelitian, website serta hasil penelitian yang berhubungan dengan masalah penelitian ini.

## 3. Bahan Hukum Tersier

Data tersier adalah sejumlah informasi yang mendukung sumber data primer dan sekunder atau buku penunjang yang berfungsi untuk memperluas wawasan berkaitan dengan pemecahan masalah penelitian. Yaitu seperti kamus bahasa Indonesia, internet, buku penelitian hukum, ensiklopedia dan sebagainya.

### 3. Teknik Pengumpulan Data

Teknik pengumpulan data adalah cara atau metode yang digunakan dalam pengumpulan data berupa pencatatan peristiwa, hal-hal, keterangan atau karakteristik dari sebagian atau seluruh elemen masyarakat. Pengumpulan data ini bertujuan untuk memperoleh informasi yang dibutuhkan dalam rangka mencapai tujuan penelitian.<sup>43</sup> Mengingat penelitian ini adalah penelitian yang bersifat Yuridis Normatif yang memusatkan perhatian pada data sekunder, maka Teknik pengumpulan data yang digunakan dalam penelitian ini dititik beratkan pada penelitian kepustakaan (*Library Research*) yaitu pengumpulan data melalui buku-buku, kamus-kamus hukum, Undang-Undang, dan jurnal-jurnal hukum, dan

---

<sup>42</sup> Soerjono Soekanto, *Pengantar Penelitian Hukum*, No. Edisi 3 (Jakarta: UI Pres, 1986), 52.

<sup>43</sup> W. Gulo, *Metodologi Penelitian*, (Jakarta: Pt. Grasindo, 2005), 110.

dokumen lain serta media tulis lainnya yang mempunyai kaitannya dengan penelitian ini yang dilakukan dengan dua cara yaitu dengan kutipan langsung dan kutipan tidak langsung.

#### **4. Teknik Pengelolaan dan Analisis Data**

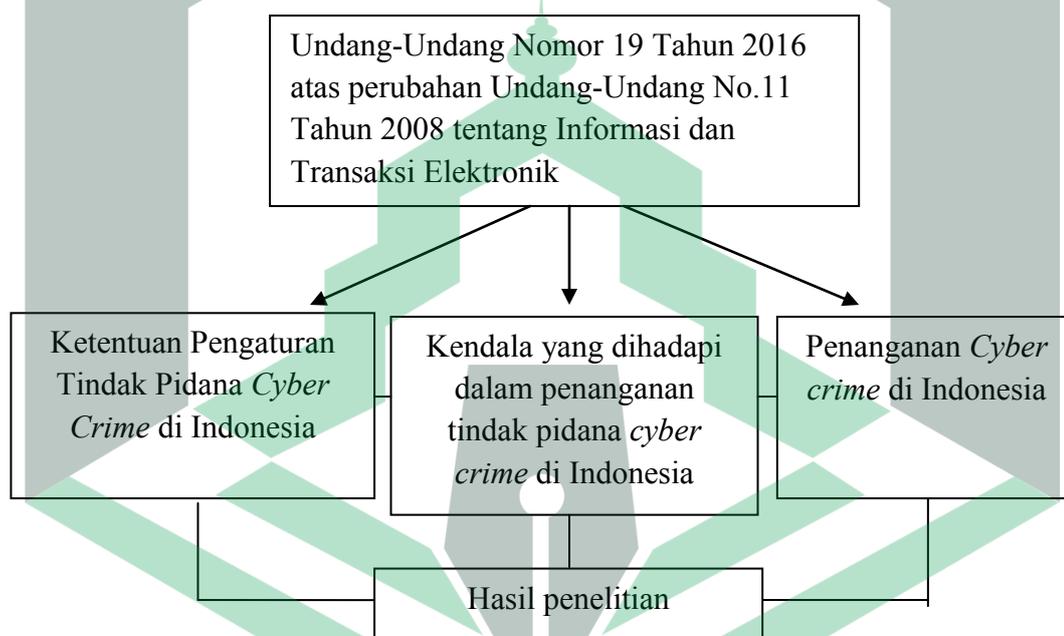
Analisis data yaitu menguraikan data dalam bentuk kalimat yang baik dan benar sehingga mudah dibaca dan diinterpretasikan. Teknik analisis data yang digunakan dalam penelitian ini dilakukan dengan cara deskriptif kualitatif. Teknik pengelolaan dan analisis data yang diperoleh dengan menggunakan langkah-langkah sebagai berikut:

1. Mengidentifikasi data, setelah semua data yang terkait penelitian dikumpulkan, kemudian data diidentifikasi dengan menandai data yang relevan dalam penelitian ini.
2. Klasifikasi data, yaitu menempatkan data tersebut dalam kelompok-kelompok yang sesuai sehingga bisa diperoleh data yang objektif dan sistematis terhadap penelitian.
3. *Analyzing*, yaitu proses menganalisa terhadap seluruh data yang diperoleh dalam penelitian ini.
4. *Editing*, yaitu memeriksa serta memperbaiki data yang dianggap salah dalam penelitian ini. Setelah data ini disusun sistematis dan sesuai dengan pokok-pokok bahasan dalam penelitian, maka data-data yang disusun dianalisis secara kualitatif deskriptif yaitu menafsirkan data-data dalam model uraian kalimat sehingga data ini mampu memberikan penjelasan mengenai

permasalahan yang dimaksud. Sehingga dapat ditarik kesimpulan yang akan menjawab permasalahan dari penelitian ini.

## H. Kerangka Pikir

Kerangka pikir merupakan suatu diagram yang menjelaskan secara garis besar alur logika perjalanan sebuah penelitian. Kerangka pikir dibuat berdasarkan pertanyaan penelitian (*research question*) dan mempresentasikan suatu himpunan dari beberapa konsep serta hubungan diantara konsep-konsep tersebut<sup>44</sup>. Skema kerangka pikir dalam penelitian ini adalah sebagai berikut:



**Gambar 2.1 Kerangka pikir**

Penelitian ini untuk mengetahui bahwa Indonesia telah memiliki Undang-Undang Khusus yang menyangkut teknologi informasi dan transaksi elektronik yang mengatur Kejahatan Dunia Maya (*cyber crime*), yaitu Undang-Undang Nomor 19 Tahun 2016 atas perubahan Undang-Undang No.11 Tahun 2008

<sup>44</sup> Gregor Polancik, *Empirical Research Method Poster*, (Jakarta: Gema Insani, 2008),

tentang Informasi dan Transaksi Elektronik, yang membahas tentang tata cara, batasan penggunaan komputer dan sanksi yang akan diberikan jika terdapat pelanggaran. Seperti halnya masuk dan mengakses jaringan komputer orang lain tanpa izin yang mana hal tersebut dapat merugikan orang lain.

Kerangka pikir yang menjadi garis besar dalam penelitian ini adalah *cyber crime* yang pernah terjadi di Indonesia. Beberapa tahun terakhir perkembangan teknologi komunikasi dan informasi berkembang dengan pesat, hampir dalam segala bidang. Munculnya berbagai penemuan baru memberikan kemudahan dalam kehidupan manusia, khususnya pada bidang komunikasi komunikasi dengan ditemukannya internet yang memberikan dampak yang cukup besar. Dengan adanya internet bukan hanya memberikan manfaat terhadap kehidupan manusia, namun juga memunculkan dampak negatif yang tidak dapat dihindari. Salah satu dampak negatif yang muncul dari adanya internet adalah munculnya kasus *cyber crime*.

Berdasarkan keadaan tersebut, peneliti tertarik untuk melakukan penelitian tentang bagaimana tinjauan yuridis tindak pidana yang terjadi pada media internet (*Cyber crime*) di Indonesia, serta kendala yang di hadapi dalam penanganan tindak pidana *cyber crime* di Indonesia, dan bagaimana penanganan tindak pidana *cyber crime* di Indonesia.

## **I. Definisi Istilah**

Berhubungan dengan istilah seringkali menimbulkan bermacam-macam penafsiran, maka penulis merasa perlu mendefinisikan terlebih dahulu beberapa istilah yang digunakan dalam Skripsi ini. Istilah pokok yang dijelaskan antara lain:

1. Tinjauan Yuridis adalah segala sesuatu yang berkaitan dengan hukum yang berkaitan dengan tindak pidana *Cyber Crime*.
2. Tindak pidana adalah suatu perbuatan yang dilarang oleh suatu aturan hukum yang mana disertai ancaman (sanksi) dan dapat dikenai hukuman pidana bagi barang siapa melanggar larangan tersebut”. dan pelakunya ini dapat dikatakan merupakan “subjek” tindak pidana.
3. *Cyber crime* merupakan segala macam pengguna jaringan komputer untuk tujuan kriminal atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital. *Cyber crime* dapat dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/atau suatu computer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Kejahatan komputer diasosiasikan dengan *Hacker*, biasanya menimbulkan arti yang negatif.

## **BAB II**

### **KETENTUAN TINDAK PIDANA *CYBER CRIME* DI INDONESIA**

#### **A. Konsep Tindak Pidana**

##### **1. Pengertian Tindak Pidana**

Tindak pidana atau biasa disebut dengan kejahatan merupakan fenomena masyarakat karena itu tidak dapat dilepaskan dari ruang dan waktu. Menurut *Van Hamel*, tindak pidana adalah kelakuan orang yang dirumuskan dalam undang-undang, yang bersifat melawan hukum, yang patut dipidana dan dilakukan dengan kesalahan. Dalam pemerintahan suatu negara pasti diatur mengenai hukum dan pemberian sanksi atas pelanggaran hukum tersebut. hukum merupakan keseluruhan kumpulan peraturan-peraturan atau kaedah-kaedah dalam suatu kehidupan bersama yang dapat dipaksakan pelaksanaannya dengan suatu sanksi.<sup>45</sup>

Tindak pidana sebagai fenomena sosial yang terjadi di muka bumi mungkin tidak akan pernah berakhir sejalan dengan perkembangan dan dinamika sosial yang terjadi dalam masyarakat. Masalah tindak pidana ini nampaknya akan terus berkembang dan tidak akan pernah surut, baik dilihat dari segi kualitas maupun kuantitasnya, perkembangan ini menimbulkan keresahan bagi masyarakat dan pemerintah. Tindak pidana merupakan suatu bentuk perilaku menyimpang yang selalu ada dan melekat pada setiap bentuk masyarakat, dalam arti bahwa tindak pidana akan selalu ada seperti perlu lebih ditingkatkan dan diupayakan secara terarah dan terpadu, antara lain kodifikasi dan unifikasi bidang-bidang

---

<sup>45</sup> Sudikno Mertokusomo, *Mengenal Hukum*, (Yogyakarta: Liberty Yogyakarta, 2003), 40.

hukum tertentu serta penyusunan Perundang-Undangan baru yang sangat dibutuhkan guna menjawab semua tantangan dari semakin meningkatnya kejahatan dan perkembangan tindak pidana. Berbagai macam tindak pidana yang terjadi dalam masyarakat salah satunya adalah kejahatan penipuan, bahkan dewasa ini banyak sekali terjadi tindak pidana penipuan dengan berbagai macam bentuk dan perkembangannya. Yang menunjuk pada semakin tingginya tingkat intelektualitas dari kejahatan penipuan yang semakin kompleks. Hal ini berarti setiap individu harus menaati peraturan-peraturan yang ditetapkan oleh pemerintah di dalam berlangsungnya kehidupan bermasyarakat dan bernegara.

Perundang-Undangan memegang peran dalam berbagai bidang dalam kehidupan manusia. Kemajuan budaya ilmu pengetahuan dan teknologi (*IPTEK*), perilaku manusia didalam kehidupan bermasyarakat dan bernegara justru semakin kompleks, perilaku yang demikian apabila ditinjau dari segi hukum, tentunya ada perilaku yang sesuai dengan norma dan ada yang dapat dikategorikan sebagai bentuk pelanggaran dari norma. Perilaku yang menyimpang dari norma biasanya akan menjadikan suatu permasalahan baru dibidang hukum dan merugikan masyarakat.<sup>46</sup> Istilah tindak pidana sebagai terjemahan dari istilah *strafbaar feit* atau *delic*, tetapi didalam berbagai Perundang-Undangan yang berlaku di Indonesia, dikenal dengan istilah-istilah yang tidak seragam dalam menerjemahkan *strafbaar feit*, adapun beberapa istilah yang diperlukan dalam bahasa Indonesia diantaranya sebagai berikut. Tindak pidana merupakan suatu istilah yang mengandung suatu istilah yang mengandung suatu pengertian dasar

---

<sup>46</sup> Bambang Wahyo, *Tindak Pidana dan Pemidanan*, (Jakarta: Sinar Grafika, 2000), 3.

dalam ilmu hukum, para pakar hukum pidana menggunakan istilah “tindak pidana” dengan istilah: **Pertama** *strafbaar feit* adalah peristiwa pidana. **Kedua** *Strafbaar Handlung* adalah perbuatan kriminal, **Ketiga** *Criminal Act* adalah perbuatan kriminal. Tindak pidana merupakan suatu bentuk perilaku menyimpang yang selalu ada dan melekat pada setiap bentuk masyarakat, dalam arti bahwa tindak pidana akan selalu ada setiap penyakit dan kematian yang selalu berulang seperti halnya dengan musim yang selalu berganti dari tahun ke tahun.<sup>47</sup>

Secara keseluruhan perbedaan yang mendasar antara *wetboek van strafrecht* dan Undang-Undang No.1 Tahun 2023 adalah filosofi yang mendasari dibentuknya *wetboek van strafrecht* dilandasi oleh pemikiran aliran klasik yang berkembang pada abad ke-18 yang memusatkan perhatian hukum pidana pada perbuatan atau tindak pidana. Sedangkan UU No. 1 Tahun 2023 mendasarkan diri pada pemikiran aliran neo-klasik yang menjadi keseimbangan antara faktor objektif (perbuatan/lahiriah) dan faktor subjektif (orang/batiniah). Dengan telah diterapkannya UU No.1 Tahun 2023, diharapkan dapat terwujud usaha pembangunan hukum nasional yang dilakukan secara terarah, terpadu, dan terencana sehingga dapat mendukung pembangunan nasional di berbagai bidang sesuai dengan tuntutan pembangunan serta tingkat kesadaran hukum dan dinamika yang berkembang dalam masyarakat.

Istilah tindak pidana sebagai terjemahan dari *strafbaar feit* yang dikenal dalam hukum pidana belanda. *Strafbaar feit*, didalam Kitab Undang-Undang Hukum Pidana tidak terdapat penjelasan mengenai apa sebenarnya yang dimaksud

---

<sup>47</sup> Susilo, Kriminologi (*Pengetahuan Tentang Sebab-Sebab Kejahatan*), (Bogor: Politeia, 1985.

dengan *Strafbaar feit* itu sendiri. Biasanya tindak pidana disinonimkan dengan delik, yang berasal dari bahasa latin yakni kata *delictum*.<sup>48</sup> Delik dalam bahasa belanda disebut *strafbaar feit*, terdiri atas tiga kata, yaitu *straf*, *baar*, *feit*. Yang masing-masing memiliki arti, *straf* diartikan sebagai pidana atau hukum, *baar* diartikan sebagai dapat dan boleh, *feit* diartikan sebagai tindak, peristiwa, pelanggaran dan perbuatan. Jadi istilah *strafbaar feit* sebagai peristiwa yang dapat dipidana atau perbuatan yang dapat dipidana.<sup>49</sup>

Jonkers merumuskan bahwa *strafbaar feit* sebagai peristiwa pidana yang diartikannya sebagai suatu perbuatan yang melawan hukum yang berhubungan dengan kesengajaan atau kesalahan yang dilakukan oleh orang yang dapat dipertanggungjawabkan.<sup>50</sup>

Moeljatno menggunakan istilah perbuatan pidana dalam menerjemahkan kata *strafbaar feit*. Perbuatan pidana adalah suatu perbuatan yang dilarang oleh aturan hukum yang disertai ancaman (sanksi) bagi setiap orang yang melanggar larangan tersebut. Dapat juga dikatakan bahwa perbuatan pidana adalah perbuatan yang mana suatu aturan hukum yang dilarang dan diancam pidana, perlu diingat bahwa larangan ditujukan kepada perbuatan (yaitu suatu keadaan atau kejadian yang ditimbulkan oleh perbuatan seseorang), sedangkan ancaman pidananya ditujukan kepada seseorang yang menimbulkan kejadian tersebut. Penggunaan kata perbuatan sebagai suatu pengertian abstrak yang menunjuk kepada dua

---

<sup>48</sup> Teguh Prasetyo, *Hukum Pidana*, (Jakarta: Rajawali Pers,2016),47.

<sup>49</sup> Amir Ilyas, *Asas-Asas Hukum Pidana:Memahami Tindak Pidana dan Pertanggungjawaban Pidana Sebagai Syarat Pemidanaan*, (Yogyakarta: Rangkap Education Yogyakarta & Pukap-Indonesia,2012),19.

<sup>50</sup> Amir Ilyas, *Asas-Asas Hukum Pidana:Memahami Tindak Pidana dan Pertanggungjawaban Pidana Sebagai Syarat Pemidanaan*, (Yogyakarta: Rangkap Education Yogyakarta & Pukap-Indonesia,2012),20

keadaan konkret yaitu pertama, adanya kejadian tertentu dan kedua, adanya orang yang berbuat yang menimbulkan kejadian tersebut.<sup>51</sup>

Menurut Pompe, perkataan *strafbaar feit* itu secara teoritis dapat dirumuskan sebagai suatu pelanggaran norma (gangguan terhadap tata tertib hukum) yang sengaja ataupun tidak dengan sengaja telah dilakukan oleh seorang pelaku, dimana penjatuhan hukuman terhadap pelaku tersebut adalah perlu demi terpeliharanya tertib hukum dan terjaminnya kepentingan umum.<sup>52</sup> Simons telah merumuskan *strafbaar feit* itu sebagai suatu tindakan melanggar hukum yang telah dilakukan dengan sengaja atau ataupun tidak sengaja oleh seseorang yang dapat mempertanggungjawabkan atas tindakannya yang mana oleh undang-undang telah dinyatakan sebagai suatu tindakan yang dapat dihukum.<sup>53</sup> Alasan dari Simons apa sebabnya *strafbaar feit* itu harus dirumuskan diatas adalah pertama, untuk adanya suatu *strafbaar feit* itu diisyaratkan bahwa disitu harus terdapat suatu tindakan yang dilarang maupun yang diwajibkan oleh Undang-Undang, dimana pelanggaran terhadap larangan semacam itu telah dinyatakan sebagai suatu tindakan yang dapat dihukum, dan kedua, agar suatu tindakan itu dapat dihukum, maka tindakan tersebut harus memenuhi semua unsur dari delik seperti yang dirumuskan dalam Undang-Undang, dan setiap *strafbaar feit* sebagai pelanggaran terhadap pelanggaran atau kewajiban menurut undang-undang itu, pada hakikatnya merupakan suatu tindakan melawan hukum.<sup>54</sup>

---

<sup>51</sup> Moeljanto, *Asas-Asas Hukum Pidana*, (Jakarta: PT.Rineka Cipta,2008), 59.

<sup>52</sup> P.A.F Lamintang dan Franciscus Theojunior Lamintang, *Dasar-Dasar Hukum Pidana di Indonesia*, (Jakarta: Sinar Grafika,2014),180.

<sup>53</sup> P.A.F Lamintang dan Franciscus Theojunior Lamintang, *Dasar-Dasar Hukum Pidana di Indonesia*, (Jakarta: Sinar Grafika,2014),183.

Beberapa penjelasan para ahli dalam memberikan pengertian mengenai tindak pidana, dapat disimpulkan bahwa tindak pidana adalah suatu perbuatan yang melawan hukum atau tindakan yang salah terhadap suatu larangan dan kewajiban yang tercantum dalam undang-undang yang sifatnya dilakukan dengan sengaja ataupun tidak dengan sengaja dan memenuhi seluruh unsur-unsur dari delik.

## 2. Pengertian Hukum Pidana

Hukum pidana yaitu bagian dari keseluruhan hukum yang berlaku di suatu negara, yang mengadakan dasar-dasar dan peraturan untuk menentukan perbuatan-perbuatan yang tidak boleh dilakukan, menentukan kapan dan hal apa kepada mereka yang telah melanggar larangan yang dapat dikenakan atau dijatuhi pidana sebagaimana yang telah diancamkan, menentukan dengan cara bagaimana pengenaan pidana itu dapat dilakukan apabila ada orang yang disangka telah melanggar.

Istilah tindak pidana adalah sebagai terjemahan dari istilah bahasa belanda yaitu "*strafbaarfeit*" atau "*delict*". Di dalam bahasa Indonesia dari *strafbaar feit* atau *delict* terdapat beberapa istilah: 1) Tindak pidana, 2). Perbuatan pidana, 3). Peristiwa pidana, 3). Pelanggaran pidana, 4). Perbuatan yang boleh dan dapat dihukum.

Adapun beberapa pendapat yang dikemukakan para sarjana dan para ahli mengenai tindak pidana yaitu diantaranya sebagai berikut:

1. Wirjono Prodjodikoro, berpendapat bahwa tindak pidana adalah suatu perbuatan yang pelakunya bisa di kenakan hukuman pidana.

2. Muljatno berpendapat bahwa perbuatan pidana adalah suatu perbuatan yang dilarang oleh suatu aturan hukum, yang mana larangan ini disertai dengan ancaman (sanksi) yang berupa pidana tertentu, bagi siapa saja yang melanggar larangan tersebut.
3. R. Tresna mengemukakan bahwa peristiwa pidana adalah sesuatu perbuatan atau serangkaian perbuatan manusia, yang bertentangan dengan undang-undang atau peraturan-peraturan lainnya, terhadap perbuatan mana yang bisa dilakukan tindakan penghukuman.<sup>55</sup>

Pengertian tindak pidana menurut Simons ialah suatu tindakan atau perbuatan yang diancam dengan pidana oleh undang-undang, bertentangan dengan hukum dan dilakukan dengan kesalahan oleh orang yang mampu bertanggungjawab. Sedangkan Menurut Van Hamel tindak pidana merupakan perbuatan manusia yang melakukan kesalahan dengan perbuatan melawan hukum yang dirumuskan dalam Undang-Undang, dan patut untuk dikenakan pidana.<sup>56</sup>

Tindak pidana dapat juga dikatakan suatu perbuatan pidana yang memiliki definisi sebagai berikut: “perbuatan yang dilarang oleh suatu aturan hukum, yang mana larangan ini disertai dengan ancaman (sanksi) yang berupa pidana tertentu bagi siapa saja yang melanggar larangan tersebut”.

Suatu tindak pidana dibagi menjadi tiga bagian, yaitu:<sup>57</sup>

---

<sup>55</sup> Teguh Prasetyo, *Hukum Pidana*, (Jakarta: PT. Raja Grafindo Persada, 2016), 137.

<sup>56</sup> Agus Rusianto, *Tindak Pidana dan Pertanggungjawaban Pidana*, ( Jakarta : Kencana, 2016), 2.

<sup>57</sup> Laden Marpaung, *Asas Teori Praktik Hukum Pidana*, (Jakarta: Sinar Grafika,2008),15.

- a. Tindak pidana terhadap ketertiban umum yaitu mencakup keamanan negara, martabat kepala negara, kekuasaan umum, tata tertib, peradilan keuangan, materai dan cap.
- b. Tindak pidana terhadap kesusilaan
- c. Tindak pidana terhadap orang yang mencakup rahasia pribadi, kehormatan, perlindungan terhadap nyawa dan lain sebagainya.

### 3. Unsur-Unsur Tindak Pidana

Suatu Peraturan Perundang-Undangan pidana selalu mengatur tentang tindak pidana. Perefleksian suatu tindak pidana berdasarkan hukum positif ialah peristiwa yang ditentukan berdasarkan aturan Undang-Undang tertentu dan dapat menyebabkan seseorang dijatuhi hukuman. Supaya suatu perbuatan yang dilakukan seseorang dapat dipidana sesuai dengan ketentuan yang berlaku, maka dalam perbuatan tersebut harus dipenuhi semua unsur pidana dari delik sebagaimana yang telah dirumuskan sebelumnya. Dimana dalam hal ini, secara garis besar menurut para teoritis, unsur tindak pidana terbagi menjadi 2 (dua) yakni unsur subjektif dan unsur objektif.<sup>58</sup>

Adapun maksud dari unsur subjektif yaitu unsur yang melekat atau berkaitan dengan diri si pelaku dan termasuk segala sesuatu yang terkandung di dalamnya. Sedangkan, unsur objektif ialah segala unsur yang berkaitan dengan keadaan tertentu diluar diri si pelaku yang berhubungan dengan perbuatan atau

---

<sup>58</sup>Amir Ilyas, *Asas-Asas Hukum Pidana: Memahami Tindak Pidana dan Pertanggungjawaban Pidana Sebagai Syarat Pemidanaan*, (Yogyakarta: Rangkang Education Yogyakarta & Pukap-Indonesia,2012),45.

tindakan yang harus dilakukan, dimana perbuatan atau tindakan tersebut dalam hal ini bertentangan dengan ketentuan Perundang-Undangan.<sup>59</sup>

Menurut Simons, unsur-unsur tindak pidana (*strafbaar feit*) adalah:

1. Perbuatan manusia (positif atau negatif, berbuat atau tidak berbuat atau membiarkan).
2. Diancam dengan pidana (*strafbaar gesteld*)
3. Melawan hukum (*onrechtmatig*)
4. Dilakukan dengan kesalahan oleh orang yang mampu bertanggungjawab

Simons juga menyebutkan adanya unsur objektif dan unsur subjektif dari tindak pidana (*strafbaar feit*).

Unsur Objektif :

- a) Perbuatan orang
- b) Akibat yang kelihatan dari perbuatan itu.
- c) Mungkin ada keadaan tertentu yang menyertai perbuatan itu seperti dalam pasal 281 KUHP sifat “*openbaar*” atau “*dimuka umum*”

Unsur Subjektif

- a) Orang yang mampu bertanggung jawab
- b) Adanya kesalahan (*dollus atau culpa*)
- c) Perbuatan harus dilakukan dengan kesalahan

Kesalahan ini dapat berhubungan dengan akibat dari perbuatan atau dengan keadaan mana perbuatan itu dilakukan. Sementara menurut Moeljatno unsur-unsur perbuatan pidana:

---

<sup>59</sup>S.R.Sianturi, *Asas-Asas Hukum Pidana di Indonesia dan Penerapannya*, (Jakarta:PT.Citra Aditya Bakti, 1996),205.

- a) Perbuatan (manusia)
  - b) Yang memenuhi rumusan dalam Undang-Undang (syarat formal)
  - c) Bersifat melawan hukum (syarat materil).<sup>60</sup>
4. Perbandingan KUHP
    - a. KUHP Lama

KUHP merupakan salah satu produk hukum peninggalan kolonial Hindia Belanda. Induk peraturan hukum pidana Indonesia adalah Kitab Undang-Undang Hukum Pidana (KUHP), awalnya KUHP bernama *Wetboek Van Strafrecht voor Nederlandsch Indie* (WvSNI) yang diberlakukan di Indonesia pertama kali dengan *Koninklijk Besluit* (Titah Raja) No. 33 peraturan WvSNI ini dibentuk pada tanggal 15 Oktober 1915, namun baru diberlakukan pertama kali sejak tanggal 1 Januari 1918. WvSNI merupakan turunan dari WvS negeri Belanda yang dibuat pada tahun 1881 dan diberlakukan di negara Belanda pada tahun 1886, walaupun WvSNI ini nota bene turunan dari WvS Belanda, tetapi pemerintah kolonial pada saat itu menerapkan asas konkordansi (penyesuaian) bagi pemberlakuan WvS di negara jajahannya. Namun selama WvSNI diberlakukan, masih terdapat unsur-unsur kolonial di dalamnya. Misalnya, terdapat aturan tentang kerja rodi dan denda yang digunakan masih dalam mata uang gulden yang digunakan di Hindia Belanda (Indonesia) saat itu. Setelah Indonesia merdeka tanggal 17 Agustus 1945, para pendiri bangsa mencoba merumuskan hukum pidana yang akan diberlakukan di Indonesia sebagai negara yang berdaulat. Tanggal 26 Februari 1946, WvSNI diubah menjadi Kitab Undang-Undang Hukum Pidana (KUHP) lewat UU No. 1

---

<sup>60</sup> Rahmanuddin Tomalili, *Hukum Pidana*, (Yogyakarta: CV Budi Utama, 2019), 12.

tahun 1946. Beberapa pasal dihapuskan dan disesuaikan dengan kondisi dan misi kolonialisme Belanda atas wilayah Indonesia.<sup>61</sup> Perubahan ini juga turut menghapuskan aturan tentang kerja rodi serta penggantian denda dari mata uang golden ke rupiah. KUHP ini menjadi acuan hukum pidana positif hingga sekarang.

Pemberlakuan hukum pidana kolonial ini, secara politis dan sosiologis justru menimbulkan problem tersendiri bagi bangsa Indonesia, problematika tersebut di antaranya sebagai berikut :

- 1) Kemerdekaan Indonesia yang sejak 59 tahun yang lalu telah diproklamkan merupakan awal pendobran hukum kolonial menjadi hukum yang bersifat nasional. Namun pada realitasnya, hukum pidana positif (KUHP) Indonesia merupakan warisan kolonial Belanda. Secara politis hal ini menimbulkan masalah bagi bangsa yang merdeka.<sup>62</sup> Dengan kata lain, meskipun Indonesia merupakan negara yang merdeka, namun hukum pidana Indonesia belum bisa melepaskan diri dari penjajahan.
- 2) *Wetboek van Strafrecht* atau yang disebut Kitab Undang-Undang Hukum Pidana (KUHP) telah diberlakukan di Indonesia sejak tahun 1918. Hal ini berarti KUHP telah berumur lebih dari 87 tahun. Jika umur KUHP dihitung sejak dibuat pertama kali di Belanda tahun 1881 , maka KUHP telah berumur lebih dari 124 tahun. Oleh karena itu, KUHP dapat dianggap telah using dan sangat tua, walaupun Indonesia sendiri telah beberapa kali merubah materi KUHP ini. Namun demikian, perubahan ini tidak sampai kepada masalah

---

<sup>61</sup>Kanter dan Sianturi, *Asas-Asas Hukum Pidana di Indonesia dan Penerapannya* (Jakarta: Alumni AHM-PTHM,1982).

<sup>62</sup> Sudarto, *Kapita Selekta Hukum Pidana* (Bandung: Alumni,1981).

substansial dari KUHP tersebut. KUHP Belanda sendiri pada saat ini sudah banyak mengalami perkembangan.

- 3) Wujud asli hukum pidana Indonesia adalah *Wetboek van Strafrecht* yang menurut UU Nomor 1 tahun 1946 bisa disebut dengan KUHP. Ini menandakan bahwa wujud asli KUHP adalah berbahasa Belanda. KUHP yang tersebar di pasaran adalah KUHP yang di terjemahkan dari bahasa Belanda oleh pakar beberapa pakar hukum pidana, seperti terjemahan Mulyatno, Andi Hamzah, Sunarto surodiprto, R. Susilo, dan badan pembinaan hukum nasional. Tidak ada teks resmi terjemahan *wetboek van strafrecht* yang di keluarkan oleh negara Indonesia. Oleh karena itu, sangat mungkin dalam setiap terjemahan memiliki redaksi yang berbeda-beda.
- 4) KUHP kolonial Belanda memang memiliki jiwa yang berbeda dengan jiwa bangsa Indonesia. KUHP warisan zaman Hindia Belanda ini berasal dari sistem hukum kontinental (*Civil Law System*) atau menurut Rene David disebut dengan *The Roman-Germanic Family*. *The roman Germanic family* ini dipengaruhi oleh ajaran yang menonjolkan aliran individualisme dan liberalisme (*individualism, liberalism, and individual right*). Hal tersebut sangat berbeda dengan kultur bangsa Indonesia yang menjunjung tinggi nilai-nilai sosial. Apabila kemudian KUHP ini dipaksakan untuk tetap berlaku, benturan nilai dan kepentingan yang muncul tidak mustahil justru akan menimbulkan kejahatan-kejahatan baru.

5) Jika KUHP dilihat dari tiga sisi masalah dasar dalam hukum pidana, yaitu pidana, tindak pidana, dan pertanggungjawaban pidana, maka masalah-masalah dalam KUHP adalah:

a) Pidana

KUHP tidak menyebutkan tujuan dan pedoman pemidanaan bagi hakim atau penegak hukum yang lain, sehingga arah pemidanaan tidak tertuju pada tujuan dan pola yang sama. Pidana dalam KUHP juga bersifat kaku dalam arti tidak dimungkinkannya modifikasi pidana yang didasarkan pada perubahan atau perkembangan diri pelaku. Sistem pemidanaan dalam KUHP juga bersifat kaku sehingga tidak memberikan keleluasaan bagi hakim untuk memilih pidana yang tepat untuk pelaku tindak pidana. Pelaksanaan pidana seperti pidana mati, pidana denda, pidana penjara, dan pidana bagi anak.

b) Tindak Pidana

Asas legalitas dalam KUHP yaitu terdapat dalam pasal :

Pasal 1 ayat (1) KUHP : “tiada suatu perbuatan dapat dipidana, kecuali atas kekuatan aturan pidana dalam perundang-undangan yang telah ada, sebelum perbuatan dilakukan”

Asas legalitas dalam bahasa latin, dikenal sebagai *Nullum delictum nulla poena sine praevia lege poenalli* yang artinya tidak ada delik, tidak ada pidana tanpa peraturan terlebih dahulu. Atau menentukan bahwa tidak ada perbuatan yang dilarang dan diancam dengan pidana jika tidak ditentukan terlebih dahulu dalam Perundang-Undangan. Asas legalitas mengandung

tiga makna atau pengertian, yaitu **Pertama** tidak ada perbuatan yang dilarang dan diancam dengan pidana kalau hal itu terlebih dahulu belum dinyatakan dalam suatu aturan Undang-Undang. **Kedua** untuk menentukan adanya perbuatan pidana tidak boleh digunakan analogi (kias), **Ketiga** aturan hukum pidana tidak berlaku surut. Dengan demikian, KUHP tidak memberikan tempat bagi hukum yang hidup di tengah masyarakat yang tidak tertulis dalam perundang-undangan.

#### c) Pertanggungjawaban Pidana

Beberapa masalah yang timbul dalam aspek pertanggungjawaban pidana ini diantaranya mengenai asas kesalahan. Dalam pasal 36 ayat (1) KUHP dikenal asas yang bernama "*geenstraf zonder schuld*". Yang artinya tidak ada kesalahan maka tidak dapat dipidana. Artinya apabila seseorang melakukan suatu tindak pidana tetapi dirinya tidak memenuhi unsur-unsur dari kesalahan maka dirinya tidak dapat dipidana. Yang menjadi unsur-unsur dari kesalahan, salah satunya adalah memenuhi bentuk dari kesalahan yaitu kesengajaan dan kealpaan. Kesengajaan adalah apabila seorang pelaku mengetahui akibat dari perbuatan dan memang hal tersebut yang dikehendaki atau dimaksudkan oleh pelaku. Kealpaan adalah sifat kekurangan untuk jauh melihat ke depan akan akibat yang akan ditimbulkan serta kurangnya sifat kehati-hatian. Asas kesalahan merupakan penyeimbang dari asas legalitas yang dicantumkan dalam pasal 1 ayat (1), yang berarti bahwa seseorang bisa dipidana karena secara objektif memang telah melakukan tindak pidana (memenuhi rumusan asas legalitas) dan

secara subjektif terdapat unsur kesalahan dalam diri pelaku (memenuhi rumusan asas *culpabilitas*).<sup>63</sup> dasar adanya tindak pidana adalah adanya asas legalitas, sedangkan dasar dapat dipidananya pembuat adalah adalah asas kesalahan. Ini berarti bahwa pembuat tindak pidana hanya akan dipidana jika ia mempunyai kesalahan dalam melakukan tindak pidana tersebut. kapan seseorang dapat dikatakan mempunyai kesalahan merupakan hal yang menyangkut masalah pertanggungjawaban pidana. Seseorang mempunyai kesalahan bilamana pada waktu melakukan tindak pidana, dilihat dari segi kemasyarakatan ia dapat dicela oleh karena perbuatan tersebut.

Hal yang sama dikatakan oleh Sudarto,

“dipidananya seseorang tidaklah cukup apabila orang itu telah melakukan perbuatan yang bertentangan dengan hukum atau bersifat melawan hukum. Jadi meskipun perbuatan tersebut memenuhi rumusan delik dalam Undang-Undang dan tidak dibenarkan, namun hal tersebut belum memenuhi syarat untuk penjatuhan pidana. Untuk pembedaan masih perlu adanya syarat untuk penjatuhan pidana. Untuk pembedaan masih perlu adanya syarat, bahwa orang yang melakukan perbuatan itu mempunyai kesalahan atau bersalah. Dengan kata lain, orang tersebut harus dapat di pertanggungjawabkan atas perbuatannya atau jika dilihat dari sudut perbuatannya, perbuatannya dapat dipertanggungjawabkan kepada orang tersebut.”<sup>64</sup>

#### b. KUHP Baru

Usaha pembaharuan hukum pidana didasarkan pada alasan-alasan politik, sosiologis maupun praktis, alasan politik dilandasi oleh pandangan bahwa suatu negara merdeka harus mempunyai hukum sendiri yang bersifat nasional demi kebanggaan nasional. Alasan sosiologis dilandasi oleh adanya kehendak hukum

<sup>63</sup> Ahmad Bahje, “Sejarah dan Problematika Hukum Pidana Materil di Indonesia”, *SOSIO-RELIGIA* 5, No.2 (2006),15-19.

<sup>64</sup> Sudarto, *Hukum Pidana 1*, (Semarang : FH UNDIP,1988).

yang mencerminkan nilai kebudayaan dari suatu bangsa, sedangkan alasan praktis dilandasi pada kenyataan bahwa biasanya bekas-bekas negara jajahan mewarisi hukum yang pernah menjajahnya dengan bangsa aslinya, yang kemudian banyak dari generasi muda dari negara yang baru merdeka tersebut tidak paham. Peraturan yang mengatur tentang pidana yang tersirat dalam KUHP Indonesia merupakan warisan dari jaman penjajahan Belanda.

Usaha pembaharuan hukum di Indonesia yang sudah lama dimulai sejak proklamasi kemerdekaan pada tanggal 17 Agustus 1945 melalui Undang-Undang Dasar Negara Republik Indonesia tahun 1945, khususnya alinea keempat yang berbunyi:

Kemudian dari pada itu untuk membentuk suatu Pemerintah Negara Indonesia yang melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial, maka disusunlah kemerdekaan kebangsaan Indonesia itu dalam suatu Undang-Undang Dasar Negara Republik Indonesia yang terbentuk dalam suatu susunan Negara Republik Indonesia yang berkedaulatan rakyat dengan berdasar kepada ketuhanan yang Maha Esa, kemanusiaan yang adil dan beradab, persatuan Indonesia dan kerakyatan yang dipimpin oleh hikmat kebijaksanaan dalam permusyawaratan perwakilan, serta dengan mewujudkan suatu Keadilan Sosial bagi Seluruh Rakyat Indonesia.

Berdasarkan perumusan tujuan nasional yang teruang dalam alinea keempat UUD NKRI Tahun 1945 tersebut, maka dapat diketahui dua tujuan nasional yang utama, yakni (1) untuk melindungi segenap bangsa Indonesia, dan (2) untuk memajukan kesejahteraan umum berdasarkan Pancasila. Menurut Barda Nawawi Arief, terdapat dua kata kunci dari tujuan nasional, yaitu “perlindungan masyarakat” dan “kesejahteraan masyarakat”. dengan adanya dua kata kunci tersebut, terlihat adanya asas keseimbangan dalam tujuan pembangunan nasional.

Perlu diingat, bahwa kedua istilah juga sering digabungkan dalam satu istilah saja, yaitu “*social defense*”, karena didalam istilah “perlindungan masyarakat” sudah termuat juga “kesejahteraan masyarakat.”<sup>65</sup>

Pembaharuan hukum pidana pada dasarnya adalah membangun atau memperbaharui pokok-pokok pemikiran, konsep, ide awalnya, bukan sekedar memperbaharui atau mengganti perumusan pasalnya (undang-undang) secara tekstual. Pembaharuan hukum pidana harus ditempuh melalui pendekatan yang berorientasi pada kebijakan (*policy ori-ented approach*) dan sekaligus pendekatan yang berorientasi pada nilai.

Pembaharuan hukum pidana Indonesia diharapkan dapat bersifat komprehensif dan menyeluruh, tidak hanya ditinjau dari suatu pembaharuan KUHP. Seperti yang tercantum pada alinea sebelumnya pembaharuan hukum pidana meliputi berbagai aspek yang terkandung dalam nilai-nilai bangsa Indonesia. Sedangkan pembaharuan KUHP mengartikan suatu pembaharuan materi hukum pidana. Ruang lingkup pembaharuan sistem hukum pidana sendiri meliputi: Pembaharuan Substansi Hukum Pidana; Pembaharuan Struktur Hukum Pidana; dan Pembaharuan Budaya Hukum Pidana.<sup>66</sup>

Adapun beberapa tujuan yang melandasi pembaharuan suatu hukum pidana di Indonesia, meliputi untuk mengetahui tujuan bersifat politik dimana suatu Rancangan Undang-Undang Negara Indonesia bersifat secara nasional mencakup seluruh aspek masyarakat dengan keanekaragaman bangsa berdasarkan

---

<sup>65</sup> Marcus Priyo Gunarto, “Asas Keseimbangan dalam Konsep Rancangan Undang-Undang Kitab Undang-Undang Hukum Pidana,” MIMBAR HUKUM 24, No.1 (2012):85-86.

<sup>66</sup> Marcus Priyo Gunarto, “Asas Keseimbangan dalam Konsep Rancangan Undang-Undang Kitab Undang-Undang Hukum Pidana,” MIMBAR HUKUM 24, No.1 (2012), 86.

pancasila. Mengetahui suatu aspek pembaharuan hukum pidana dibidang sosiologi yang meninjau perubahan berdasarkan nilai kebudayaan yang terkandung di dalamnya, yang mana mengandung pandangan kolektif masyarakat tentang nilai yang berlaku. Tujuan yang lain yang mendasari pembaharuan ini bersifat praktis, sehingga dapat disesuaikan dengan perkembangan yang terjadi.

Barda Nawawi Arief menjelaskan bahwa pembaharuan hukum pidana tidak bisa dilepaskan dari ide kebijakan pembangunan sistem hukum nasional yang berlandaskan pancasila sebagai nilai kehidupan kebangsaan yang menjadi cita-cita bangsa. Ini berarti, pembaharuan Hukum Pidana nasional juga dilatarbelakangi dan bersumber atau berorientasi dari ide dasar (*basic ideas*) pancasila yang didalamnya mengandung “keseimbangan nilai/ide/paradigma” yakni:<sup>67</sup>

- 1) Ketuhanan (moral religious)
- 2) Kemanusiaan (humanistik)
- 3) Kebangsaan
- 4) Demokrasi
- 5) Keadilan sosial

Keseimbangan lima sila tersebut di atas, dapat dipadatkan menjadi “keseimbangan tiga pilar” yaitu: 1) pilar ketuhanan (religius), 2) pilar kemanusiaan (humanistik) dan 3) pilar kemasyarakatan (kebangsaan, nasionalistik, demokrasi, kerakyatan dan keadilan sosial).

---

<sup>67</sup>Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan dan Celah Hukumnya*, (Depok: PT. Raja Grafindo Persada, 2013), 110.

Kebijakan perumusan sistem pidana dalam KUHP/WvS lebih berorientasi pada pelaku. Nilai filosofi yang menjadi latarbelakang disusunnya KUHP/WvS adalah “individualism,liberalisme” yang diilhami oleh aliran klasik/neo-klasik menghendaki hukum pidana yang tersusun sistematis dan menitikberatkan pada kepastian hukum yang dalam hal ini berorientasi pada perbuatan dan pelaku tindak pidana. Asas keseimbangan dalam merumuskan suatu tindak pidana, tidak hanya dilakukan dengan adanya “tindak pidana” (TP) dan “kesalahan atau pertanggung jawaban pidana” (K/PJP), tetapi juga didasarkan pada tujuan pidanaan”. Maka persyaratan pidanaan dengan konsep tersebut dapat diskemakan seperti di bawah ini:

PIDANA = Tindak Pidana +  
Kesalahan + Tujuan pidana

Skema pidanaan diatas menunjukkan ide keseimbangan. Skema diatas berbeda dengan syarat pidanaan yang hanya bertolak atau terfokus pada tiga masalah pokok hukum pidana yaitu tindak pidana, kesalahan/pertanggungjawaban pidana dan pidana.

Menurut Barda Nawawi Arief, ide keseimbangan yakni mencakup: <sup>68</sup>

- Keseimbangan *monodualistik* antara kepentingan umum /masyarakat dengan kepentingan individu atau perorangan
- Keseimbangan antara perlindungan atau kepentingan pelaku tindak pidana (ide individualisasi pidana) dengan korban tindak pidana.

<sup>68</sup> Sudikno Mertokusomo, *Mengenal Hukum*, (Yogyakarta: Liberty Yogyakarta, 2003),45.

- Keseimbangan antara unsur/ faktor “objektif “ (perbuatan lahiriah) dengan unsur/ faktor “subjektif” orang/batiniah/sikap batin); ide *daad-dader strafrecht*
- keseimbangan antara kepastian hukum/kelenturan/elastisitas/fleksibilitas dengan keadilan
- keseimbangan antara kriteria formal dan material
- keseimbangan antara nilai-nilai nasional dengan nilai-nilai global/internasional/universal.

KUHP yang selama ini berlaku di Indonesia, belum memiliki asas keseimbangan. Pembaharuan hukum pidana juga mencakup pada beberapa dan mempertimbangkan masalah-masalah hukum pidana yang mana mampu menjaga keselarasan, keserasian, dan keseimbangan diantara pihak kepentingan negara, kepentingan umum, dan kepentingan individu; penggunaan hukum pidana diharapkan selaras terhadap tindakan pencegahan lain yang bersifat non penal; hukum pidana dirumuskan untuk dapat meredam faktor utama yang bersifat kriminogen; tindak pidana harus tepat dan teliti dalam menyimpulkn suatu perbuatan yang dilarang; serta diferensiasi prinsip pada kepentingan yang dirusak, status pelaku dalam kerangka asas kulpabilitas (suatu perbuatan pelaku yang disengaja).<sup>69</sup>

---

<sup>69</sup> Sudikno Mertokusomo, *Mengenal Hukum*, (Yogyakarta: Liberty Yogyakarta, 2003),45

## B. Konsep Cyber Crime

### 1) Pengertian Kejahatan Dunia Maya (*cyber crime*)

Masa awalnya, *cyber crime* didefinisikan sebagai kejahatan komputer (*computer crime*). The British Law Commission, mengartikan "*computer crime*" sebagai manipulasi komputer dengan cara apapun yang dilakukan dengan itikad buruk untuk memperoleh uang, barang atau keuntungan lainnya atau dimaksudkan untuk menimbulkan kerugian kepada pihak lain. Mandell membagi "*computer crime*" atas dua kegiatan, yaitu:

- a. Penggunaan komputer untuk melaksanakan perbuatan penipuan, pencurian atau penyembunyian yang dimaksud untuk memperoleh keuntungan keuangan, keuntungan bisnis, kekayaan atau pelayanan.
- b. Ancaman terhadap komputer itu sendiri, seperti pencurian perangkat keras atau lunak, sabotase dan pemerasan.<sup>70</sup>

Tindak pidana mayantara diidentik dengan tindak pidana di ruang siber (*cyber space*) atau yang bisa juga dikenal dengan *cyber crime*. Teknologi informasi dapat juga berdampak negatif, hal ini harus diantisipasi dan ditanggulangi dengan hukum yang terkait dengan kejahatan teknologi informasi dan komunikasi. Pengertian *cyber crime* yaitu sebagai kejahatan dibidang komputer yang secara umum dapat diartikan sebagai penggunaan komputer secara illegal. Kejahatan *cyber crime* dibagi menjadi dua kategori, yakni *cyber crime* dalam arti sempit dan dalam pengertian luas. *Cyber crime* dalam arti sempit kejahatan terhadap tindakan illegal yang ditunjukan untuk menyerang sistem

---

<sup>70</sup> Budi Sahariyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan dan Celah Hukumnya*, (Jakarta:Rajawali Pers 2012),

komputer, sedangkan *cyber crime* dalam arti luas mencakup kejahatan terhadap tindakan illegal yang dilakukan melalui jaringan komputer dan kejahatan yang menggunakan sarana komputer.<sup>71</sup>

Kejahatan dunia maya (*cyber crime*) merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet. Kejahatan dunia maya (*cyber crime*) di definisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer berbasis pada kecanggihan perkembangan teknologi internet.<sup>72</sup>

Sistem teknologi informasi berupa internet telah dapat menggeser paradigma para ahli hukum terhadap definisi kejahatan komputer, pada awalnya para ahli hukum terfokus pada alat/perangkat keras yaitu komputer. Namun dengan adanya perkembangan teknologi informasi berupa jaringan internet, maka fokus dari identifikasi terhadap definisi *cyber crime* telah diperluas lagi yaitu seluas aktivitas yang dapat dilakukan di dunia *cyber/* maya melalui sistem informasi yang digunakan. Jadi tidak sekedar pada komponen hardware-nya saja kejahatan ini dimaknai sebagai *cyber crime*, tetapi sudah dapat diperluas dalam lingkup dunia yang dijelajahi oleh sistem teknologi informasi yang bersangkutan. Sehingga lebih tepat jika pemaknaan dari *cyber crime* adalah kejahatan teknologi informasi, juga sebagai kejahatan mayantara. Pada dasarnya *cyber crime* meliputi semua tindak pidana yang berkenaan dengan sistem informasi itu sendiri, serta

---

<sup>71</sup> Barada Nawawi Arief, *Tindak Pidana Mayantara dan Perkembangan Kajian Cyber Crime di Indonesia*, (Jakarta: Rajawali Pers, 2006), 25.

<sup>72</sup> Nanda Risky Rilandi, "Tinjauan Yuridis Tindak Pidana *Cyber Crime* Berdasarkan Hukum Pidana." *Jurnal Hukum Dan Social Politik*, 1, No.2, (Mei 12, 2023), 36-47. <https://doi.org/10.59581/Jhsp-Widyakarya.V1i2.214>.

sistem informasi yang merupakan sarana untuk menyampaikan/pertukaran informasi kepada pihak lainnya.

Kejahatan di bidang teknologi informasi dapat digolongkan sebagai *white colour crime* karena pelaku *cyber crime* adalah orang yang menguasai penggunaan internet beserta aplikasinya atau ahli di bidangnya. Kejahatan tersebut sering kali dilakukan secara transnasional atau melintasi batas negara sehingga dua kriteria kejahatan melekat sekaligus dalam kejahatan *cyber* ini, yaitu *white colour crime* dan *transnational crime*. Berdasarkan beberapa literature serta praktiknya, *cyber crime* memiliki beberapa karakteristik, yaitu: **pertama** Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah siber/*cyber space*, sehingga tidak dapat dipastikan yuridiksi negara mana yang berlaku terhadapnya. **Kedua** Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet. **Ketiga** Perbuatan tersebut mengakibatkan kerugian materil maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional. **Keempat** Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya. **Kelima** Perbuatan tersebut sering dilakukan secara transnasional/melintas batas negara.<sup>73</sup>

Sebelum diberlakukan Undang-Undang ITE, aparat hukum menggunakan KUHP dalam menangani kasus-kasus kejahatan dunia *cyber*. Dalam ketentuan-ketentuan yang terdapat dalam KUHP tentang *cyber crime* masih bersifat global.

---

<sup>73</sup> Aswan, *Tindak Pidana Penipuan Berbasis Transaksi Elektronik*, (Jakarta: Guepedia, 2019),

Indonesia telah membentuk peraturan mengenai kejahatan dalam dunia *cyber* pada Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Rumusan tindak pidana dalam UU ITE, diatur dalam Bab VII: perbuatan yang dilarang, yang mencakup pasal 27 sampai pasal 37, sedangkan ancaman pidananya di tentukan dalam Bab XI: ketentuan pidana, yang mencakup pasal 45 sampai dengan pasal 52. Selain itu perbuatan yang merupakan bagian dari *cyber crime*, sebagaimana yang dikemukakan sebelumnya, amat beranekaragam dan cukup rumit berkenaan dengan pembuktian menurut hukum acara pidana, sehingga memerlukan keterampilan dari penyidik berkenaan dengan masalah-masalah komputer dan internet.<sup>74</sup>

## 2) Jenis-jenis *Cyber Crime*

- ***Unauthorized Access***: kejahatan yang dilakukan seseorang dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Probing dan port merupakan contoh kejahatan ini.
- ***Illegal Contents***: kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat

---

<sup>74</sup> Budi Sahariyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan dan Celah Hukumnya*, (Jakarta:Rajawali Pers 2012), 10.

dianggap melanggar hukum dan mengganggu ketertiban umum, contohnya adalah penyebaran pornografi, penyebaran suatu berita bohong atau fitnah yang akan menghancurkan martabat dan harga diri pihak lain atau pemuatan suatu informasi yang merupakan rahasia negara, dan propaganda untuk melawan pemerintahan yang sah, dan sebagainya.<sup>75</sup>

- **Penyebaran Virus Secara Sengaja:** Penyebaran virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.
- **Data Forgery:** Kejahatan jenis ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database.
- **Cyber Espionage:** Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen atau data-data pentingnya tersimpan dalam suatu sistem.<sup>76</sup>
- **Sabotage, and Extortion:** merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic*

---

<sup>75</sup> Budi Sahariyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan dan Celah Hukumnya*, (Jakarta: Rajawali Pers, 2012), 60

<sup>76</sup> Budi Sahariyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan dan Celah Hukumnya*, (Jakarta: Rajawali Pers, 2012), 59

*bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya atau sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai *cyber terrorism*.

- **Cyberstalking:** Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan email dan dilakukan berulang kali. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal ini bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya.
- **Carding:** merupakan kejahatan yang menggunakan teknologi komputer untuk melakukan transaksi di internet, dengan menggunakan card credit orang lain sehingga kejahatan ini dapat menimbulkan kerugian bagi orang lain baik materil maupun non materil.
- **Cracking:** kejahatan dengan menggunakan teknologi komputer yang dilakukan untuk merusak system keamanan suatu system komputer dan biasanya melakukan pencurian, tindakan anarkis begitu mereka mendapatkan *cracker* dimana *hacker* sendiri identik dengan perbuatan negatif.

- **Hacking dan cracker:** Istilah hacker biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut *cracker*. Boleh dibilang cracker ini sebenarnya adalah *hacker* yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas *cracking* di internet memiliki lingkup yang sangat luas, mulai dari pembajakan *account* milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (*Denial of Service*). *Dos attack* merupakan serangan yang bertujuan melumpuhkan target (*hang, crash*) sehingga tidak dapat memberikan layanan.<sup>77</sup>
- **Cybersquatting and Typosquatting:** kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun *typosquatting* adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan.
- **Hijacking:** kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah *Software Piracy* (pembajakan perangkat lunak).
- **Cyber Teroris:** Suatu tindakan *cyber crime* termasuk *cyber terrorism* jika mengancam pemerintah atau warganegara, termasuk *cracking* ke situs pemerintah atau militer.

---

<sup>77</sup> Barda Nawawi Arief, *Tindak Pidana Mayantara*, (Jakarta: Rajawali Pers, 2006)

Jenis-jenis *cyber crime* berdasarkan motif yaitu **pertama**, *cyber crime* sebagai tindakan kejahatan murni : dimana orang yang melakukan kejahatan yang dilakukan secara sengaja, dimana orang tersebut secara sengaja dan terencana untuk melakukan pengerusakan, pencurian, tindakan anarkis, terhadap suatu sistem informasi dan komputer. **Kedua**, *cyber crime* sebagai tindakan kejahatan abu-abu: dimana kejahatan ini tidak jelas antara kejahatan kriminal atau bukan karena dia melakukan pembobolan tapi tidak merusak, mencuri atau melakukan perbuatan anarkis terhadap sistem informasi atau komputer tersebut. contoh kejahatan *cyber crime* dari beberapa motif yang disebutkan diatas yaitu antara lain:<sup>78</sup> a) *cyber crime* yang menyerang individu : kejahatan yang dilakukan terhadap orang lain dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik, mencoba ataupun mempermainkan seseorang untuk mendapatkan kepuasan pribadi. Contohnya pornografi, dan lain-lain. b) *cyber crime* yang menyerang hak cipta (hak milik): kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah dengan tujuan untuk kepentingan pribadi/umum ataupun demi materi/non materi. c) *cyber crime* yang menyerang pemerintah: kejahatan yang dilakukan dengan pemerintah sebagai objek dengan motif melakukan teror, membajak ataupun mengancam keamanan suatu pemerintahan yang bertujuan untuk mengacaukan sistem pemerintahan.

---

<sup>78</sup> Yurizal, *Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia*, (Malang: Media Nusa Creative, 2015), 29.

### 3) *Cyber Crime* yang Sering Terjadi di Indonesia

Kejahatan *cyber crime* yang marak di Indonesia meliputi penipuan kartu kredit, penipuan perbankan, pencemaran nama baik, *defacing*, *cracking*, pornografi, judi online, penyebaran berita bohong melalui internet dan terorisme. Ada beberapa contoh kasus *cyber crime* yang terjadi di Indonesia, diantaranya adalah:<sup>79</sup>

#### a) Tindak pidana penipuan digital *phishing*.

Tindak pidana penipuan digital *phishing* merupakan semua jenis tindakan penipuan dilakukan melalui pengambilan informasi dan data penting dimana pelaku mengarahkan korban untuk masuk dalam sebuah situs atau laman palsu agar terjebak dan akhirnya terpedaya. Tindak pidana penipuan ini biasanya yang ditujukan kepada seseorang atau badan hukum caranya agar memberikan informasi atau data pribadi seperti nomor rekening bank atau nomor kartu kredit. Penipu biasanya menghubungi secara tiba-tiba kepada calon korbannya melalui email, pesan teks, panggilan telepon, dan media sosial lainnya. Dengan mengaku sebagai pengusaha sah dan resmi seperti bank, perusahaan telekomunikasi, penyedia internet. Pelaku penipuan memberitahukan untuk segera memperbarui pada akun tertentu untuk menyegarkan sistem yang ada atau meminta melakukan pengisian survey tertentu dengan alasan mendapatkan kesempatan memenangkan suatu hadiah diakhir. Berasal dari keterangan tersebut penipu memperoleh data lengkap dan penipu dengan mudah melakukan kejahatan penipuan dengan menggunakan dan memanfaatkan kemajuan teknologi digital.

---

<sup>79</sup> Yurizal, *Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia*, (Malang: Media Nusa Creative, 2015), 30.

Penipu memberikan informasi dan mengatakan bahwa telah terjadi aktivitas tidak sah atau mencurigakan pada akun calon korbannya, dan hanya pihaknya yang dapat membantu memperbaikinya, dengan syarat dapat bekerjasama dengan memberikan keterangan data yang benar agar dapat mempermudah dalam proses perbaikan atau pembaharuannya. Untuk menghindari penipuan ini, pengguna layanan harus selalu memeriksa validasi email, pesan teks, media sosial lainnya, secara detail dan memastikan kontak dari pemilik layanan resmi dan menghubungi langsung pemilik layanan pada laman resminya.<sup>80</sup>

Al Qur'an ada banyak ayat yang sering membahas tentang penipuan, salah satunya surat Al-Baqarah Ayat 9 yang berbunyi:

تُخَدِعُونَ اللَّهَ وَالَّذِينَ آمَنُوا وَمَا تُخَدِعُونَ إِلَّا أَنْفُسَهُمْ وَمَا يَشْعُرُونَ

Terjemahnya: mereka hendak menipu Allah dan orang-orang yang beriman, Padahal mereka hanya menipu dirinya sendiri sedang mereka tidak sadar.

ayat tersebut diatas menjelaskan bahwa penipuan mereka terhadap orang-orang mukmin di dunia ini, pada hakikatnya merupakan tipuan terhadap diri mereka sendiri. Karena merasa telah tercapai keinginan mereka dan menyangka bahwa tindakan itu dapat mendatangkan kebahagiaan bagi mereka. Padahal sebenarnya hal itu justru merupakan sumber kebinasaan, serta menyeret kepada

<sup>80</sup> Yurizal, *Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia*, (Malang: Media Nusa Creative, 2015),

kemurkaan dan siksa Allah Swt yang sangat pedih, yang sama sekali tidak mereka harapkan.

b) Pencurian Nomor Kredit

Menurut Rommy Alkatiry, penyalahgunaan kartu kredit milik orang lain di internet merupakan kasus *cyber crime* terbesar yang berkaitan dengan dunia bisnis internet di Indonesia. Nama dan kartu kredit orang lain yang diperoleh di berbagai tempat (restaurant, hotel, atau segala tempat yang melakukan transaksi pembayaran dengan kartu kredit) dimasukkan diaplikasi pembelian barang di internet.

c) Peretasan dan *spamming* media sosial.

*Spamming* media sosial terjadi ketika seorang membuat akun palsu atau menjadi teman atau diikuti banyak orang. Akun palsu ini memberikan keleluasaan mengirim spam dengan banyak pesan sehingga dapat menyebarkan *malware* yaitu kontraksi perangkat lunak berbahaya ke sistem data dan perangkat. *Malware* adalah nama menyeluruh untuk berbagai jenis virus yang akan masuk ke komputer, ponsel, dan tablet sehingga dapat mencuri semua data dan informasi pribadi. Peretasan juga dapat menyerang dan menyebarkan konten bohong dan hoax.

Q.S An-Nur 24: 11

إِنَّ الَّذِينَ جَاءُوا بِالْإِفْكِ عُصْبَةٌ مِّنكُمْ لَا تَحْسَبُوهُ شَرًّا لَّكُم بَلْ هُوَ خَيْرٌ لَّكُمْ لِكُلِّ  
 أَمْرٍ مِّنْهُمْ مَا أَكْتَسَبَ مِنَ الْإِثْمِ وَالَّذِي تَوَلَّى كِبْرَهُ مِنْهُمْ لَهُ عَذَابٌ عَظِيمٌ ﴿١١﴾

Terjemahnya : Sesungguhnya orang-orang yang membawa berita bohong itu adalah dari golongan kamu juga. janganlah kamu kira bahwa berita bohong itu buruk bagi kamu bahkan ia adalah baik bagi

kamu. tiap-tiap seseorang dari mereka mendapat Balasan dari dosa yang dikerjakannya. dan siapa di antara mereka yang mengambil bahagian yang terbesar dalam penyiaran berita bohong itu baginya azab yang besar.<sup>81</sup>

Q.S. An-Nahl ayat 105

إِنَّمَا يَفْتَرِي الْكَذِبَ الَّذِينَ لَا يُؤْمِنُونَ بِآيَاتِ اللَّهِ وَأُولَٰئِكَ هُمُ

الْكٰذِبُونَ ﴿١٠٥﴾

Terjemahnya: Sesungguhnya yang mengada-adakan kebohongan, hanyalah orang-orang yang tidak beriman kepada ayat-ayat Allah, dan mereka Itulah orang-orang pendusta.

Kedua Ayat tersebut menjelaskan bahwa orang yang membawa berita bohong atau berita buruk itu sesama manusia dan akan mendapat balasan atas perbuatan mereka. Apabila terus menerus menyebarkan berita bohong orang tersebut akan menerima azab yang besar. Ayat diatas menjadi salah satu dasar yang ditetapkan oleh agama untuk diterapkan dalam kehidupan sosial. Bisa juga menjadi cara untuk berfikir logis ketika menerima suatu berita. Karena kemampuan manusia yang tidak dapat menjangkau informasi secara menyeluruh maka membutuhkan orang lain untuk mengkonfirmasi berita tersebut. tetapi harus berhati-hati juga dengan sumber berita atau pihak yang dijadikan referensi berita, Ayat di atas mengajarkan kita untuk berfikir logis dan berdasarkan ilmu pengetahuan untuk melawan kebohohan.

d) Pencemaran Nama Baik

Undang-Undang Informasi dan Transaksi Elektronik (ITE) No.11 Tahun 2008 tidak disebutkan tentang pencemaran nama baik, tetapi dengan merujuk pasal 433

<sup>81</sup> Lajnah Pentashihain Mushaf Al-Qur'an Departemen Agama Republik Indonesia, *Al-Qur'an dan Terjemahnya Syaamil Quran*,

ayat (1) KUHP pencemaran nama baik dapat di artikan sebagai perbuatan menyerang kehormatan atau nama baik seseorang dengan menuduhkan suatu hal yang dimaksudnya terang supaya hal itu diketahui umum, tentu dalam hal ini menggunakan media elektronik.<sup>82</sup>

Konteks islam *cyber crime* adalah tindakan yang dilarang oleh Allah Swt, di dalam al-Qur'an banyak kata yang mempunyai konotasi yang sama dengan istilah penginaan atau menyerang harga diri seseorang, seperti kata fitnah, hasad, ghibah dan namimah yang semua kata lain mempunyai arti kata menghina, mencaci, menjelekan orang lain dengan tanpa bukti. Adapun ayat Al-Qur'an yang membahas tentang larangan penghinaan/pencemaran nama baik yaitu:

QS. Al-Hujarat (49) :11

يٰۤاَيُّهَا الَّذِيْنَ ءَامَنُوْا لَا يَسْخَرُوْا قَوْمًا مِّنْ قَوْمٍ عَسَىٰ اَنْ يَّكُوْنُوْا خَيْرًا مِّنْهُمْ وَلَا نِسَاءً مِّنْ نِّسَاءٍ عَسَىٰ اَنْ يَّكُنَّ خَيْرًا مِّنْهُنَّ وَلَا تَلْمِزُوْا اَنْفُسَكُمْ وَلَا تَنَابَزُوْا بِاللُّغَبِ  
بِئْسَ الْاَسْمُ الْفُسُوْقُ بَعْدَ الْاِيْمٰنِ ۗ وَمَنْ لَّمْ يَتُبْ فَاُولٰٓئِكَ هُمُ الظَّٰلِمُوْنَ ﴿١١﴾

Terjemahnya: Hai orang-orang yang beriman, janganlah sekumpulan orang laki-laki merendahkan kumpulan yang lain, boleh jadi yang ditertawakan itu lebih baik dari mereka. dan jangan pula sekumpulan perempuan merendahkan kumpulan lainnya, boleh jadi yang direndahkan itu lebih baik. dan janganlah suka mencela dirimu sendiri dan jangan memanggil dengan gelaran yang mengandung ejekan. seburuk-buruk panggilan adalah (panggilan) yang buruk sesudah iman dan Barangsiapa yang tidak bertobat, Maka mereka Itulah orang-orang yang zalim.<sup>83</sup>

<sup>82</sup> Budi Sahariyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan dan Celah Hukumnya*, (Jakarta: Rajawali Pers, 2012), 35

<sup>83</sup> Lajnah Pentashihain Mushaf Al-Qur'an Departemen Agama Republik Indonesia, *Al-Qur'an dan Terjemahnya*, 516.

QS. At Taubah 9:79

الَّذِينَ يَلْمُزُونَ الْمُطَّوِّعِينَ مِنَ الْمُؤْمِنِينَ فِي الصَّدَقَاتِ وَالَّذِينَ لَا  
 سِجْدُونَ إِلَّا جُهْدَهُمْ فَيَسْخَرُونَ مِنْهُمْ سَخِرَ اللَّهُ مِنْهُمْ وَلَهُمْ عَذَابٌ أَلِيمٌ ﴿٧٩﴾

Terjemahnya: (orang-orang munafik itu) Yaitu orang-orang yang mencela orang-orang mukmin yang memberi sedekah dengan sukarela dan (mencela) orang-orang yang tidak memperoleh (untuk disedekahkan) selain sekedar kesanggupannya, Maka orang-orang munafik itu menghina mereka. Allah akan membalas penghinaan mereka itu, dan untuk mereka azab yang pedih.<sup>84</sup>

Ayat tersebut diatas menjelaskan bahwa kedua Firman Allah tersebut terdapat kalimat larangan untuk tidak berbuat penghinaan, “janganlah laki-laki diantara kain merendahkan laki-laki yang lain dan jangan pula wanita mukmin yang lain”. Sebab boleh jadi mereka yang direndahkan itu lebih baik di sisi Allah daripada mereka yang merendahkan. Janganlah kalian saling mencela yang lain, dan jangan pula memanggil seseorang memanggil saudaranya dengan panggilan yang tidak disukainya. Jadi yang dimaksud dengan menghinaan ialah memandang rendah atau menjatuhkan martabat seseorang

#### e) Ujaran Kebencian

Tindakan komunikasi yang dilakukan oleh suatu individu atau kelompok dalam bentuk provokasi, hasutan, ataupun hinaan kepada individu maupun kelompok yang lain dalam berbagai aspek seperti RAS, warna kulit, etnis, gender,dll.

<sup>84</sup> Lajnah Pentashihain Mushaf Al-Qur'an Departemen Agama Republik Indonesia, *Al-Qur'an dan Terjemahnya Syaamil Quran*, 199.

f) *Defacing* (membajak situs web)

Metode kejahatan *deface* adalah mengubah tampilan sesuai keinginan pelaku kejahatan. Kejahatan jenis ini bisa menampilkan tulisan-tulisan provocative atau gambar lucu. merupakan salah satu jenis kejahatan dunia maya yang paling favorit karena hasil kejahatannya dapat langsung dilihat oleh masyarakat.<sup>85</sup>

g) Virus dan Trojan

Virus komputer merupakan program komputer yang dapat menggandakan atau menyalin sendiri sendiri dan menyebar dengan cara menyisipkan salinannya ke dalam program atau dokumen lain. Trojan adalah sebuah bentuk perangkat lunak yang mencurigakan (*malicious software*) yang dapat merusak sebuah sistem atau jaringan. Tujuan dari Trojan adalah memperoleh informasi dari target (password, kebiasaan user yang tercatat dalam sistem log, data dan lain-lain), dan mengendalikan target (memperoleh hak akses pada target).

Adapun beberapa kasus *cyber crime* yang menyerang server, sempat menyita perhatian publik di Indonesia.<sup>86</sup>

1. Pencurian Data Bank Syariah Indonesia (2023)

Hal ini terjadi pada Mei 2023, salah satu server bank syariah terbesar di Indonesia dikabarkan lumpuh selama 5 hari. Yang mana hal tersebut menyebabkan para nasabah tidak dapat mengakses aplikasi *mobile banking* mereka. Grup *hacker* asal Rusia, Lockbit, mengaku bertanggung jawab atas

<sup>85</sup> Budi Sahariyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan dan Celah Hukumnya*, (Jakarta: Rajawali Pers, 2012),

<sup>86</sup> AMT IT Solutions “6 Kasus *Cyber Crime* di Indonesia Menyerang Server,” <https://amt-it.com/blog/kasus-cyber-crime-di-indonesia/>, Diakses Pada Tanggal 17 Juni 2023, Pukul: 20:30

lumpuhnya server Bank tersebut. mereka juga mengklaim telah mencuri data sebanyak 1,5 *terabyte*, termasuk didalamnya data pribadi nasabah dan pegawai. Mereka pun mengancam pihak bank untuk membayar sejumlah uang agar data tersebut dapat dipulihkan, jika tidak maka data-data tersebut akan dijual ke dark web. Kasus *cyber crime* ini pun masuk ke dalam jenis serangan *Ransomware* terbesar di Indonesia.

## 2. Pembobolan Data Oleh Hacker Bjorka (2022)

Sepanjang tahun 2022 terjadi banyak kasus *cyber crime* yang mengincar data pribadi beberapa perusahaan di Indonesia. Seperti *hacker* Bjorka di tahun 2022. Data atau informasi yang berhasil dicuri diantaranya seperti data registrasi kartu SIM milik Kominfo, data nasabah Bank Indonesia, data pasien beberapa rumah sakit di Indonesia, data pelamar Pertamina, data pelanggan PLN, data pelanggan jasa marga, dan lain-lain. Korban dari pencurian data yang dilakukan oleh Bjorka umumnya datang dari beberapa perusahaan yang ada di Indonesia dengan keamanan server yang lemah.

## 3. Situs web DPR RI Down dan berganti nama

Dunia *cyber crime* juga akrab dengan istilah *hacktivism*, yaitu meretas situs web pemerintah atau organisasi, website DPR RI pernah jadi korban peretasan yang mana hal itu ditandai dengan tidak bisa mengakses halaman [dpr.go.id](http://dpr.go.id). Setelah diselidiki, hal ini ditemukan sebagai hasil dari serangan DDoS. Sehingga situs DPR RI pun mendapat tsunami request yang membuat server semakin berat memuat hingga akhirnya crash. Motif kejahatan ini sengaja dibuat oleh para peretas dengan tujuan untuk merusak situs. Setelah pengunjung dapat mengakses

situs, muncul kata-kata dewan penghianat rakyat. Rupanya serangan ini adalah bentuk protes *hacktivist* terhadap Undang-Undang. Tim IT DPR RI langsung menutup lokasi dan melakukan perawatan, namun meskipun situs tersebut akhirnya dapat dipulihkan, web menjadi lebih lambat karena dampak serangan virus.<sup>87</sup>

#### 4. Perusakan Data Kejaksaan Agung RI (2021)

Lemahnya server website Kejaksaan Agung RI pada saat itu, membuat situs web berhasil diretas oleh seorang *hacker* asal Indonesia dengan nama Gh05t666nero alias MFW. *Hacker* tersebut berhasil mengubah tampilan website Kejaksaan Agung RI dengan tampilan protes serta segel “HACKED” berwarna merah. Selain itu, pelaku juga mencuri 3.086.224 data pribadi yang ada di website tersebut.

#### 5. Penyerangan terhadap website sekretariat kabinet RI

Pada saat yang sama, situs web Sekretariat Kabinet Indonesia yaitu setkab.go.id, di serang oleh serangan sabotase untuk mengubah tampilan dan nuansa situs target mereka. Rupanya, peretasan ini dilakukan untuk tujuan ekonomi, yaitu menjual skrip backdoor dari situs web korban kepada mereka yang menginginkannya. Awalnya, situs setkab.go.id diretas dan tidak bisa diakses. Tampilan website kemudian berubah menjadi hitam dengan gambar pengunjuk rasa yang membawa bendera merah putih dan bertuliskan “padang Blackhat II

---

<sup>87</sup> AMT IT Solutions “6 Kasus *Cyber Crime* di Indonesia Menyerang Server,” <https://amt-it.com/blog/kasus-cyber-crime-di-indonesia/>, Diakses Pada Tanggal 17 Juni 2023, Pukul: 20:30

anon illusion team pwned by zyy ft luthfifake”. Menurut penyelidikan polisi, peretasan ini terjadi karena kelemahan sistem keamanan dan kelalaian operator.<sup>88</sup>

#### 6. Peretasan terhadap website BPJS Kesehatan (2021)

Peristiwa peretasan ini terjadi pada bulan Mei 2021, dimana situs badan penyelenggara jaminan sosial (BPJS) kesehatan, khususnya bpjs-kesehatan.go.id, diteras. Hal ini mengakibatkan data 279 juta orang Indonesia dibocorkan dan dijual di forum online raid forums oleh akun bernama “Kotz”. Dataset yang berisi NIK, nomor ponsel, email, alamat, dan gaji itu dijual seharga 0,15 bitcoin atau Rp 84,4 juta. Untuk mencegah penyebaran data data lebih luas, kominfo kemudian meminta untuk memutuskan akses tautan unduhan data pribadi dan memblokir Raid Forums.

#### 7. Kebocoran data asuransi jiwa BRI Life (2021)

Kasus peretasan di Indonesia juga terjadi pada perusahaan asuransi BRI Life. Pada Juli 2021, sekitar 2 juta data nasabah BRI Life diduga bocor dan dijual secara online seharga \$7.000 atau sekitar Rp 101,6 juta. Hal ini pertama kali diungkap oleh akun twitter @UnderTheBreach yang diklaim peretasan telah mengambil 250GB data BRI Life, termasuk 2 juta data nasabah dalam format file PDF dan 463.000 dokumen lainnya. Data tersebut berisi informasi tentang foto KTP, rekening, nomor pajak, akta kelahiran, rekam medis. Rupanya kebocoran

---

<sup>88</sup> AMT IT Solutions “6 Kasus *Cyber Crime* di Indonesia Menyerang Server,” <https://amt-it.com/blog/kasus-cyber-crime-di-indonesia/>, Diakses Pada Tanggal 17 Juni 2023, Pukul: 20:30

data tersebut terjadi karena adanya celah keamanan pada sistem elektronik BRI Life yang di salahgunakan oleh pihak yang tidak bertanggung jawab.<sup>89</sup>

#### 8. Kebocoran data e-HAC Kemenkes (2021)

Kebocoran data terjadi pada juli 2021, dimana aplikasi Electronic Health Aleart (e-HAC) kementerian kesehatan RI juga telah menjadi korban serangan siber yang disebabkan oleh peretas. Aplikasi health aleart card, data 1,3 juta orang Indonesia bocor. Selain bocornya data pengguna e-HAC, kasus ini juga mengakibatkan terungkapnya data tes Covid-19 penumpang, data rumah sakit, dan data pegawai e-HAC. Serangan ini terjadi karena kurangnya protocol keamanan aplikasi yang memadai dan penggunaan database Elasticsearch yang dianggap kurang aman untuk menyimpan data.

Era kemajuan teknologi informasi ditandai dengan meningkatnya penggunaan internet dalam setiap aspek kehidupan manusia. Meningkatnya penggunaan internet dari satu sisi memberikan banyak kemudahan bagi manusia dalam melakukan aktivitasnya, namun disisi lain memudahkan bagi para pihak tertentu untuk melakukan tindak pidana.

#### **C. Ketentuan Tentang Pengaturan Tindak Pidana *Cyber Crime* di Indonesia**

Instrument hukum memberikan landasan atau pedoman bagi para penegak hukum yang akan diterapkan kepada para pelaku *cyber crime*. Sebagai hukum positif, pembuatannya melalui mekanisme pembuatan Perundang-Undangan, dan sekaligus melekat sifat *Ius Constitutum*, yakni menjadi hukum positif yang

---

<sup>89</sup>Achmad Farid, "14 Kasus Cyber Crime Yang Mengemparkan Warganet" 11 Oktober 2022, <https://www.Exabytes.Co.Id/Blog/Kasus-Cyber-Crime-di-Indonesia/>, Diakses Pada Tanggal 17 Juni 2023, Pukul: 23;15.

memberikan sanksi bagi peristiwa atau perbuatan kriminal yang menggunakan komputer.<sup>90</sup>

Sistem teknologi informasi berupa internet telah dapat menggeser paradigma para ahli hukum terhadap definisi kejahatan komputer, pada awalnya para ahli hukum terfokus pada alat/perangkat keras yaitu komputer. Namun dengan adanya perkembangan teknologi informasi berupa internet, maka fokus dari identifikasi terhadap definisi *cyber crime* lebih diperluas lagi yaitu seluas aktivitas yang dapat dilakukan didunia *cyber*/maya melalui sistem informasi yang digunakan. Jadi tidak sekedar pada komponen hardware-nya saja kejahatan itu dimaknai sebagai *cyber crime* tetapi sudah dapat diperluas dalam lingkup dunia yang dijelajah oleh sistem teknologi informasi yang bersangkutan . sehingga lebih tepat jika pemaknaan dari *cyber crime* adalah kejahatan teknologi informasi, juga sebagai kejahatan mayantara. Pada dasarnya *cyber crime* meliputi semua tindak pidana yang berkenaan dengan sistem informasi itu sendiri, serta sistem informasi yang merupakan sarana untuk menyampaikan atau pertukaran informasi kepada pihak lainnya.<sup>91</sup> Adapun beberapa aturan yang mengatur tindak pidana *cyber crime* yaitu:

#### 1. UUD 1945

##### **Pasal 28 F**

Setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia.

---

<sup>90</sup> Hermawan Sulistiyo, *Cyber Crime: Modus Operandi dan Penanggulangannya* (Cet. 1; Yogyakarta: LaksBang Pressindo,2007), 62

<sup>91</sup>Aswan, *Tindak Pidana Penipuan Berbasis Transaksi Elektronik*, (Makassar: Guepedia,2019),44.

Hak berkomunikasi dan memperoleh informasi menurut pasal 28 F UUD 1945 adalah hak asasi manusia yang dijamin oleh negara untuk setiap orang. Hak ini memungkinkan seseorang untuk berkomunikasi dengan orang lain dan memperoleh informasi yang dibutuhkan. Pasal ini juga menegaskan bahwa hak untuk memperoleh informasi merupakan salah satu wujud dari kehidupan berbangsa dan negara juga diwajibkan untuk mengembangkan pribadi dan lingkungan sosial seseorang melalui hak ini. Dalam konteks ini, undang-undang keterbukaan informasi public menjadi penting sebagai landasan hukum yang berkaitan dengan hak setiap orang untuk memperoleh informasi.

## 2. Kitab Undang-Undang Hukum Pidana

Sebelum berlakunya UU ITE, yang mengatur kasus *cyber crime*, penegak hukum menggunakan ketentuan KUHP dan ketentuan dalam beberapa undang-undang yang mengatur tindak pidana *cyber crime*. Saat ini, telah terdapat reformasi atau pembaharuan terhadap KUHP lama. Reformasi ini terwujud melalui hadirnya UU No. 1 tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (“KUHP Baru”). Meski secara paradigmatik, KUHP baru memberikan pembaharuan politik hukum serta filosofi pidanaan yang modernis, namun pengaturan terhadap beberapa ketentuan masih memiliki persamaan.<sup>92</sup> Misalnya KUHP lama dan KUHP baru sama-sama mengakui dan mengatur tindak pidana yang tergolong dalam kejahatan *cyber crime*, sebagai sebuah tindak pidana sehingga dilarang dan diancam pidana.

---

<sup>92</sup>Emmilia Rusdiana. “Alternatif Pidana Bagi Pelaku Tindak Pidana Peretasan di Indonesia dalam Undang-Undang Informasi dan Transaksi Elektronik.” *Jurnal Hukum*, 1, No.1 (Januari, 9, 2023).

Meskipun secara konseptual tidak terdapat perbedaan antara tindak pidana yang tergolong kasus *cyber crime* dalam KUHP lama dengan KUHP baru, namun terdapat perbedaan. Perbedaan tersebut terletak pada sanksi yang diancamkan. Misalnya seperti KUHP lama memberikan ancaman untuk tindak pidana mengakses komputer atau sistem elektronik orang lain dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik. KUHP lama memberikan ancaman pidana tunggal berupa pidana penjara paling lama 6 tahun. Sementara itu dalam KUHP baru memberikan ancaman sanksi alternatif, yakni disamping pidana penjara paling lama 6 tahun, namun dapat pula dijatuhi pidana alternatif berupa pidana denda paling banyak kategori V. Sesuai dengan pasal 79 KUHP baru yang dimaksud dengan pidana denda paling banyak kategori V adalah pidana denda sebesar Rp. 500.000.000,00 (lima ratus juta rupiah). Artinya jika pidana alternatif pasal 492 KUHP baru diterjemahkan maka tindak pidana penipuan dapat dijatuhi pidana dengan pidana denda paling banyak 500 juta rupiah.<sup>93</sup>

Pasal-pasal di dalam KUHP biasanya digunakan lebih dari satu pasal karena melibatkan beberapa perbuatan sekaligus pasal-pasal yang dapat dikenakan dalam KUHP terbaru pada *cyber crime* yaitu:<sup>94</sup>

### **Pasal 332 KUHP**

- (1) Setiap orang dengan sengaja atau tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun, dipidana dengan pidana penjara paling lama 6 (enam) tahun atau pidana denda paling banyak kategori V.
- (2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun

<sup>93</sup> Emmilia Rusdiana. "Alternatif Pidana Bagi Pelaku Tindak Pidana Peretasan di Indonesia dalam Undang-Undang Informasi dan Transaksi Elektronik." *Jurnal Hukum*, 1, No.1 (Januari, 9, 2023).

<sup>94</sup> H. Sofwan Jannah, "Penegakan Hukum Cyber Crime Ditinjau dari Hukum Positif dan Hukum Islam" *Jurnal Al-Mawarid*, 12, No. 1 (Agustus 2012)

dengan tujuan untuk memperoleh informasi elektronik dan dokumen elektronik, dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak kategori V.

- (3) Setiap orang dengan sengaja atau tanpa hak atau melawan hukum mengakses komputer atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan, dipidana dengan pidana penjara paling lama 8 (delapan) tahun atau pidana denda paling banyak kategori VI.

Pasal 332 KUHP ini dapat dikenakan untuk penipuan dengan seolah-olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu *website* sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan. Tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesan tidak kunjung datang sehingga pembeli tersebut tertipu.<sup>95</sup>

#### **Pasal 333 KUHP**

Dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak kategori VI, setiap orang yang;

- a. Tanpa hak menggunakan atau mengakses komputer atau sistem elektronik dengan cara apa pun, dengan maksud memperoleh, mengubah, merusak, atau menghilangkan informasi pertahanan nasional hubungan internasional yang dapat menyebabkan gangguan atau bahaya terhadap negara atau hubungan dengan subjek hukum internasional;
- b. Tanpa hak melakukan tindakan yang menyebabkan transmisi dari program, informasi, kode atau perintah komputer atau sistem elektronik yang dilindungi negara menjadi rusak;
- c. Tanpa hak atau melampaui wewenangnya menggunakan atau mengakses komputer atau sistem elektronik, baik dari dalam maupun luar negeri untuk memperoleh informasi dari komputer atau sistem elektronik yang dilindungi oleh negara;
- d. Tanpa hak menggunakan atau mengakses komputer atau sistem elektronik milik pemerintah;
- e. Tanpa hak atau melampaui wewenangnya menggunakan atau mengakses komputer atau sistem elektronik yang dilindungi oleh negara, yang mengakibatkan komputer atau sistem elektronik tersebut menjadi rusak;

---

<sup>95</sup> H. Sofwan Jannah, "Penegakan Hukum Cyber Crime Ditinjau dari Hukum Positif dan Hukum Islam" *Jurnal Al-Mawarid*, 12, No. 1 (Agustus 2012)

- f. Tanpa hak atau melampaui wewenangnya menggunakan atau mengakses komputer atau sistem elektronik yang dilindungi oleh masyarakat, yang mengakibatkan komputer atau sistem elektronik tersebut menjadi rusak;
- g. Mempengaruhi atau mengakibatkan terganggunya komputer atau sistem elektronik yang digunakan oleh pemerintah;
- h. Menyebarkan atau memperdagangkan, atau memanfaatkan kode akses atau informasi yang serupa dengan hal tersebut, yang dapat digunakan menerobos komputer atau sistem elektronik dengan tujuan menyalahgunakan komputer atau sistem elektronik yang digunakan atau dilindungi oleh pemerintah; atau
- i. Menggunakan perbuatan dalam rangka hubungan internasional dengan maksud merusak komputer atau sistem elektronik lainnya yang dilindungi negara dan berada di wilayah yurisdiksi Indonesia dan ditujukan kepada siapa pun;

Pasal 333 KUHP dapat dikenakan pada kasus *deface* atau *hacking* serta data *interference* (menggangu data komputer) dan *system interference* (menggangu sistem komputer), yang membuat sistem milik orang lain, seperti *website* atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya.

#### **Pasal 334 KUHP**

Dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun atau pidana denda paling banyak kategori VI, setiap orang yang;

- a. Tanpa hak atau melampaui wewenangnya menggunakan atau mengakses komputer atau sistem elektronik dengan maksud memperoleh keuntungan atau memperoleh informasi keuangan dari bank sentral, lembaga perbankan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayaran atau yang mengandung data laporan nasabahnya;
- b. Tanpa hak menggunakan data atau mengakses dengan cara apa pun kartu kredit atau kartu pembayaran milik orang lain dalam transaksi elektronik untuk memperoleh keuntungan;
- c. Tanpa hak atau melampaui wewenangnya menggunakan atau mengakses komputer atau sistem elektronik bank sentral, lembaga perbankan atau lembaga keuangan yang dilindungi, dengan maksud menyalahgunakan, atau untuk mendapatkan keuntungan daripadanya; atau
- d. Menyebarkan, memperdagangkan, atau memanfaatkan kode akses atau informasi yang serupa dengan hal tersebut yang dapat digunakan menerobos komputer atau sistem elektronik dengan maksud menyalahgunakan yang akibatnya dapat memengaruhi sistem

elektronik bank sentral, lembaga perbankan atau lembaga keuangan, serta perniagaan di dalam dan luar negeri.

Pasal 334 KUHP ini dikenakan untuk kasus *carding* dimana pelaku mencuri nomor kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang diambil dengan menggunakan software card generator di internet untuk melakukan transaksi di *e-commerce*. Setelah dilakukan transaksi dan barang dikirimkan, kemudian penjual yang ingin mencairkan uangnya di bank ternyata ditolak karena pemilik kartu bukanlah orang yang melakukan transaksi.

#### **Pasal 407 KUHP**

- (1) Setiap orang yang memproduksi, membuat, memperbanyak, menggandakan, menyebarkan, menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan, pornografi, dipidana dengan pidana penjara paling singkat 6 (enam) bulan atau pidana penjara paling lama 10 (sepuluh) tahun atau pidana denda paling sedikit kategori IV dan pidana denda paling banyak kategori VI.

Pasal ini dapat dikenakan untuk penyebaran pornografi maupun website porno yang banyak beredar dan mudah diakses di internet. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut di luar negeri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang illegal.

#### **Pasal 426 KUHP**

- (1) Dipidana dengan pidana penjara paling lama 9 (Sembilan) tahun atau pidana denda paling banyak kategori VI, setiap orang yang tanpa izin;
- a. Menawarkan atau memberikan kesempatan untuk main judi dan menjadikan sebagai mata pencaharian atau turut serta dalam perusahaan perjudian;
  - b. Menawarkan atau memberi kesempatan kepada umum untuk main judi atau turut serta dalam perusahaan perjudian, terlepas dari ada tidaknya suatu syarat atau tata cara yang harus dipenuhi untuk menggunakan kesempatan tersebut; atau
  - c. Menjadikan turut serta pada permainan judi sebagai mata pencaharian.

- (2) Jika tindak pidana sebagaimana dimaksud pada ayat (1) dilakukan dalam menjalankan profesi, dapat dijatuhi pidana tambahan berupa pencabutan hak sebagaimana dimaksud dalam pasal 86 huruf f.

**Pasal 427 KUHP**

Setiap orang yang menggunakan kesempatan main judi yang diadakan tanpa izin, dipidana dengan pidana penjara paling lama 3 (tiga) tahun atau pidana denda paling banyak kategori III.

Kedua pasal diatas dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di internet.

**Pasal 433 KUHP**

- (1) Setiap orang yang dengan lisan menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal, dengan maksud supaya hal tersebut diketahui umum, dipidana karena pencemaran, dengan pidana penjara paling lama 9 (Sembilan) bulan atau pidana denda paling banyak kategori II.
- (2) Jika perbuatan sebagaimana dimaksud pada ayat (1) dilakukan dengan tulisan atau gambar yang disiarkan, dipertunjukkan atau ditempelkan di tempat umum, dipidana karena pencemaran tertulis, dengan pidana penjara lama 1 (satu) tahun 6 (enam) bulan atau pidana denda paling banyak kategori III.
- (3) Perbuatan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak dipidana jika dilakukan untuk kepentingan umum karena terpaksa membela diri.

Pasal ini dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media internet. Modusnya adalah pelaku menyebarkan email kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan email ke suatu mailing list sehingga banyak orang mengetahui cerita tersebut. tindakan penghinaan ataupun pencemaran dapat ditemukan di berbagai kolom komentar di dunia maya, terutama ketika korban memindai identitas, foto, atau video pribadinya.

**Pasal 482 KUHP**

- (1) Dipidana karena pemerasan dengan pidana penjara paling lama 9 (Sembilan) tahun, setiap orang dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa orang dengan kekerasan atau ancaman kekerasan untuk;

- a. Memberikan suatu barang, yang sebagian atau seluruhnya milik orang tersebut atau milik orang lain; atau
  - b. Memberikan utang, membuat pengakuan utang, atau menghapuskan piutang.
- (2) Ketentuan sebagaimana dimaksud dalam pasal 479 ayat (2) sampai dengan ayat (4) berlaku juga bagi pemerasan sebagaimana dimaksud pada ayat (1).

#### **Pasal 483 KUHP**

- (1) Dipidana karena pengancaman dengan pidana penjara paling lama 4 (empat) tahun atau pidana denda paling banyak kategori IV, setiap orang dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan ancaman pencemaran atau pencemaran tertulis atau dengan ancaman akan membuka rahasia, memaksa orang supaya:
- a. Memberikan suatu barang yang sebagian atau seluruhnya milik orang tersebut atau milik orang lain; atau
  - b. Memberi utang, membuat pengakuan utang, atau menghapuskan piutang.
- (2) Tindak pidana sebagaimana dimaksud pada ayat (1) hanya dapat dituntut atas pengaduan korban tindak pidana.

Dari kedua pasal diatas dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui e-mail yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku biasanya mengetahui rahasia korban. Berdasarkan beberapa penjelasan tersebut bahwa terdapat 9 pasal yang mengatur tentang tindak pidana *cyber crime* dalam KUHP terbaru yaitu dalam UU No. 1 Tahun 2023.

3. Undang-Undang No. 19 Tahun 2016 atas Perubahan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Hadirnya Undang-Undang No. 19 Tahun 2016 atas Perubahan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), tidak terlepas dari perkembangnya penggunaan teknologi. Kejahatan-kejahatan siber yang berkembang saat ini, merupakan dampak dari digitalisasi dan

membatasi perbuatan-perbuatan yang dilarang menurut hukum. UU ITE sejatinya menjadi regulator berkenaan dengan transaksi elektronik, dan kejahatan-kejahatan yang merupakan perluasan dari kejahatan yang tercantum dalam KUHP.<sup>96</sup>

Kejahatan merupakan entitas yang selalu melekat dengan dinamika perkembangan peradaban umat manusia. Kejahatan yang oleh saparinah sadli disebut sebagai perilaku menyimpang, selalu ada dan melekat pada setiap bentuk masyarakat; oleh karena itu, upaya penanggulangan kejahatan sesungguhnya merupakan usaha yang terus menerus dan terus berkesinambungan. Semakin majunya peradaban manusia, sebagai implikasi dari perkembangan ilmu pengetahuan dan teknologi, munculnya berbagai jenis kejahatan berdimensi baru, yang termasuk di dalamnya *cyber crime*. sejalan dengan itu diperlukan upaya penanggulangan untuk menjamin ketertiban dalam masyarakat. Dalam perspektif hukum, upaya ini direalisasikan dengan hukum pidana. Hukum pidana diharapkan mampu memenuhi ketertiban masyarakat.

Akan tetapi dalam menghadapi perkembangan masyarakat, hukum pidana tidak selamanya mampu menjawab terhadap dampak negatif yang timbul dari kejahatan. Hal ini dikarenakan teknologi yang membawa perubahan dalam masyarakat begitu pesat, sementara hukum pidana merupakan produk sejarah tertentu berjalan dengan logika sejarah yang menanginnya walaupun dalam batas tertentu mempunyai prediktabilitas atas perkembangan masyarakat.

Dua muatan besar yang diatur dalam UU ITE ialah mengenai pengaturan transaksi elektronik dan mengenai tindak pidana siber. Pada UU ITE dimuat

---

<sup>96</sup> Yurizal, *Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia*, (Malang: Media Nusa Creative, 2018).

tentang perbuatan yang dilarang pada pasal 27 sampai pasal 37. Konstruksi pasal-pasal tersebut mengatur secara lebih detail tentang pengembangan modus-modus kejahatan tradisional sebagaimana yang tercantum dalam kitab undang-undang hukum pidana (KUHP).<sup>97</sup>

Pasal 27 misalnya, mengatur masalah pelanggaran kesusilaan, perjudian, pencemaran nama baik, dan tindakan pemerasan dan pengancaman. Untuk lebih jelasnya dapat dilihat sebagai berikut:

**Pasal 27**

- (4) Setiap orang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
- (5) 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 perjudian.
- (6) Setiap orang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
- (7) Setiap orang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.<sup>98</sup>

Pasal 27 di atas menjelaskan perkembangan modus kejahatan dan/atau pelanggaran dengan media komputer/internet (dalam bentuk informasi/dokumen elektronik). Hal tersebut sangatlah penting khususnya membantu para penegak hukum dalam memproses dan mengadili kasus-kasus yang telah menggunakan media informasi elektronik untuk memuluskan kejahatan/pelanggaran yang dilakukan.

<sup>97</sup> Yurizal, *Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia*, (Malang: Media Nusa Creative, 2018).

<sup>98</sup> Undang-Undang Republik Indonesia No. 19 Tahun 2019 Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE).

Di sisi lain persoalan SARA merupakan persoalan kebangsaan yang sangat rentan untuk menimbulkan konflik. Indonesia sebagai bangsa yang memiliki tingkat heterogenitas yang cukup tinggi telah menjadikan “SARA” sebagai salah satu produk konflik yang sangat mudah tersulut. Oleh karena itu, perkembangan modus pengoptimalisasian “SARA” sebagai produk yang rawan konflik harus diatur dengan penyesuaian perkembangan modus yang menggunakan media komputer/internet. Lebih jelasnya dapat dilihat sebagai berikut:

#### **Pasal 28**

- (1) Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
- (2) Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).<sup>99</sup>

Pasal 28 mengatur tentang perlindungan konsumen dan aspek SARA. Hal ini sangat beralasan mengingat banyak transaksi perdagangan yang dilakukan dengan menggunakan media komputer/internet di mana baik produsen maupun konsumen tidak pernah bertemu satu sama lainnya. Sehingga aspek kepercayaan (trust) memegang peranan penting dalam transaksi perdagangan.

#### **Pasal 29**

Setiap orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakutkan yang ditujukan secara pribadi.

Pasal 29 UU ITE dapatlah dianggap sebagai suatu perkembangan yang sangat signifikan dalam pengaturan hukum mengenai adanya ancaman yang sering dilakukan dan/atau dialamatkan kepada seseorang dengan menggunakan

---

<sup>99</sup>Undang-Undang Republik Indonesia No. 19 Tahun 2019 Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE).

media informasi/dokumen elektronik. Perkembangan produk elektronik sangatlah memudahkan bagi seseorang untuk memuluskan langkah jahatnya dalam mencapai tujuan yang diinginkan.

Pasal 30 UU ITE menyebutkan bahwa:

**Pasal 30**

- (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun.
- (2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
- (3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.<sup>100</sup>

Pasal 30 diatas dengan jelas menyebutkan bahwa tindak illegal yang dilakukan seseorang (*criminal*) terhadap sistem elektronik orang lain dengan tujuan untuk memperoleh informasi/dokumen elektronik dan/atau upaya pembobolan, penerobosan, dan penjebolan, yang melanggar dan melampaui sistem pengamanan yang dilarang. Beberapa kasus yang relevan dan telah terjadi dalam praktik dunia siber dapat dilihat pada kasus pembobolan kartu kredit, pembobolan situs KPU, penyerangan terhadap situs website secretariat Kabinet RI, peretasan website BPJS Kesehatan dan masih banyak contoh kasus lainnya.

**Pasal 31**

- (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain.

---

<sup>100</sup> Undang-Undang Republik Indonesia No. 19 Tahun 2019 Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE).

- (2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, yang bersifat publik dari, ke, dan di dalam suatu komputer dan/atau sistem elektronik milik orang lain, baik yang tidak menyebabkan perubahan apapun maupun adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan.

### **Pasal 32**

- (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun untuk mengubah, menambah, mengurangi dan melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik orang lain atau milik publik.
- (2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik milik orang lain yang tidak berhak.
- (3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu informasi elektronik dan /atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal 32 ini berisikan kategori perbuatan yang dilarang adalah setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik atau dokumen elektronik milik orang lain atau milik publik. Sehingga informasi elektronik atau dokumen elektronik tersebut dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Berdasarkan rumusan perbuatan yang dikriminalisasi sebagai tindak pidana siber dalam UU ITE terdapat unsur delik yang dirumuskan, yaitu unsur “dengan sengaja” dan “tanpa hak”. Dalam beberapa pasal unsur “tanpa hak” dirumuskan alternative dengan “melawan hukum”, penggunaan kata “dengan

sengaja” mengandung arti bahwa tindak pidana siber sebagaimana diatur dalam UU ITE diancam dengan pidana apabila melakukannya dengan sengaja.

Segala upaya yang bersifat mengikat, lebih banyak memberikan informasi mengenai hukuman dan jenis pelanggaran/kejahatan dunia maya secara spesifik. *Cyberlaw* merupakan istilah hukum yang terkait dengan pemanfaatan TI. Istilah lain adalah hukum TI (*Law Of IT*), hukum dunia maya (*Virtual World Law*) dan hukum mayantara. Perkembangan teknologi yang sangat pesat membutuhkan pengaturan hukum yang berkaitan dengan pemanfaatan teknologi tersebut. Ruang lingkup dari *cyberlaw* adalah: <sup>101</sup>

- a. Hak cipta, hak merek, pencemaran nama baik (*defamation*), *hate speech* (fitnah, penistaan dan penghinaan),
- b. Serangan terhadap fasilitas komputer (*hacking, viruses, illegal access*), pengaturan sumber daya internet *IP address, domain name*,
- c. Kenyamanan individu (*privacy*), tindakan kriminal yang bisa menggunakan TI sebagai alat.
- d. Isu procedural (yurisdiksi, pembuktian, penyidikan), transaksi elektronik dan digital, pornografi,
- e. Perlindungan konsumen, pemanfaatan internet dalam aktifitas keseharian (*e-commerce, e-government, e-education, e-medics*).

#### 4. Undang-Undang No.28 Tahun 2014 tentang Hak Cipta

Berdasarkan Undang-Undang ini, suatu program atau data mempunyai nilai puluhan kali lipat dibandingkan nilai dari komputer atau media lainnya

---

<sup>101</sup> Renny NS. Koloay “Perkembangan Hukum Indonesia Berkenaan dengan Teknologi Informasi dan Komunikasi” *Jurnal Hukum Unsrat*,22,No.5 (12 Januari 2016),23.

dimana data atau program tersebut tersimpan yang menjadikan banyak orang yang ingin mengambilnya secara tidak sah untuk disalah gunakan atau diambil manfaatnya tanpa izin pemiliknya. Menurut pasal 1 angka (9) Undang-Undang No. 28 Tahun 2014 tentang Hak Cipta, bahwa program komputer adalah seperangkat instruksi yang diekspresikan dalam bentuk bahasa, kode skema atau dalam bentuk lain yang ditujukan agar komputer bekerja untuk melakukan fungsi tertentu atau untuk mencapai hasil tertentu. Hak cipta untuk program komputer berlaku selama 50 tahun (pasal 59).<sup>102</sup>Harga program komputer/software yang sangat mahal bagi warga negara Indonesia merupakan peluang yang cukup menjanjikan bagi para pelaku bisnis guna mengadakan serta menjual software bajakan dengan harga yang sangat murah. Maraknya pembajakan software di Indonesia yang terkesan “dimaklumi” tentunya sangat merugikan pemilik hak cipta. Tindakan pembajakan program komputer tersebut merupakan delik aduan (pasal 120).

5. Undang-Undang No. 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme.

Undang-Undang No. 5 Tahun 2018 ini mengatur mengenai alat bukti elektronik sesuai dengan pasal 27 huruf (b) yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu. Digital evidence atau alat bukti elektronik sangatlah berperan dalam penyelidikan kasus terorisme, karena saat ini komunikasi antar para pelaku di lapangan dengan pimpinan atau aktor intelektualnya dilakukan dengan memanfaatkan fasilitas di internet untuk

---

<sup>102</sup> Renny NS. Koloay “Perkembangan Hukum Indonesia Berkenaan dengan Teknologi Informasi dan Komunikasi” *Jurnal Hukum Unsrat*,22,No.5 (12 Januari 2016),13.

menerima pemerintah atau menyampaikan kondisi dilapangan karena para pelaku mengetahui pelacakan terhadap internet lebih sulit dibandingkan pelacakan melalui handphone. Berkaitan dengan penggunaan hukum pidana. Nigel walker sebagaimana dikutip oleh Muladi, mengatakan bahwa ada 6 (enam) syarat prinsip yang harus diperhatikan oleh pembentuk Undang-Undang, yaitu: <sup>103</sup>

- a. Hukum pidana tidak digunakan semata-mata untuk tujuan pembalasan;
- b. Tindak pidana yang dilakukan harus menimbulkan kerugian dan korban yang jelas;
- c. Hukum pidana tidak digunakan apabila masih ada cara lain yang lebih baik dan lebih prima;
- d. Kerugian yang ditimbulkan karena ppidanaan harus lebih kecil dari pada akibat tindak pidana;
- e. Harus mendapatkan dukungan masyarakat; dan
- f. Harus dapat diterapkan dengan efektif.

Perlu diperhatikan juga pendapat Sudarto mengenai pengguna hukum pidana dan kriminalisasi suatu perbuatan menjadi tindak pidana, sebagai berikut: <sup>104</sup>

- a) Hukum pidana harus digunakan untuk mewujudkan masyarakat adil dan makmur,
- b) Merata materil dan spiritual.
- c) Hukum pidana bertugas untuk menanggulangi dan tindak penanggulangan itu sendiri untuk kesejahteraan masyarakat atau untuk pengayoman masyarakat.

<sup>103</sup> Teguh Prasetyo, *Hukum Pidana*, (Jakarta:PT. Raja Grafindo Persada, 2016),130.

<sup>104</sup> M. Ramli. Ahmad, *Cyber Law dan Haki dalam Sistem Hukum Indonesia*,(Bandung: Pt. Refika Aditama, 2006) 127.

- d) Hukum pidana digunakan untuk mencegah atau menaggulangi perbuatan yang tidak dikehendaki, yaitu perbuatan yang mendatangkan kerugian pada masyarakat.
- e) Penggunaan sarana hukum pidana dengan saksi yang negatif perlu disertai dengan perhitungan biaya yang harus dikeluarkan dan hasil yang diharapkan akan dicapai (*cost and benefit principle*).

#### 6. Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi

Menurut Pasal 1 Undang-Undang No. 36 Tahun 1999, telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optic, radio, atau sistem elektromagnetik lainnya. Dari definisi tersebut, maka internet dan segala aktifitas yang dimilikinya merupakan salah satu bentuk alat komunikasi karena dapat mengirimkan dan menerima setiap informasi dalam bentuk gambar, suara maupun film dengan sistem elektromagnetik. Penyalahgunaan internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan Undang-Undang ini:

- a. *Illegal access*, perbuatan melakukan akses secara tidak sah terhadap sistem komputer ini belum diatur secara jelas di dalam sistem perundang-undangan di Indonesia. Untuk sementara waktu, Pasal 22 Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 tentang Telekomunikasi dapat diterapkan. Pasal 22 Undang-Undang Telekomunikasi Menyatakan:<sup>105</sup>

---

<sup>105</sup> M. Ramli. Ahmad, *Cyber Law dan Haki dalam Sistem Hukum Indonesia*, (Bandung: Pt. Refika Aditama, 2006) 129.

“setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi: a). akses ke jaringan telekomunikasi; dan/atau, b). akses ke jasa telekomunikasi; dan/atau, c). akses ke jaringan telekomunikasi khusus. Pasal 50 Undang-Undang telekomunikasi memberikan ancaman pidana terhadap barang siapa yang melanggar ketentuan pasal 22 Undang-Undang Telekomunikasi dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah).

semua tindak pidana dalam Undang-Undang Nomor 36 Tahun 1999 dinyatakan sebagai kejahatan.

- b. *Illegal interception in the computers, systems and computer networks operation* (interpretasi secara tidak sah terhadap operasional komputer, sistem, dan jaringan komputer). Pasal 40 Undang-Undang Telekomunikasi dapat diterapkan terhadap jenis perbuatan intersepsi ini. Pasal 56 Undang-Undang Telekomunikasi memberikan ancaman pidana terhadap barang siapa yang melanggar ketentuan pasal 40 tersebut dengan pidana penjara paling lama 15 (lima belas) tahun.

#### 7. Undang-Undang No. 32 Tahun 2002 tentang Penyiaran

- a) Pasal 57 Jo. Pasal 36 ayat (5) mengancam pidana terhadap siaran yang: 1. Bersifat fitnah, menghasut, menyesatkan, dan/atau bohong. 2. Menonjolkan unsur kekerasan, cabul, perjudian, penyalahgunaan narkoba dan obat terlarang; atau. 3. Mempertentangkan suku, agama, ras, dan antar golongan.
- b) Pasal 57 Jo. Pasal 36 ayat (6) mengancam pidana terhadap siaran yang memperolokkan, merendahkan dan/atau mengabaikan nilai-nilai agama, martabat, atau merusak hubungan internasional.<sup>106</sup>

#### 8. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi

<sup>106</sup> M. Ramli. Ahmad, *Cyber Law dan Haki dalam Sistem Hukum Indonesia*, (Bandung: Pt. Refika Aditama, 2006) 130..

Perlindungan data pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari perlindungan dari pribadi dan ditujukan untuk menjamin hak warga negara atas perlindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya perlindungan data pribadi. Dengan adanya undang-undang 27 tahun 2022 tentang perlindungan data pribadi, pemerintah dan masyarakat memiliki pengaturan hukum yang jelas, agar data pribadi yang dimiliki dapat terjaga dengan baik.

pasal 65 Undang-Undang Nomor 12 Tahun 2022 yang menyatakan bahwa:

- (1) Setiap orang yang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi.
- (2) Setiap orang dilarang secara melawan hukum mengungkapkan data pribadi yang bukan miliknya.
- (3) Setiap orang dilarang secara melawan hukum menggunakan data pribadi yang bukan miliknya.

#### **Pasal 66**

Setiap orang yang dilarang membuat data pribadi palsu atau memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain.

#### **Pasal 67**

- (1) Setiap orang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi sebagaimana dimaksud dalam pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp.5.000.000.000,00 (lima miliar rupiah).
- (2) Setiap orang dengan sengaja dan melawan hukum mengungkapkan data pribadi yang bukan miliknya sebagaimana dimaksud dalam pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp.4.000.000.000,00 (empat miliar rupiah).
- (3) Setiap orang dengan sengaja dan melawan hukum menggunakan data pribadi yang bukan miliknya sebagaimana dimaksud dalam pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp.5.000.000.000,00 (lima miliar rupiah).

## Pasal 68

Setiap orang dengan sengaja membuat data pribadi palsu atau memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain sebagaimana dimaksud dalam pasal 66 dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau pidana denda paling banyak Rp. 6.000.000.000,00 (enam miliar rupiah).

Dengan ditetapkannya Undang-Undang tentang perlindungan data pribadi diharapkan perlindungan data pribadi masyarakat dapat terjamin dan dilindungi serta bagi oknum yang selalu memanfaatkan data pribadi keuntungan sendiri bisa mendapatkan efek jera karena sudah terdapat sanksi administratif serta sanksi pidana bagi yang dengan sengaja dan melawan hukum terhadap Undang-Undang tentang Perlindungan data pribadi Islam adalah agama yang banyak berbicara tentang keamanan. Beberapa diantaranya dapat kita temukan dalam Q.S An-Nur ayat 27:

يٰۤاَيُّهَا الَّذِيْنَ ءَامَنُوْا لَا تَدْخُلُوْا بُيُوْتًا غَيْرَ بُيُوْتِكُمْ حَتّٰى تَسْتَأْذِنُوْا وَّتَسَلِّمُوْا  
عَلٰى اَهْلِهَا ذٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُوْنَ

Terjemahnya : Hai orang-orang yang beriman, janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. yang demikian itu lebih baik bagimu, agar kamu (selalu) ingat.

فَاِنْ لَّمْ تَجِدُوْا فِيْهَا اَحَدًا فَلَا تَدْخُلُوْهَا حَتّٰى يُؤْذَنَ لَكُمْ وَاِنْ قِيْلَ لَكُمْ  
اَرْجِعُوْا فَاَرْجِعُوْا هُوَ اَزْكٰى لَكُمْ وَاللّٰهُ بِمَا تَعْمَلُوْنَ عَلِيْمٌ

Terjemahnya: jika kamu tidak menemui seorangpun didalamnya, Maka janganlah kamu masuk sebelum kamu mendapat izin. dan jika dikatakan kepadamu: "Kembali (saja)lah, Maka hendaklah kamu kembali. itu bersih bagimu dan Allah Maha mengetahui apa yang kamu kerjakan.

Kedua Ayat tersebut diatas menegaskan bahwa agama islam secara jelas dan nyata mengatur mengenai perlindungan data pribadi. Data pribadi harus dilindungi karena jika bocot atau disalahgunakan dapat merusak harkat dan martabat seseorang. Dalam konsepnya, melindungi informasi yang bersifat pribadi merupakan kebutuhan primer karena tergolong dalam maqashid syari'at, yaitu perlindungan kehormatan diri (*hifdzul'irdh*).

Berdasarkan analisis tersebut dapat disimpulkan bahwa aturan mengenai kasus *cyber crime* di Indonesia terdapat dalam beberapa UU yaitu KUHP, Undang-Undang Nomor 19 Tahun 2016 Perubahan Undang-Undang No.11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik (UU ITE), Undang-Undang No.28 Tahun 2014 tentang Hak Cipta, Undang-Undang No. 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme, Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi, dan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.

### **BAB III**

## **KENDALA DALAM PENANGANAN *CYBER CRIME* DI INDONESIA**

#### **A. Faktor Yang Mempengaruhi Terjadinya *Cyber Crime***

Soerjono Soekanto mengemukakan bahwa secara konseptual penegakan hukum adalah kegiatan menyerasikan hubungan nilai-nilai yang terjabarkan dalam kaidah-kaidah dan sikap tindak sebagai rangkaian penjabaran nilai tahap akhir, untuk menciptakan, memelihara dan mempertahankan kedamaian pergaulan hidup.<sup>107</sup> Dengan kata lain penegakan hukum merupakan suatu sistem yang menyangkut penyerasian antara nilai dengan kaidah serta perilaku nyata manusia. Dengan demikian penegakan hukum pidana merupakan pelaksanaan dari peraturan-peraturan pidana. Kaidah-kaidah tersebut menjadi pedoman atau tindakan atau perilaku yang dianggap pantas dan seharusnya. Perilaku atau sikap tindak itu bertujuan untuk memelihara, menciptakan, dan mempertahankan kedamaian.

Masalah pokok yang melanda penegakan hukum yakni terdapat pada faktor- faktor yang mempengaruhinya secara langsung maupun tidak langsung. Yang mana faktor tersebut mempunyai arti yang netral.<sup>108</sup> Menurut Soerjono Soekanto faktor-faktornya adalah:

---

<sup>107</sup> Soerjono Soekanto . *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum*, (Jakarta: UI Press,1983)

<sup>108</sup> M.Faal. *Penyaringan Perkara Pidana Oleh Polisi (Deskresi Kepolisian)*, (Jakarta: PT.Pradnya Paramita,1991)

a. Faktor Hukumnya Sendiri atau Peraturan Itu Sendiri

Meskipun eksistensi pengaturan tindak pidana *cyber crime* tidak hanya dalam Undang-Undang Nomor 19 Tahun 2016 atas perubahan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, tetapi terdapat juga didalam Undang-Undang khusus di luar KUHP. Salah satu asas dalam hukum pidana menentukan bahwa tiada perbuatan yang dapat dihukum pidana jikalau hal belum dinyatakan dalam suatu aturan Perundang-Undangan (asas legalitas). Menurut Muladi bahwa secara oprasional Perundang-Undangan pidana mempunyai kedudukan strategis terhadap sistem peradilan pidana. Yang mana hal tersebut memberikan definisi tentang perbuatan yang dirumuskan sebagai tindak pidana. Mengendalikan usaha-usaha pemerintah untuk memberantas kejahatan dan memidana sipelaku, memberikan batasan tentang pidana yang dapat diterapkan untuk setiap kejahatan. dengan kata lain yang mengatur segala prosedur dan tata cara yang harus dipatuhi didalam berbagai perangkat system peradilan pidana yaitu Peraturan Perundang-Undangan pidana yang menciptakan dan mengatur segala prosedur dan tata cara yang harus dipenuhi dalam berbagai perangkat system peradilan pidana.<sup>109</sup>

b. Faktor Penegak Hukum

Faktor penegak hukum menjadi penyebab maraknya kejahatan *cyber crime*.. hal ini dilatarbelakangi kurangnya pengetahuan dan kemampuan penegak hukum dibidang IT dan pemahaman tentang seluk beluk teknologi informasi (internet), sehingga pada saat pelaku tindak pidana ditangkap, aparat penegak

---

<sup>109</sup> Muladi. *Kapita Selektia Peradilan Pidana* (Semarang: UNDIP,1995).

hukum mengalami kesulitan untuk menemukan alat bukti yang dapat dipakai menjerat pelaku, terlebih apabila kejahatan melawan hukum yang dilakukan di dunia maya memiliki sistem pengoperasian yang sangat rumit. Disamping itu, aparat penegak hukum di daerah pun belum siap dalam mengantisipasi maraknya kejahatan ini terlebih apabila daerah tersebut belum dilengkapi dengan jaringan internet. Perlu diketahui, dengan teknologinya yang semakin canggih, memungkinkan kejahatan yang dilakukan di suatu daerah dan akibat yang ditimbulkan dapat terjadi di daerah lain, bahkan hingga keluar negeri.

c. Faktor Sarana dan Fasilitas Pendukung

Kurangnya sarana dan prasarana dalam mengungkap kasus *cyber crime* saat ini seperti halnya peralatan *computer forensic* yang canggih guna pembuktian kejahatan *cyber*. Jika fasilitas pendukung tidak terpenuhi maka mustahil penegak hukum akan mencapai tujuannya. Kepastian dan kecepatan penyelesaian perkara tergantung pada fasilitas pendukung yang ada dalam bidang-bidang pencegahan dan pemberantasan kejahatan. Untuk itu Faktor sarana atau fasilitas khusus untuk kepentingan penyidikan tindak pidana *cyber crime* mutlak di perlukan, khususnya oleh penyidik Polri karena pada tahap penyelidikan dan/atau penyidikan.<sup>110</sup>

d. Faktor Masyarakat

*Cyber crime* adalah sebuah perbuatan yang tercela serta melanggar kepatuhan di masyarakat serta perbuatan melawan hukum, meskipun Undang-Undang secara khusus mengatur *cyber crime*, namun hal tersebut belum sepenuhnya dapat dipatuhi dan disadari oleh seluruh pengguna layanan teknologi

---

<sup>110</sup> Soerjono Soekanto . *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*, (Jakarta: UI Press,1983)

informasi sebagai instrument hukum. Sampai saat ini kesadaran hukum masyarakat Indonesia dalam merespon aktivitas *cyber crime* masih dirasakan kurang. Hal ini disebabkan karena kurangnya pengetahuan dan pemahaman masyarakat terhadap jenis kejahatan *cyber crime*. dimana hal ini dapat menyebabkan upaya penanganan *cyber crime* mengalami kendala, dalam hal ini kendala yang berkenaan dengan penataan hukum dan proses pengawasan masyarakat terhadap setiap aktivitas yang diduga berkaitan dengan *cyber crime*.

e. Faktor Kebudayaan

Faktor lain yang mempengaruhi yaitu nilai kebudayaan, faktor kecenderungan untuk tidak melaporkan kejahatan atau sikap toleransi terhadap tindakan ilegal, juga dapat berkontribusi pada tingkat kejahatan *cyber*. Sikap yang tidak proaktif terhadap kejahatan *cyber crime* atau sikap yang kurang peduli dapat mempengaruhi tingkat kejahatan di masyarakat. ada beberapa faktor kebudayaan yang dapat mempengaruhi terjadinya *cyber crime* di Indonesia, diantaranya:<sup>111</sup>

**Pertama**, pendidikan dan kesadaran digital: Tingkat pendidikan dan kesadaran digital dimasyarakat memiliki peran penting dalam mempengaruhi tingkat kejahatan *cyber*. Jika tingkat pendidikan digital rendah dan kesadaran tentang ancaman kejahatan *cyber* minim, individu cenderung lebih rentan terhadap serangan dan penipuan online. **Kedua**, budaya kerja dan etika: budaya kerja yang kurang mengedepankan integritas dan etika dapat memicu tindakan penipuan dan pengelapan melalui media digital. Jika terdapat budaya yang meremehkan pentingnya kejujuran dan tanggungjawab, resiko terjadinya kejahatan *cyber*

---

<sup>111</sup> Soerjono Soekanto. *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum*, (Jakarta: UI Press,1983)

meningkat. **Ketiga**, penghargaan terhadap privasi dan keamanan data: budaya yang kurang memperhatikan privasi dan keamanan data dapat menyebabkan individu dan organisasi menjadi rentan terhadap serangan *cyber*. Jika penggunaan teknologi dan media digital tidak disertai dengan kesadaran akan perlunya melindungi privasi dan data pribadi, pelaku kejahatan dapat dengan mudah memanfaatkan celah tersebut. **Keempat**, budaya sosial media: Indonesia memiliki tingkat penggunaan media sosial yang tinggi. Budaya yang berkembang di media sosial, seperti keinginan untuk mendapatkan popularitas, pertumbuhan followers, dan pengaruh di platform online, dapat mendorong individu untuk terlibat dalam kegiatan ilegal seperti penyebaran hoax, kejahatan *cyber* terorganisir, atau penipuan online. **Kelima**, perilaku konsumsi online: budaya konsumsi online yang meningkat di Indonesia, seperti belanja online atau kegiatan perbankan digital, dapat meningkatkan resiko terjadinya *cyber crime*. Jika individu tidak mengadopsi praktik keamanan digital yang baik, seperti penggunaan kata sandi yang kuat, atau berbagi informasi pribadi dengan ceroboh, mereka menjadi lebih rentan terhadap serangan *cyber*.<sup>112</sup>

Kelima faktor diatas merupakan hal yang bisa mempengaruhi terjadinya kejahatan *cyber crime* Indonesia, yaitu ketidaksempurnaan sistem hukum terkait kejahatan *cyber* dan kurangnya kemampuan penegak hukum yang memadai dapat mempengaruhi angka keberhasilan penangkapan dan penuntutan pelaku *cyber crime* serta kurangnya sanksi yang memadai juga dapat mengurangi efektivitas penegakan hukum dalam mencegah dan mengurangi kejahatan siber. Teknologi

---

<sup>112</sup>Soerjono Soekanto. *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum*, (Jakarta: UI Press,1983)

dan penggunaan internet dimana pertumbuhan teknologi dan penetrasi internet di Indonesia telah membuka pintu bagi tindakan kriminal yang berkaitan dengan dunia maya. Semakin banyak orang yang menggunakan internet, maka semakin banyak juga potensi pelaku kejahatan *cyber*. Tingkat kesadaran dan pemahaman masyarakat tentang keamanan digital memainkan peran penting dalam pencegahan kejahatan *cyber*.

Kurangnya pemahaman tentang ancaman keamanan digital dapat membuat masyarakat menjadi target yang lebih mudah bagi pelaku kejahatan. Kesenjangan teknologi dan aksesibilitas dimana ketimpangan dalam akses teknologi dan internet antara perkotaan dan daerah pedesaan di Indonesia dapat menyebabkan perbedaan tingkat kejahatan *cyber*. Daerah dengan akses terbatas atau infrastruktur teknologi yang lemah mungkin menjadi sasaran yang lebih mudah bagi pelaku kejahatan, serta faktor kecenderungan untuk tidak melaporkan kejahatan atau sikap toleransi terhadap tindakan ilegal, juga dapat berkontribusi pada tingkat kejahatan *cyber*. Sikap yang tidak proaktif terhadap kejahatan *cyber crime* atau sikap yang kurang peduli dapat mempengaruhi tingkat kejahatan di masyarakat.<sup>113</sup> serta ada faktor lain lain yang juga dapat mempengaruhi terjadinya kejahatan *cyber crime* yaitu kondisi ekonomi yang sulit dan kurangnya kesempatan kerja yang dapat mendorong orang untuk terlibat dalam kegiatan kriminal, termasuk kejahatan *cyber*.

---

<sup>113</sup> Sutarman, *Pengantar Teknologi Informasi* (Yogyakarta: PT Bumi Aksara, 2009),

Kejahatan merupakan salah satu bentuk dari perilaku menyimpang yang selalu ada dan melekat pada tiap bentuk masyarakat.<sup>114</sup> Kejahatan terjadi tidak hanya disebabkan oleh faktor individu seseorang tetapi juga disebabkan oleh faktor eksternal seperti yang berasal dari lingkungan sekitar dan kehidupan sosialnya. *Cyber crime* semakin marak terjadi, yaitu ditandai dengan munculnya berbagai modus yang beraneka ragam. Para pelaku sangat lihai dalam menjalankan aksinya, mereka adalah individu yang cerdas dan kreatif. Namun mereka menggunakan kemampuan tersebut untuk melakukan suatu kejahatan yang dapat menimbulkan kerugian bagi orang lain baik itu kerugian materiil maupun immaterial. Selain faktor yang dikemukakan oleh Soerjono Soekanto diatas. Adapun beberapa faktor lain yang mempengaruhi adanya kejahatan *cyber crime* yaitu faktor politik, faktor ekonomi, dan faktor sosial budaya.

#### 1. Faktor Politik

Mencermati maraknya *cyber crime* yang terjadi di Indonesia dengan permasalahan yang dihadapi oleh aparat penegak hukum, proses kriminalisasi di bidang *cyber* telah terjadi dan merugikan masyarakat. media *cyber* memberitakan tentang *cyber crime* yang dilakukan oleh orang Indonesia, sebagaimana kasus yang terjadi di Indonesia mengakibatkan citra Indonesia kurang baik dimata dunia dalam penegakan hukum *cyber crime*.

Penyebaran virus komputer dapat merusak jaringan komputer yang digunakan oleh pemerintah, perbankan, pelaku usaha maupun perorangan yang dapat berdampak terhadap kekacauan dalam sistem jaringan. Dapat dipastikan

---

<sup>114</sup>Uladi dan Barda Nawawi Arief. *Teori-Teori Dan Kebijakan Pidana*, (Bandung: PT Alumni,2010), 148.

apabila sistem jaringan komputer perbankan tidak berfungsi dalam satu hari saja dapat menimbulkan kekacauan pembayaran maupun transaksi keuangan bagi nasabah. Kondisi ini memerlukan kebijakan politik pemerintah Indonesia untuk menganggulangi *cyber crime* yang berkembang di Indonesia. Aparat penegak hukum telah berupaya keras untuk menindak setiap pelaku *cyber crime*, tetapi penegakkan hukum tidak dapat berjalan maksimal sesuai harapan masyarakat. Untuk menghindari kerugian yang lebih besar akibat tindakan pelaku kejahatan *cyber crime* maka dikeluarkanlah UU No.19 Tahun 2016 perubahan atas UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang merupakan peraturan yang lebih khusus mengatur kejahatan yang berkaitan dengan teknologi informasi, sebagai kebijakan politik pemerintahan Indonesia untuk menanggulangi maraknya tindak pidana *cyber crime*. Dengan perangkat hukum ini aparat penegak hukum tidak ragu-ragu lagi dalam melakukan penegakan hukum terhadap *cyber crime*.<sup>115</sup>

## 2. Faktor Ekonomi

Kemajuan ekonomi suatu bangsa salah satunya dipengaruhi oleh promosi barang-barang produksi. Jaringan komputer dan internet merupakan media yang sangat murah untuk melakukan suatu promosi. Banyak masyarakat yang memanfaatkan media untuk mencari barang-barang kepentingan perorangan maupun korporasi. Produk barang yang dihasilkan oleh industri di Indonesia sangat banyak dan digemari oleh komunitas Internasional, seperti halnya barang kerajinan, ukiran dan barang-barang lainnya. Dengan itu para pelaku bisnis harus

---

<sup>115</sup> Sutarman, *Pengantar Teknologi Informasi* (Yogyakarta: PT Bumi Aksara, 2009),

mampu memanfaatkan sarana internet saat ini. Krisis ekonomi yang melanda bangsa Indonesia harus dijadikan pelajaran bagi masyarakat untuk segera bangkit. Seluruh komponen bangsa Indonesia harus berpartisipasi untuk mendukung pemulihan ekonomi. Media internet dan jaringan komputer merupakan salah satu media yang dapat dimanfaatkan oleh seluruh masyarakat untuk memperkenalkan Indonesia pada dunia.

### 3. Faktor Sosial Budaya

Untuk faktor sosial budaya dapat dilihat dari beberapa aspek, yaitu:

#### a) Kemajuan Teknologi Informasi

Pesat kemajuan teknologi informasi sungguh tidak dapat dibendung oleh siapapun di negeri ini. Semua orang sangat membutuhkan teknologi, informasi, bahkan 'levelitas' kebutuhan setiap orang terhadap teknologi itu berbeda-beda. Ada yang menganggap sebagai sebuah kebutuhan primer, setelah kebutuhan makan dan minum. Sehari tanpa informasi, diibaratkan sehari tanpa minum, oleh karenanya tak mengherankan jika terbentuklah sebuah komunitas baru dunia informasi (TI) yang memainkan peran penting bagi kesejahteraan manusia, termasuk pertumbuhan ekonomi, politik, sosial budaya, dan aspek kehidupan yang lainnya. Menurut Agus Raharjo setidaknya ada 2 (dua) hal yang membuat teknologi informasi dianggap penting dalam memacu pertumbuhan ekonomi dunia yaitu : **pertama** teknologi informasi mendorong permintaan atas produk-produk teknologi informasi itu sendiri, seperti komputer, modem, sarana untuk

membangun jaringan internet dan sebagainya. **Kedua** memudahkan transaksi bisnis terutama bisnis keuangan di samping bisnis umum lainnya.<sup>116</sup>

Meskipun peranan tersebut lebih condong pada bidang ekonomi, namun dapat dilihat betapa pentingnya peranan teknologi informasi untuk mengefektifkan layanan dan kepentingan sebagai tenaga dorong kemajuan komunikasi global dengan berbagai pihak agar maksud dan tujuan masing-masing dapat tercapai.

#### b) Sumber Daya Manusia yang Berpengalaman

Sumber daya manusia dalam teknologi informasi mempunyai peranan penting sebagai pengendali dari sebuah alat. Yang mana apakah alat itu digunakan sebagai sarana kebijakan untuk mencapai kesejahteraan umat manusia, ataukah alat itu akan dikriminalisasikan sehingga dapat merugikan kepentingan orang lain atau bahkan dapat merusak kepentingan negara dan masyarakat. Teknologi sebagai hasil dan pengembangan manusia kemudian dimanfaatkan dalam berbagai aspek, namun disisi lain dapat membawa petaka bagi umat manusia sebagai akibat adanya penyimpangan. Di Indonesia sumber daya pengelola teknologi informasi ini cukup, namun sumber daya manusia untuk memproduksi atau menciptakan teknologi ini masih kurang. Penyebab adanya berbagai hal, diantaranya yaitu kurangnya tenaga peneliti dan kurangnya biaya penelitian atau mungkin kurangnya perhatian dan apresiasi terhadap penelitian. Sehingga sumber daya

---

<sup>116</sup>Agus Raharjo, *Cyber Crime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* (Bandung: Citra Aditya Bakti, 2002), 1.

manusia di Indonesia lebih banyak sebagai pengguna saja dan jumlahnya cukup banyak.<sup>117</sup>

c) Komunitas baru

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

Adapun beberapa faktor-faktor lain yang mempengaruhi terjadinya *cyber crime* diantaranya, yaitu:<sup>118</sup>

a) Akses Internet Yang Tidak Terbatas.

Saling terhubungnya antara jaringan yang satu dengan yang lain memudahkan pelaku kejahatan untuk melakukannya. Dengan menggunakan internet juga kita diberikan kenyamanan dan kemudahan dalam mengakses segala sesuatu tanpa ada batasannya. Dengan kenyamanan itulah yang menjadi faktor utama bagi sebagian oknum untuk melakukan tindak kejahatan *cyber crime* dengan mudahnya.

<sup>117</sup> Sutarman. *pengantar teknologi informasi* (Yogyakarta:PT.Bumi aksara,2009).

<sup>118</sup>Eliasta Ketaren., "Cyber Crime, Cyber Space, dan Cyber Law." *Jurnal Times*, 5, No.2, (Februari, 13, 2017), 35-40.

b) Kelalaian Pengguna Komputer

Hal ini merupakan salah satu penyebab utama *cyber crime*. Seperti orang-orang selalu memasukkan semua data-data penting ke dalam internet sehingga memberikan kemudahan bagi sebagian oknum untuk melakukan kejahatan.

c) Mudah dilakukan dengan Resiko Keamanan yang Kecil dan Tidak di Perlukan Peralatan yang Super Modern.

Internet merupakan sebuah alat yang dengan mudahnya kita gunakan tanpa memerlukan alat khusus dalam menggunakannya. Namun, pendorong utama tindak kejahatan di internet atau *cyber crime* yaitu susahnya melacak orang yang menyalahgunakan fasilitas dari internet tersebut.<sup>119</sup>

d) Para pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu besar, dan fanatik akan teknologi komputer.

Pengetahuan para pelaku kejahatan komputer tentang cara kerja sebuah komputer jauh diatas operator kompuer. Hal ini merupakan faktor yang sulit untuk dihindari karena kelebihan atau kecerdasan dalam mengakses internet yang dimiliki seseorang di zaman sekarang ini banyak yang disalahgunakan demi mendapat keuntungan semata.

e) Kurangnya Perhatian Masyarakat dan Penegak Hukum.

Masyarakat dan penegak hukum saat ini masih memberi perhatian yang sangat besar terhadap kejahatan konvensional. Pada kenyataannya, para pelaku *cyber crime* masih tetap melakukan aksi kejahatannya. Hal ini disebabkan karena

---

<sup>119</sup> Eliasta Ketaren., "Cyber Crime, Cyber Space, dan Cyber Law." *Jurnal Times*, 5, No.2, (Februari, 13, 2017), 38.

rendahnya faktor pengetahuan tentang penggunaan internet yang lebih dalam pada masyarakat.

f) Sistem Keamanan Jaringan Yang Lemah.

Penggunaan fasilitas internet kebanyakan lebih mementingkan desain yang dimilikinya dan menyepelkan tingkat keamanannya. Sehingga dengan lemahnya sistem keamanan jaringan tersebut menjadi celah besar bagi sebagian oknum untuk melakukan tindak kejahatan.<sup>120</sup>

Kasus-kasus *cyber crime* yang merupakan perkembangan dari *computer crime* apabila dilakukan sebelumnya lahirnya Undang-Undang ITE, maka bagi pelakunya didakwa dengan menggunakan kriteria peraturan hukum pidana konvensional. Perbuatan pidana yang digunakan untuk menjerat pelakunya tersebut adalah penipuan, kecurangan, pencurian, perusakan, dan lain-lainnya yang pada pokoknya dilakukan secara langsung oleh pelaku. Jika dilakukan dengan memanfaatkan sarana komputer (internet) saat sekarang telah dapat diterapkan dengan pasal-pasal yang terdapat dalam Undang-Undang ITE tercantum dalam Bab 7 untuk “perbuatan yang dilarang” (pasal 27-37) dan dalam Bab 11 untuk “ketentuan pidana” (Pasal 45-52).<sup>121</sup>

Posisi *cyber crime* dalam Undang-Undang ITE menjadi terlihat jelas, karena Undang-Undang tersebut menjadi bagian integral dari rangkaian perundang-undangan yang mengaturnya. Sehingga *cyber crime* yang menjadi modus baru dalam kejahatan terhadap perkembangan teknologi informasi dapat

<sup>120</sup> Eliasta Ketaren., “Cyber Crime, Cyber Space, dan Cyber Law.” *Jurnal Times*, 5, No.2, (Februari, 13, 2017), 35-40.

<sup>121</sup> Niniek Suparni, *Cyber Space: Problematika dan Antisipasi Pengaturannya* (Cet.1; Jakarta: Sinar Grafika, 2009), 112-113.

ditanggulangi. Untuk itu, perundang-undangan di Indonesia yang berkaitan dengan *cyber crime* harus terkonstruksi dengan sempurna agar kejahatan-kejahatan baru dapat terakomodir di dalamnya.

## **B. Kendala dalam Penanganan Tindak Pidana *Cyber Crime* di Indonesia**

Meskipun di Indonesia telah terdapat aturan-aturan yang bisa menjerat para pelaku *cyber crime*, faktanya hal ini belum dijalankan secara maksimal hal ini masih bisa dijumpai adanya kendala-kendala dalam penanganan kasus *cyber crime*. Perangkat hukum yang ada saat ini oleh sebagian kalangan dianggap belum memadai. Pidana Penyalahgunaan Informasi dan Transaksi Elektronik. Dalam upaya penanganan *cyber crime* oleh aparat kepolisian terdapat beberapa kendala yang menghambat upaya penanganan *cyber crime* yaitu diantaranya penindakan kasus *cyber crime* sering mengalami hambatan terutama dalam penangkapan tersangka dan penyitaan barang bukti. Dalam penangkapan tersangka seringkali kita tidak dapat menentukan secara pasti siapa pelakunya karena mereka melakukannya cukup melalui komputer yang dapat dilakukan dimana saja tanpa ada yang mengetahuinya sehingga tidak ada saksi yang mengetahui secara langsung.<sup>122</sup>

Meskipun sudah ada beberapa pasal yang bisa menjerat pelaku *cyber crime* ke penjara masih dijumpai adanya kendala dalam penanganan *cyber crime* menurut Soerjono Soekanto yaitu diantaranya:

---

<sup>122</sup> Utin Indah Permata Sari, "Kebijakan Penegakan Hukum dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police di Indonesia." *Jurnal Hukum*, 2, No.1, (Oktober 2021), 112.

## 1. Faktor Hukum

Perangkat hukum yang ada di sebagian kalangan saat ini dianggap masih belum memadai. UU No. 19 Tahun 2016 atas perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, baru sebuah tameng bagi pengguna teknologi dan informatika dalam mencapai kepastian hukum. UU ITE sampai saat ini masih bersifat abstrak, para ahli memberikan pendapat mengenai pasal 27 ayat (3) UU ITE sebagai berikut: Menurut Rudi Rusdiah mengatakan yaitu: "bahwa pasal 27 ayat (3) UU ITE dapat menimbulkan ketidakpastian hukum karena pengertiannya terlalu umum, singkat dan tidak detail. Di lihat dari asas dan tujuan sebuah Undang-Undang seharusnya setiap pasal dan ayat harus pasti, jelas, serta harus detail materil dan substansinya untuk memberikan kepastian hukum. Sedangkan Menurut Ronny Wuisan, mengatakan yaitu: "bahwa dalam pasal 27 ayat (3) UU ITE tidak ditemukan istilah mendistribusikan sehingga akan menimbulkan multitafsir. Dalam rumusan pasal 27 menggunakan istilah mendistribusikan, mentransmisikan tidak dikutip secara konsisten. Sedangkan pasal 28 ayat (2) memakai kata menyebarkan, ini suatu hal yang membingungkan dan akan menimbulkan ambigulasi. Akibatnya menimbulkan multitafsir, ambiguitas dan akan menimbulkan ketidakpastian hukum. Sehingga menimbulkan kesulitan pembuktian, UU ITE merupakan pengembangan tindak pidana khususnya dari KUHP, yang dikaitkan dengan

perkembangan teknologi informasi sebagai alat atau instrumen dalam melakukan kejahatan.<sup>123</sup>

## 2. Faktor Penegak Hukum

Kemampuan Penyidikdi bidang IT masih sangat minim dan kurangnya pengawasan terhadap penggunaan internet menciptakan terjadinya kejahatan dunia maya. Kejahatan ini menggunakan akses intenet yang tidak hanya terjadi dalam suatu wilayah. Keterbatasan tenaga ahli dalam melakukan penyelidikan menjadi faktor yang mempengaruhi keberhasilan aparat kepolisian dalam memberantas kasus *cyber crime*, dengan jumlah tenaga ahli yang sangat minim menjadi batu hambatan dalam memberantas kasus kejahatan dunia maya yang tidak bisa diselesaikan dengan waktu yang efisien, sehingga hal tersebut dimanfaatkan oleh para pelaku dalam menjalankan aksinya dengan lebih leluasa.

Secara umum penyidik Polri masih sangat minim dalam penguasaan operasional komputer dan pemahaman terhadap *Hacking* komputer serta kemampuan melakukan penyidikan terhadap kasus dunia maya. Personil *cyber police* hanya memiliki beberapa anggota, yang mana hal tersebut tidak sepadan dengan laporan kasus yang masuk dalam catatan kepolisian tentang kejahatan dunia maya, keterbatasan jumlah personil sebetulnya bisa diatasi dengan cara melakukan kerjasama, baik oleh pihak kepolisian, atau oleh pihak universitas dan perguruan tinggi maupun kerja sama internasional dalam memberantas *cyber crime*. Hal ini diperlukan untuk membuat tenaga ahli dalam bidang teknologi informasi. Para toko publik juga berperan penting dalam memberikan masukan

---

<sup>123</sup>Arifah, D. A. "Kasus *Cyber Crime* di Indonesia" *Jurnal hukum* ,18. No.2, (September 2011), 1-11

kepada pemerintah dalam keamanan jaringan internet. Beberapa faktor yang sangat berpengaruh (determinan) adalah: Pertama, Kurangnya pengetahuan tentang komputer. Kedua, Pengetahuan teknis dan pengalaman para penyidik dalam menangani kasus-kasus *cyber crime* masih terbatas. Ketiga, Faktor sistem pembuktian yang menyulitkan para penyidik

### 3. Alat Bukti

Persoalan alat bukti yang dihadapi dalam penyidikan terhadap *cyber crime* antara lain berkaitan dengan karakteristik kejahatan *cyber crime* itu sendiri, yaitu : sasaran atau media *cyber crime* adalah data atau sistem komputer atau sistem internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelakunya, *cyber crime* seringkali dilakukan tanpa saksi, yang mana saksi korban seringkali berada jauh diluar negeri sehingga menyulitkan penyidik melakukan pemeriksaan saksi dan pemberkasan hasil penyidikan.<sup>124</sup> Pembuktian merupakan faktor yang sangat penting mengingat infrastruktur teknologi informasi belum sepenuhnya dapat terakomodir dalam sistem KUHP Indonesia, sehingga diharapkan ketentuan mengenai pemanfaatan teknologi informasi diatur secara tegas sehingga terdapat suatu kepastian.

Berbicara mengenai pembuktian secara elektronik, tidak terlepas dari alat elektronik itu sendiri, proses pembuktian secara elektronik sebagaimana telah dibahas pada bagian sebelumnya, merupakan pembuktian yang melibatkan berbagai hal terkait teknologi informasi seperti informasi atau dokumen elektronik dalam perkara *cyber crime* yang tetap didasarkan pada ketentuan pembuktian

---

<sup>124</sup>Dista Amalia Arifah, "Kasus Cyber Crime di Indonesia." *Jurnal Bisnis dan Ekonomi (JBE)*, 18, No.2,(September 2011),192-193,

sebagaimana diatur dalam Kitab Undang-Undang Hukum Acara Pidana Serta Peraturan Perundang-Undangan lainnya seperti Undang-Undang Nomor 19 Tahun 2019 Perubahan Atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Proses pembuktian secara elektronik, tentunya harus didukung oleh berbagai alat bukti secara elektronik pula, hal ini dapat dilihat dalam ketentuan tentang alat bukti yang sah dalam pasal 184 KUHAP yang menyebutkan alat bukti yang sah terdiri dari : (1) keterangan saksi; (2) keterangan ahli (3) surat; (4) petunjuk; (5) keterangan terdakwa. Proses pembuktian pada kasus *cyber crime* pada dasarnya tidak berbeda dengan pembuktian pada kasus pidana konvensional, tetapi dalam kasus *cyber crime* terdapat ada beberapa hal yang bersifat elektronik yang menjadi hal utama dalam pembuktian, antara lain adanya informasi elektronik atau dokumen elektronik. Ketentuan hukum mengenai pembuktian dalam kasus *cyber crime* telah diatur dalam Pasal 5 Ayat (1) dan Ayat (2) Undang-Undang Nomor 11 Tahun 2008, yang menyatakan bahwa informasi dan dokumen elektronik dianggap sebagai alat bukti yang sah dalam proses pembuktian kasus *cyber crime* dan alat bukti elektronik tersebut dianggap pula sebagai perluasan dari alat bukti yang berlaku dalam hukum acara pidana yang berlaku di Indonesia, dalam hal ini alat bukti yang terdapat dalam pasal 184 KUHAP. Alat bukti ini harus mampu membuktikan telah terjadi suatu perbuatan dan mengakibatkan adanya akibat dari perbuatan *cyber crime*.

a. Keterangan Saksi

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

b. Keterangan Ahli

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

c. Alat Bukti Surat

Surat merupakan alat bukti yang penting dalam proses penyelidikan dan penyidikan kasus *cyber crime*, surat menjadi alat bukti yang sah dengan di dukung oleh keterangan saksi.

d. Petunjuk

Pengumpulan data secara fisik dalam *cyber crime* akan sulit dipenuhi, lebih mudah mencari petunjuk yang mengindikasikan telah adanya suatu niat jahat berupa akses secara tidak sah antara lain dengan melihat dan mendengarkan keterangan saksi di pengadilan atau hasil *print out* data, atau juga dari keterangan terdakwa di pengadilan. Petunjuk yang diajukan dipersidangan adalah bukti elektronik(yang disertai keterangan ahli) maka petunjuk ini bersifat lebih kuat dan memberatkan terdakwa.

e. Keterangan Terdakwa

Pasal 187 ayat 1 KUHAP menentukan bahwa keterangan terdakwa adalah apa yang terdakwa lakukan, dalam kasus *cyber crime*, keterangan terdakwa yang dibutuhkan terutama mengenai cara pelaku melakukan perbuatannya, akibat yang ditimbulkan.

4. Faktor Sarana dan Fasilitas Pendukung

Kapasitas komputer forensik serta minimnya tenaga ahli dalam bidang informasi dan teknologi juga harus diimbangi dengan adanya sarana dan prasarana yang memadai dalam menunjang keamanan jaringan dan juga untuk memudahkan pelacakan pelaku *cyber crime* dapat diatasi dengan cepat. Untuk membuktikan jejak-jejak para *Hacker*, dan *cracker* dalam melakukan aksinya terutama yang berhubungan dengan program dan data-data komputer, sarana Polri belum memadai karena belum ada komputer forensik. Fasilitas ini diperlukan untuk mengungkap data-data digital serta merekam dan menyimpan bukti berupa *soft copy* (image, program, dsb). Dalam hal ini Polri masih belum mempunyai fasilitas

komputer forensik (*forensic computing*), yang memadai. Fasilitas *forensic computing* yang akan didirikan Polri diharapkan akan dapat melayani dua hal penting yaitu pengumpulan bukti (*evidence collection*), dan saksi ahli (*expert witness*).<sup>125</sup> Keterbatasan anggaran operasional yang kurang menjadi faktor signifikan dalam mengungkapkan kasus kejahatan siber, dengan keterbatasan anggaran berdampak langsung pada peralatan yang digunakan maupun minimnya biaya operasional pihak kepolisian untuk mendeteksi pelaku *cyber crime*.

Berdasarkan beberapa kendala yang telah disebutkan di atas penulis menyimpulkan bahwa Perangkat hukum yang ada di sebagian kalangan saat ini dianggap masih belum memadai, Kemampuan Penyidik di bidang IT masih sangat minim dan kurangnya pengawasan terhadap penggunaan internet menciptakan terjadinya kejahatan dunia maya, Secara umum penyidik Polri masih sangat minim dalam penguasaan operasional komputer dan pemahaman terhadap *Hacking* komputer serta kemampuan melakukan penyidikan terhadap kasus dunia maya. Personil *cyber police* hanya memiliki beberapa anggota, yang mana hal tersebut tidak sepadan dengan laporan kasus yang masuk dalam catatan kepolisian tentang kejahatan dunia maya, Persoalan alat bukti yang mana data atau sistem komputer atau sistem internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelakunya, sehingga hal tersebut menyulitkan penyidik melakukan pemeriksaan saksi dan pemberkasan hasil penyidikan. sarana dan fasilitas pendukung Polri belum memadai dan Keterbatasan anggaran operasional yang kurang menjadi faktor signifikan dalam mengungkapkan kasus kejahatan siber,

---

<sup>125</sup>Isnatul Liviani, "Kejahatan Teknologi Informasi (*Cyber Crime*) dan Penanggulangannya dalam Sistem Hukum Indonesia." *Jurnal Pemikiran dan Pembaharuan Hukum Islam*, 23, No.2, (Desember 2020), 422-423.

dengan keterbatasan anggaran berdampak langsung pada peralatan yang digunakan maupun minimnya biaya operasional pihak kepolisian untuk mendeteksi pelaku *cyber crime*.



## BAB IV

### PENANGANAN TINDAK PIDANA *CYBER CRIME* DI INDONESIA

#### A. Kebijakan Formulasi Hukum Pidana dalam Penanggulangan *Cyber Crime* di Indonesia

Menjawab tuntutan dan tantangan komunikasi global lewat internet, Undang-Undang yang diharapkan (*ius constituendum*) adalah perangkat hukum yang akomodatif terhadap perkembangan serta antisipatif terhadap permasalahan, termasuk dampak negatif penyalahgunaan internet dengan berbagai motif yang dapat menimbulkan korban hingga menimbulkan korban kerugian materi dan non materi. Penanggulangan terhadap tindak pidana teknologi informasi perlu diimbangi dengan pembenahan dan pembangunan sistem hukum pidana secara menyeluruh, yakni meliputi pembangunan kultur, struktur, dan substansi hukum pidana. Dalam hal ini kebijakan hukum pidana menduduki posisi yang strategis dalam pengembangan hukum pidana modern.

Barda Nawawi Arief menyatakan bahwa upaya melakukan pembaharuan hukum pidana pada hakikatnya termasuk bidang "*penal policy*" yang merupakan bagian yang terkait dengan "*law enforcement policy*" *criminal policy*, dan *social policy*. Berarti pembaharuan hukum pada hakikatnya:<sup>126</sup>

1. Merupakan bagian dari kebijakan (upaya rasional) untuk memperbaharui substansi hukum (*legal substansi*) dalam rangka lebih mengefektifkan penegak hukum;

---

<sup>126</sup> Barda Nawawi Afief, *Bunga Rampai Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, (Jakarta: Rajawali Pers, 2006), 28.

2. Merupakan bagian dari kebijakan (upaya rasional) untuk memberantas/menanggulangi kejahatan dalam rangka untuk perlindungan masyarakat;
3. Merupakan bagian dari kebijakan (upaya rasional) untuk mengatasi masalah sosial dan masalah kemanusiaan dalam rangka mencapai /menunjang tujuan nasional.

Bertolak dari kebijakan tersebut diatas, usaha dan kebijakan untuk membuat peraturan hukum pidana yang pada hakikatnya tidak dapat dilepaskan dari tujuan penanggulangan kejahatan. Dengan demikian penentuan kebijakan hukum pidana menanggulangi *cyber crime* harus dilakukan dengan pendekatan kebijakan dan didalam setiap kebijakan terkandung pula pertimbangan nilai. Oleh karena itu, pembaharuan hukum pidana dalam penanggulangan tindak pidana teknologi informasi harus pula berorientasi pada pendekatan nilai.<sup>127</sup>

a. Kebijakan Formulasi Tindak Pidana;

Hukum pidana merupakan salah satu sarana kebijakan kriminal untuk menanggulangi *cyber crime*. Dalam kebijakan hukum pidana, maka akan bersentuhan dengan persoalan kriminalisasi, baik itu perbuatan yang melawan hukum, pertanggungjawaban pidana, maupun saksi yang dijatuhkan berupa pidana, maupun tindakan.

b. Kebijakan kriminalisasi

Kriminalisasi harus memenuhi berbagai syarat antara lain bahwa perbuatan tersebut benar menampakkan korban, baik aktual maupun potensial,

---

<sup>127</sup>Barda Nawawi Afief, *Bunga Rampai Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, (Jakarta:Rajawali Pers,2006),31.

kemudian konsistensi penerapan asas *ultimum remedium*, dukungan public yang kuat, bersifat komprehensif dan tidak bersifat *ad-hoc*.<sup>128</sup>

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana). Jadi pada hakikatnya, kriminalisasi merupakan bagian dari kebijakan kriminal (*criminal policy*) dengan menggunakan sarana hukum pidana (penal), dan oleh karena itu termasuk bagian dari “kebijakan hukum pidana” (*penal policy*), khususnya kebijakan formulasinya.

#### c. Kebijakan *Cyber Crime* Melalui Pendekatan KUHP

Hukum pidana yaitu bagian dari keseluruhan hukum yang berlaku disuatu negara, yang mengadakan dasar-dasar dan peraturan untuk menentukan perbuatan-perbuatan yang tidak boleh dilakukan, menentukan kapan dan hal apa kepada mereka yang telah melanggar larangan-larangan ini dapat dikenakan atau dijatuhi pidana sebagaimana yang telah diancamkan, menentukan dengan cara bagaimana penanganan pidana itu dapat dilaksanakan apabila ada orang yang disangka telah melanggar tersebut.

Tindak pidana dapat juga dikatakan dengan perbuatan pidana yang memiliki definisi sebagai berikut: “perbuatan yang dilarang oleh suatu aturan hukum larangan mana disertai ancaman (*sanksi*) yang berupa pidana tertentu, bagi barang siapa melanggar larangan tersebut”. saat ini, Indonesia sudah memiliki Undang-Undang *cyber Law* yang mengatur mengenai *cyber crime*, rancangan Undang-Undang tersebut sudah ada sejak Tahun 2000 dan revisi terakhir dari

---

<sup>128</sup>Muladi, “Kebijakan Kriminal Terhadap *Cyber Crime*”, *Majalah Media Hukum*, 1 No.3, (23 Agustus 2003),27.

rancangan Undang-Undang tindak pidana di bidang Teknologi Informasi sejak tahun 2016 sudah dikirimkan ke Sekretariat Negara RI oleh Departemen Komunikasi dan Informasi serta dikirimkan ke DPR namun dikembalikan kembali ke Departemen Komunikasi dan Informasi untuk diperbaiki.

Kitab Undang-Undang Hukum Pidana (KUHP) merupakan hukum nasional adalah sumber hukum sekaligus payung hukum untuk menindak berbagai macam tindak pidana yang terjadi di Indonesia. Dalam kaitannya dengan masalah *cyber crime*, KUHP nasional pengaturannya dapat digolongkan menjadi dua, yaitu pengaturan secara umum/tidak langsung dan pengaturan secara khusus/langsung. Pengaturan secara langsung artinya mengatur secara eksplisit tindak pidana yang berhubungan dengan kejahatan *cyber crime*.<sup>129</sup>

Selain dari beberapa pasal dalam KUHP yang mengatur tentang tindak pidana *cyber crime* diatas, adapun beberapa langkah penting yang harus dilakukan dalam penanggulangan *cyber crime* yaitu: **Pertama**, melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut. **Kedua**, meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional. **Ketiga**, meningkatkan pemahaman serta keahlian aparaturnya mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cyber crime*. **Keempat**, meningkatkan kesadaran warga negara mengenai masalah *cyber crime* serta pentingnya pencegahan kejahatan tersebut terjadi. **Kelima** meningkatnya kerjasama antar negara, baik bilateral,

---

<sup>129</sup>Rahmanuddin Tomalili, *Hukum Pidana* ( Yogyakarta: Cv Budi Utama,2019),

regional maupun multilateral, dalam upaya penanganan *cyber crime* antara lain melalui perjanjian ekstradisi dan *mutual assistance treaties*.<sup>130</sup>

#### d. Kebijakan *Cyber Crime* Melalui Pendekatan UU ITE

Kejahatan merupakan entitas yang selalu melekat dengan dinamika perkembangan peradaban umat manusia. Kejahatan yang oleh Saparinah Sadli disebut sebagai perilaku menyimpang, selalu ada dan melekat pada setiap bentuk masyarakat; oleh karena itu, upaya penanggulangan kejahatan sesungguhnya merupakan usaha yang terus menerus dan terus berkesinambungan. Semakin majunya peradaban manusia, sebagai implikasi dari perkembangan ilmu pengetahuan dan teknologi, munculnya berbagai jenis kejahatan berdimensi baru, yang termasuk di dalamnya *cyber crime*. sejalan dengan itu diperlukan upaya penanggulangan untuk menjamin ketertiban dalam masyarakat. Dalam perspektif hukum, upaya ini direalisasikan dengan hukum pidana. Hukum pidana diharapkan mampu memenuhi ketertiban masyarakat.

Akan tetapi dalam menghadapi perkembangan masyarakat, hukum pidana tidak selamanya mampu menjawab terhadap dampak negatif yang timbul dari kejahatan. Hal ini dikarenakan teknologi yang membawa perubahan dalam masyarakat begitu pesat, sementara hukum pidana merupakan produk sejarah tertentu berjalan dengan logika sejarah yang menanginnya walaupun dalam batas tertentu mempunyai prediktabilitas atas perkembangan masyarakat.

Dua muatan besar yang diatur dalam UU ITE ialah mengenai pengaturan transaksi elektronik dan mengenai tindak pidana siber. Pada UU ITE dimuat

---

<sup>130</sup>Hermawan Sulistiyo, *Cyber Crime: Modus Operandi dan Penaggulangannya* (Cet 1:Yogyakarta: LaksBang Pressindo,2007),

tentang perbuatan yang dilarang pada pasal 27 sampai pasal 37. Konstruksi pasal-pasal tersebut mengatur secara lebih detail tentang pengembangan modus-modus kejahatan tradisional sebagaimana yang tercantum dalam Kitab Undang-Undang Hukum Pidana (KUHP).<sup>131</sup>

pasal 27 menjelaskan perkembangan modus kejahatan dan/atau pelanggaran dengan media komputer/internet (dalam bentuk informasi/dokumen elektronik). Hal tersebut sangatlah penting khususnya membantu para penegak hukum dalam memproses dan mengadili kasus-kasus yang telah menggunakan media informasi elektronik untuk memuluskan kejahatan/pelanggaran seperti kesusilaan, perjudian, pencemaran nama baik, dan tindakan pemerasan dan pengancaman.

Pasal 28 mengatur tentang perlindungan konsumen dan aspek SARA. Hal ini sangat beralasan mengingat banyak transaksi perdagangan yang dilakukan dengan menggunakan media komputer/internet di mana baik produsen maupun konsumen tidak pernah bertemu satu sama lainnya. Sehingga aspek kepercayaan (trust) memegang peranan penting dalam transaksi perdagangan.

Pasal 29 UU ITE yaitu pengaturan hukum mengenai adanya ancaman yang sering dilakukan dan/atau dialamatkan kepada seseorang dengan menggunakan media informasi/dokumen elektronik. Perkembangan produk elektronik sangatlah memudahkan bagi seseorang untuk memuluskan langka jahatnya dalam mencapai tujuan yang diinginkan.

---

<sup>131</sup>Hermawan Sulistiyo, *Cyber Crime: Modus Operandi dan Penaggulangannya* (Cet 1:Yogyakarta: LaksBang Pressindo,2007),125

Pasal 30 mengatur tentang tindak ilegal yang dilakukan seseorang (*criminal*) terhadap sistem elektronik orang lain dengan tujuan untuk memperoleh informasi/dokumen elektronik dan/atau upaya pembobolan, penerobosan, dan penjebolannya, yang melanggar dan melampaui sistem pengamanan yang dilarang. Beberapa kasus yang relevan dan telah terjadi dalam praktik dunia siber dapat dilihat pada kasus pembobolan kartu kredit, pembobolan situs KPU, penyerangan terhadap situs website sekretariat Kabinet RI, peretasan website BPJS Kesehatan dan masih banyak contoh kasus lainnya.

## **B. Penanganan Tindak Pidana *Cyber Crime* di Indonesia**

### **1. Penanganan dengan Upaya Non Hukum**

Segala upaya yang lebih bersifat preventif dan persuasif terhadap para pelaku, korban dan semua pihak yang berpotensi terkait dengan kejahatan dunia maya. Penanganan dengan upaya non hukum ini menurut Hoefnagels adalah pendekatan kejahatan tanpa menggunakan sarana pemidanaan, kebijakan penanganan kejahatan lewat jalur non hukum lebih bersifat tindakan pencegahan sebelum terjadinya kejahatan sebagaimana hakikat dari hukum sebagai *ultimum remedium*, dimana *ultimum remedium* ini adalah asas dalam hukum pidana yang mengatakan bahwa hukum pidana hendaklah dijadikan upaya terakhir penegakan hukum. Asas *ultimum remedium* ini bermakna apabila suatu perkara dapat diselesaikan melalui jalur lain (kekeluargaan, negosiasi, mediasi, perdata, atau hukum administrasi) hendaklah jalur lain tersebut terlebih dahulu dilakukan. Oleh karena itu, sasaran utamanya adalah menangani faktor-faktor kondusif penyebab terjadinya kejahatan yang berpusat pada masalah-masalah atau kondisi sosial yang

secara langsung atau tidak langsung dapat menimbulkan atau menumbuhkan suburkan kejahatan maka upaya non hukum ini mempunyai kedudukan yang strategis dan memegang peranan kunci yang harus diintensifkan dan diefektifkan.<sup>132</sup>

Beberapa masalah dan kondisi sosial yang dapat merupakan faktor kondusif penyebab timbulnya kejahatan, kebijakan yang dapat ditempuh dengan upaya non hukum ini yaitu dengan cara memperbaiki perekonomian nasional, melakukan pendidikan budi pekerti kepada setiap orang, baik secara formal maupun non formal, terutama kepada pihak yang rentan melakukan kejahatan, memperbaiki sistem kesehatan mental masyarakat, mengefektifkan kerjasama internasional dalam pemberantasan tindak pidana *cyber crime*, memperbaiki sistem pengamanan komputer, serta mengefektifkan hukum administrasi dan hukum pidana yang berhubungan dengan penyelenggaraan sistem dan jaringan komputer.

Hal ini senada dengan kesepakatan kejahatan dunia maya (*Convention on Cyber Crime*), bahwa kerjasama internasional yang perlu dilakukan dalam rangka penanggulangan kejahatan siber adalah perjanjian ekstradisi, pemberian informasi secara spontan, dan pembentukan jaringan yang dikelola oleh tenaga profesional dalam rangka menjamin terselenggaranya bantuan secepatnya untuk investigasi dan peradilan untuk mengumpulkan alat bukti elektronik. Bantuan-bantuan tersebut berupa fasilitas atau bantuan lain, dengan syarat dan izin oleh hukum nasional masing-masing negara.

---

<sup>132</sup>Eliasta Ketaren., "Cyber Crime, Cyber Space, dan Cyber Law." *Jurnal Times*, 5, No.2, (Februari, 13, 2017),42.

Sebagai salah satu bentuk dari kejahatan berteknologi tinggi (*hi-tech crime*) adapun upaya pencegahan yang bisa ditempuh yaitu melalui pendekatan teknologi, pendekatan budaya, /cultural, pendekatan edukatif/moral/moral religius, hingga pendekatan global seperti kerja sama internasional.<sup>133</sup>

a. Pendekatan Teknologi

Tindak pidana *cyber crime* yaitu kejahatan yang dilakukan di lingkungan elektronik. Oleh karena itu penanganannya memerlukan keahlian khusus, prosedur investigasi dan kekuatan dasar hukum yang mungkin saat ini masih minim tersedia di Indonesia. Upaya untuk meningkatkan penanganan tersebut diantaranya melalui pendekatan teknologi, dengan cara meningkatkan kemampuan dan pengetahuan di bidang teknologi khususnya sistem komputer. Peningkatan kemampuan ini dikhususkan melalui upaya pelatihan (*training*) bagi aparat penegak hukum, dikarenakan *cyber crime* merupakan kejahatan berteknologi canggih dan melalui dunia maya/ tidak nyata sehingga membutuhkan pembuktian yang tidak mudah. Upaya lain dengan peningkatan pengamanan bagi situs tertentu dengan cara memblok atau mengunci serta memverifikasi data pengguna internet sehingga tidak dapat diakses oleh pengguna internet yang ingin membuka situs web tersebut.

b. Pendekatan budaya/kultural

Upaya preventif dengan pendekatan budaya/cultural pada dasarnya merupakan penanggulangan dengan cara mengetahui dan mematuhi etika dalam penggunaan internet, sehingga dapat menghindari penyalahgunaan dan dampak

---

<sup>133</sup>Barda Nawawi Arief. *Pornografi, Pornoaksi dan Cybersex/Cyberporn*. (Semarang: Pustaka Magister,2007),41.

negatifnya. Pendekatan ini merupakan salah satu kebijakan non penal dalam Resolusi Kongres PBB VII/1990 mengenai kejahatan terkait komputer (*Computer Relatedcrimes*), yang menyatakan perlunya membangun/membangkitkan kepekaan masyarakat dan aparat penegak hukum terhadap masalah *cyber crime* dan menyebarluaskan/mengajarkan etika penggunaan komputer melalui media pendidikan;<sup>134</sup> 1) setiap orang harus bertanggung jawab terhadap perilaku sosial dan hukum dalam menggunakan internet; 2) tidak seharusnya ikut serta dalam berbagai bentuk siber yang mengganggu.

c. Pendekatan Edukasi/Moral/Religius

Pendidikan merupakan kunci utama dari perilaku manusia, khususnya pendidikan dalam keluarga. Mengingat tindak pidana *cyber crime* ini korbannya tidak memandang umur dikarenakan kemajuan zaman membuat anak kecil pun mampu menggunakan alat elektronik seperti Hp, komputer. Oleh karenanya diharapkan peranan guru dan khususnya orang tua untuk turut serta membantu pencegahan *cyber crime* ini. Dengan meningkatkan pendidikan moral, akhlak khususnya agama sejak usia dini diharapkan mampu menjadi salah satu upaya pencegahan bagi seseorang untuk melakukan perbuatan menyimpang atau melawan hukum.

---

<sup>134</sup>Damianusbi, "Peran Pemerintah dan Masyarakat" 05 mei 2016 , <http://damianusbi.blogspot.co.id/2016/05/peran-pemerintah--dan-masyarakat.html>, diakses 19 juni 2023, pukul 13:00 WIB.

#### d. Pendekatan Global

Pendekatan global ini dilakukan melalui kerjasama internasional. Mengingat kejahatan ini melampaui batas-batas negara.<sup>135</sup> Selama ini upaya penyidikan dan pencegahan hukum terhadap kejahatan *cyber* dibatasi dalam wilayah *teritorial* negara. Upaya lain yang dilakukan adalah peningkatan efektifitas dan perubahan terhadap penegakan hukum pidana, khususnya mengefektifkan hukum positif. Beberapa langkah yang dapat ditempuh antara lain.<sup>136</sup> Meningkatkan komitmen strategi/prioritas nasional dalam penanggulangan kejahatan dunia maya.

Upaya menangani tindak pidana *cyber crime*, resolusi kongres PBB VIII/1990 mengenai *computer related crimes* mengajukan beberapa kebijakan antara lain:<sup>137</sup>

- 1) Menghimbau negara-negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer, lebih efektif dengan mempertimbangkan langkah-langkah berikut:
  - a. Melakukan modernisasi hukum pidana materil dan hukum acara pidana.
  - b. Mengembangkan tindakan-tindakan pencegah dan pengamanan komputer.
  - c. Melakukan langkah-langkah untuk membuat peka warga masyarakat, aparat penegak hukum, dan pengadilan, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer.

<sup>135</sup>Barda Nawawi Arief. *Pornografi, Pornoaksi dan Cybersex/Cyberporn*. (Semarang: Pustaka Magister,2007),

<sup>136</sup>Barda Nawawi Arief. *Pornografi, Pornoaksi dan Cybersex/Cyberporn*. (Semarang: Pustaka Magister,2007),

<sup>137</sup>Agus Raharjo, *Cyber Crime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* (Bandung: Citra Aditya Bakti,2002),57.

- d. Melakukan upaya-upaya pelatihan bagi para hakim, penegak hukum, dan pejabat, mengenai kejahatan di bidang ekonomi dan *cyber crime*.
  - e. Memperluas aturan etika (*rules of ethics*) dalam menggunakan komputer, dan mengajarkannya melalui kurikulum informatika.
  - f. Mengadopsi kebijakan perlindungan korban sesuai deklarasi PBB mengenai korban dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya kejahatan siber.
- 2) Menghimbau agar negara-negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan tindak pidana *cyber crime*.
  - 3) Merekomendasikan kepada komite pengadilan dan pencegahan PBB untuk:
    - a) Menyebarkanluaskan pedoman dan standar untuk membantu negara anggota menghadapi *cyber crime* di tingkat nasional, regional, maupun internasional.
    - b) Mengembangkan penelitian dan analisis lebih lanjut guna menemukan cara-cara baru menghadapi permasalahan *cyber crime* dimasa mendatang.
    - c) Mempertimbangkan *cyber crime* sewaktu meninjau pengimplementasian perjanjian ekstradisi, dan bantuan kerjasama di bidang penanggulangan kejahatan.<sup>138</sup>

Solusi terhadap permasalahan yang diangkat para pengguna teknologi informasi dan komunikasi sebaiknya berhati-hati dalam melakukan komunikasi dengan orang yang tidak dikenal dan jangan mudah mempercayai orang atau lembaga yang baru dikenal lewat internet. Perlu adanya tindakan hukum yang

---

<sup>138</sup>Agus Raharjo, *Cyber Crime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* (Bandung: Citra Aditya Bakti,2002),57

tegas dari aparat penegak hukum agar dapat menimbulkan efek jera kepada pelaku tindakan *cyber crime*, perlu hukum yang secara khusus yang dapat mengatur seperti misalnya berkaitan dengan jenis-jenis alat bukti yang sah dalam kasus *cyber crime*, pemberian wewenang secara khusus kepada penyidik dalam melakukan beberapa tindakan yang diperlukan dalam rangka penyidikan kasus *cyber crime*, dan lain-lain. *Cyber crime* adalah masalah dalam dunia internet yang harus ditangani secara serius. Sebagai kejahatan, penanganan terhadap *cyber crime* dapat dianalogikan sama dengan dunia nyata, harus dengan hukum legal yang mengatur.

## 2. Penanganan dengan Upaya Hukum (*Cyberlaw*)

Penegakan hukum adalah suatu proses untuk mewujudkan keinginan hukum menjadi kenyataan. Keinginan hukum inilah yang nantinya akan menjadi pikiran badan pembuat Undang-Undang yang dirumuskan dalam peraturan-peraturan khusus. Perumusan pikiran pembuat hukum dituangkan dalam peraturan hukum yang nantinya menentukan bagaimana penegakan hukum itu dijalankan. pada kenyataannya proses penegakan hukum memuncak pada pelaksanaannya oleh para pejabat penegak hukum.<sup>139</sup> Aparat penegak hukum di Indonesia adalah hakim, jaksa, polisi. Hakim merupakan salah satu aparat hukum yang melaksanakan suatu sistem peradilan yang mempunyai tugas untuk menerima dan memutuskan perkara dengan seadil-adilnya. Dalam rangka penegakan hukum di Indonesia tugas hakim yaitu menegakkan hukum dan keadilan melalui berbagai perkara yang di hadapkan kepadanya. Jaksa adalah aparat penegak hukum yang

---

<sup>139</sup> Satjipto Raharjo, *Penegakan Hukum Suatu Tinjauan Sosiologi*, (Yogyakarta:Genta Publishing,2009).

merupakan pejabat fungsional yang diberikan kewenangan oleh Undang-Undang dalam pelaksanaan putusan pengadilan. Dan yang terakhir polisi, polisi sebagai penegak hukum yang selalu dituntut untuk melaksanakan profesinya dengan adil dan bijaksana, serta mendatangkan keamanan dan ketentraman dalam menjalankan tugas.

Lawrence M. Friedman<sup>140</sup> mengemukakan bahwa efektif dan berhasil tidaknya penegakan hukum tergantung tiga unsur sistem hukum, yakni struktur hukum (*legal structure*) substansi hukum (*legal substance*) dan budaya hukum (*legal culture*). Struktur hukum menyangkut aparat penegak hukum, substansi hukum menyangkut perangkat Perundang-Undangan dan budaya hukum yang mana merupakan hukum yang hidup (*living law*) yang dianut dalam suatu masyarakat.

### 1. Substansi Hukum

Substansi hukum dalam Teori Lawrence M. Friedman yaitu hal yang disebut sebagai sistem substansial yang menentukan bisa atau tidaknya hukum itu dilaksanakan. Substansi mencakup hukum yang hidup bukan, bukan hanya aturan yang ada dalam Kitab Undang-Undang. Substansi juga berarti produk yang dihasilkan oleh orang yang berada dalam sistem hukum mencakup keputusan yang mereka keluarkan dan aturan baru yang mereka susun. Aspek lain dari sistem hukum adalah substansinya. Yang dimaksud dengan substansinya adalah aturan, norma, dan pola perilaku nyata manusia yang berada dalam sistem itu.

---

<sup>140</sup>Lawrence M. Friedman, *Sistem Hukum Perspektif Ilmu Sosial*, (Bandung: Nusa Media,2011)

Substansi hukum menyangkut Peraturan Perundang-Undangan yang berlaku yang memiliki kekuatan hukum yang mengikat dan menjadi pedoman bagi aparat penegak hukum. Adapun yang harus dibenahi dalam hal masalah aturan yang berkaitan dengan masalah teknologi secara global mengenai *computer related crimes* dengan beberapa kebijakan yaitu melakukan modernisasi hukum pidana, baik itu pidana materil dan hukum acara pidana. Selain hal tersebut diatas yang juga diperlukan adalah melakukan kriminalisasi, dimana kebijakan ini menetapkan suatu perbuatan yang semula bukan tindak pidana menjadi suatu tindak pidana dimana harus ada harmonisasi ketentuan yang berhubungan dengan kriminalisasi, pembuktian, dan prosedur, jadi masalahnya bukan sekedar persoalan kebijakan hukum pidana. Terkait dengan masalah ini harus ada harmonisasi peraturan yang mengatur masalah *cyber crime*, sehingga dalam hal penanganannya bisa lebih efektif karena tindak pidana ITE atau *cyber crime* ini dapat dilakukan lintas daerah tanpa ada sekat-sekat, olehnya itu dalam penanganannya juga harus melibatkan beberapa negara.

## 2. Struktur Hukum

Lawrence M.Friedman dalam teorinya disebutkan bahwa hal ini disebut sebagai suatu sistem struktural yang menentukan bisa atau tidaknya hukum itu dilaksanakan dengan baik. Struktur hukum berkaitan dengan sistem peradilan yang berhubungan langsung dengan sumber daya manusia bidang hukum yang terdiri dari hakim, jaksa, polisi, pengacara, pejabat lembaga pemasyarakatan termasuk susunan kelembagaan dan yurisdiksinya<sup>141</sup> Kewenangan lembaga

---

<sup>141</sup>Achmad Ali, *Menguak Teori Hukum dan Teori Peradilan*, (Jakarta:Prenada Media Grup,2010)

penegak hukum dijamin oleh undang-undang, sehingga dalam pelaksanaan tugas dan tanggung jawabnya terlepas dari pengaruh kekuasaan pemerintah dan pengaruh lainnya. Seberapa baiknya suatu peraturan perundang-undangan bila tidak didukung oleh aparat penegak hukum yang baik maka keadilan hanya angan-angan.

Struktur dari sistem hukum terdiri atas unsur berikut ini, jumlah dan ukuran pengadilan, yurisdiksinya (termasuk jenis kasus yang berwenang mereka periksa), dan tata cara baik banding dari pengadilan ke pengadilan lainnya, struktur juga yaitu berarti bagaimana badan legislatif ditata, apa yang boleh dan tidak boleh dilakukan oleh presiden, prosedur apa yang diikuti oleh kepolisian dan sebagainya. Jadi struktur terdiri dari lembaga hukum yang ada dimaksudkan untuk menjalankan perangkat hukum yang ada<sup>142</sup>.

Penanganan yang bisa dilakukan dalam struktur hukum ini yaitu melakukan upaya-upaya seperti mengembangkan tindakan pencegahan dan pengamanan komputer, melakukan langkah-langkah untuk membuat peka masyarakat, aparat pengadilan dan penegak hukum terhadap pentingnya pencegahan kejahatan yang berkaitan dengan dunia maya, melakukan upaya-upaya pelatihan bagi para hakim, pejabat dan aparat penegak hukum mengenai kejahatan *cyber crime*, mengadopsi kebijakan perlindungan korban *cyber crime* agar mengambil langkah-langkah untuk mendorong korban untuk melaporkan adanya *cyber crime*, meningkatkan kegiatan-kegiatan internasional

---

<sup>142</sup>Lawrence M. Friedman, *Sistem Hukum Perspektif Ilmu Sosial*, (Bandung: Nusa Media, 2011)

dalam upaya penanggulangan *cyber crime*<sup>143</sup>. hal lain yang berkaitan dengan struktur adalah peningkatan kapasitas aparat penegak hukum berkaitan dengan masalah *cyber crime* atau tindak pidana di dunia maya, dalam hal ini bisa dilakukan dengan pemanfaatan para *hacker* untuk tindakan-tindakan positif seperti pencegahan tindak pidana dunia maya atau tujuan lain seperti mengumpulkan bukti-bukti terkait masalah tindak pidana dunia maya. Dan yang paling terpenting tentunya adalah peran pemerintah untuk mencegah terjadinya tindak pidana dunia maya.

### 3. Culture /Budaya Hukum

Budaya hukum diibaratkan sebagai sistem atau unsur sikap dan nilai sosial. Jadi budaya hukum berkaitan dengan sikap budaya masyarakat pada umumnya, karena menyentuh keyakinan, nilai, cita, dan harapan, sehingga dapat dikatakan, kesadaran hukum masyarakat merupakan salah satu pencerminan budaya hukum mereka<sup>144</sup>. Pengertian budaya yang lain menurut Roem Topatisomang budaya hukum meliputi persepsi, pemahaman, sikap penerimaan, praktik-praktik dan penafsiran terhadap isi dan tata laksana hukum<sup>145</sup>.

Penanganan yang bisa dilakukan melalui budaya hukum ini yaitu mengedepankan etika dan moral, dimana moral juga disini diartikan dengan nilai baik dan buruk<sup>146</sup>, dimana disebutkan bahwa konsep moral dan etika sangat penting dijadikan pedoman dan pegangan untuk menjadi pengontrol bagi diri

---

<sup>143</sup> Barda Nawawi Arief, *Tindak Pidana Mayantara*, (Jakarta: Raja Grafindo Persada, 2006),

<sup>144</sup> Barda Nawawi Arief, *Tindak Pidana Mayantara*, (Jakarta: Raja Grafindo Persada, 2006),

<sup>145</sup> Rusdin Tompo, *Ayo Lawan Korupsi* (Makassar: LBH-P2, 2005)

<sup>146</sup> Sudjito, *Hukum dalam Pelangi Kehidupan*, (Yogyakarta: Gadjah Mada University Press, 2012).

untuk tidak melakukan tindakan yang tidak bermoral dan tidak etis, karena tindakan ini dapat dilakukan dimana pun, tanpa mengenal batas dan waktu, hal ini lebih diprioritaskan pada pelaku *cyber crime*.

Kultur hukum menurut Lawrence M. Friedman<sup>147</sup> adalah sikap manusia terhadap hukum dan sistem hukum kepercayaan, nilai, pemikiran, serta harapannya. Budaya kultur erat kaitannya dengan kesadaran hukum masyarakat, semakin tinggi kesadaran hukum masyarakat maka akan tercipta budaya hukum yang baik dan dapat merubah pola pikir masyarakat mengenai hukum selama ini. Secara sederhana tingkat kepatuhan masyarakat terhadap hukum merupakan salah satu indikator berfungsinya hukum. Kultur hukum adalah suasana pemikiran sosial dan kekuatan sosial yang menentukan bagaimana hukum itu digunakan, dihindari atau disalahgunakan.

Senada dan sependapat dengan Lawrence M. Friedman, Sajipto Rahardjo<sup>148</sup> menyebutkan bahwa jika berbicara soal hukum pada dasarnya tidak dapat dipisahkan dari asas-asas paradigma hukum yang terdiri atas fundamental hukum dan sistem hukum. Beberapa fundamental hukum diantaranya legislasi, penegakan dan peradilan sedangkan sistem hukum meliputi substansi, struktur dan kultur hukum. Kesemuanya itu sangat berpengaruh terhadap efektivitas kinerja sebuah hukum. Dari beberapa definisi tersebut, dapat kita artikan bahwa berfungsinya sebuah hukum merupakan pertanda bahwa hukum tersebut telah mencapai tujuan hukum, yaitu berusaha untuk mempertahankan dan melindungi

---

<sup>147</sup>Lawrence M. Friedman, *Sistem Hukum Perspektif Ilmu Sosial*, (Bandung: Nusa Media, 2011)

<sup>148</sup>M. Friedman Sajipto Rahardjo Dikutip Sambas, Leonarda, *Teori-Teori Hukum Klasik dan Kontemporer* ( Jakarta: Ghalia Indonesia, 2016).

masyarakat dalam pergaulan hidup. Tingkat efektivitas hukum juga ditentukan oleh seberapa tinggi tingkat kepatuhan warga masyarakat terhadap aturan hukum yang telah dibuat.

Adapun kesimpulan yang penulis tarik dari beberapa teori Lawrence Meir.Friedman diatas yaitu, langkah yang ditempuh dalam penanggulangan *cyber crime* adalah fokus pada substansi yaitu masalah peraturan yakni Terkait dengan masalah ini harus ada harmonisasi peraturan yang mengatur masalah *cyber crime*. Penanganan yang bisa dilakukan dalam struktur hukum ini yaitu melakukan upaya-upaya seperti mengembangkan tindakan pencegahan dan pengamanan komputer, melakukan langkah-langkah untuk membuat peka masyarakat, aparat pengadilan dan penegak hukum terhadap pentingnya pencegahan kejahatan yang berkaitan dengan dunia maya, melakukan upaya-upaya pelatihan bagi para hakim, pejabat dan aparat penegak hukum mengenai kejahatan *cyber crime*. Dan penanganan yang bisa dilakukan melalui budaya hukum yaitu Penanganan yang bisa dilakukan melalui budaya hukum ini yaitu mengedepankan etika dan moral, dimana moral juga disini diartikan dengan nilai baik dan buruk, dimana disebutkan bahwa konsep moral dan etika sangat penting dijadikan pedoman dan pegangan untuk menjadi pengontrol bagi diri untuk tidak melakukan tindakan yang tidak bermoral dan tidak etis seperti halnya kejahatan yang dapat merugikan banyak orang seperti kejahatan dunia maya.

Salah satu kebijakan dalam penanganan kejahatan dengan menggunakan hukum pidana. Kebijakan tersebut dioperasikan dengan cara menerapkan hukum pidana, yaitu pidana materil, hukum formil dalam masyarakat. Dalam kongres

PBB ke 4 yang berlangsung di Tokyo, disepakati bahwa usaha pencegahan kejahatan termasuk penerapan hukum pidana merupakan bagian integral dari rencana pembangunan nasional. Kebijakan hukum pidana pada hakikatnya merupakan usaha untuk mewujudkan Peraturan Perundang-Undangan pidana agar sesuai dengan keadaan pada waktu tertentu (*ius constitutum*) dan masa yang akan datang (*ius constituendum*).<sup>149</sup> Dalam penanganan kasus *cyber crime* di Indonesia, terdapat beberapa upaya hukum yang dilakukan. Berikut adalah beberapa langkah yang dilakukan oleh pemerintah dan penegak hukum untuk mengatasi kasus *cyber crime* di Indonesia :

a. Kebijakan Regulasi Hukum

Pemerintah memiliki kebijakan regulasi hukum pidana terhadap tindak pidana teknologi informasi dalam mengganggu *cyber crime*. peraturan perundang-undangan menjadi landasan dalam penanganan *cyber crime* baik dari segi materil maupun formil. Teknologi informasi sekarang ini sangat strategis dan berdampak luas terhadap aktivitas kehidupan manusia oleh karena itu dibutuhkan pengaturan secara khusus dengan dibentuknya suatu Undang-Undang yang dapat menanggulangi kejahatan terhadap teknologi informasi.

Peraturan terhadap teknologi informasi agar diterima masyarakat harus mempertimbangkan semua aspirasi dan berbagai kepentingan harus diselaraskan dan diserasikan. Kebijakan hukum pidana sangat dipengaruhi oleh sistem hukum yang berlaku saat ini. Hukum pidana indonesia yang ada saat ini dan pengembangan ke depan dipengaruhi oleh tradisi hukum *civil law*. Pembentukan

---

<sup>149</sup>Lilik Mulyadi, *Bunga Rampai Hukum Pidana Prespektif, Teoritis dan Praktik*, (Bandung: PT. Alumni, 2008),390

Peraturan Perundang-Undangan di dunia siber pun, berpangkal pada keinginan masyarakat untuk mendapatkan jaminan keamanan, keadilan dan kepastian hukum. Sebagai norma hukum siber atau *cyber law* akan bersifat mengikat bagi tiap-tiap individu untuk tunduk dan mengikuti segala kaidah-kaidah yang terkandung di dalamnya.

Terdapat dua perlindungan hukum, yaitu perlindungan hukum preventif dimaksudkan sebagai pengaturan tindak pidana dibidang transaksi elektronik diatur dalam hukum positif yaitu hukum yang dipakai di Indonesia, dalam hal ini tindak pidana TI diatur dalam UU ITE yang bersifat khusus atau *lex specialis*. Sebagaimana hal tersebut, maka kebijakan hukum terkait ketentuan pidana tindak pidana dibidang transaksi elektronik tertuang dalam “*pasal 45 hingga pasal 52 UU ITE juncto pasal 27 hingga pasal 37 UU ITE terkait perbuatan yang dilarang*”. Selain itu penyuluhan dan konsultasi hukum dalam kegiatan pengabdian masyarakat ini merupakan salah satu cara untuk meningkatkan pengetahuan masyarakat.<sup>150</sup>

*Cyber crime* tidak dapat hanya di kualifikasikan dengan tindak pidana konvensional, hal ini mengingatkan dampak nyata yang ditimbulkan, yang mana apabila hanya dilakukan pendekatan kejahatan konvensional saja maka akan banyak bentuk tindakan atau perbuatan yang tidak terakomodir oleh hukum. Oleh karena itu agar pemanfaatan teknologi informasi dapat berkembang dengan optimal dan maksimal maka harus diimbangi dengan perlindungan dan penegakan hukum yang optimal, penegakan hukum disini tidak hanya memperhatikan

---

<sup>150</sup>Barda Nawawi Arief, *Tindak Pidana Mayantara*, (Jakarta: Raja Grafindo Persada, 2006),

pendekatan kepastian hukum melainkan juga harus memperhatikan pendekatan keadilan dan pemanfaatan hukum sebagaimana tujuan hukum itu sendiri.<sup>151</sup> *cyber crime* merupakan suatu kejahatan dengan memanfaatkan sarana teknologi informasi dengan memanfaatkan cela keamanan serta ketidakhati-hatian korban, *cyber crime* diatur dalam UU ITE.

## 1. KUHP

Menangani kasus yang terjadi para penyidik melakukan analogi atau perumpamaan dan persamaan terhadap pasal-pasal yang ada dalam KUHP. Pasal-pasal di dalam KUHP biasanya digunakan lebih dari satu pasal karena melibatkan beberapa perbuatan sekaligus pasal-pasal yang dapat dikenakan dalam KUHP pada *cyber crime* antara lain:<sup>152</sup>

- 1) Pasal 332 KUHP dapat dikenakan untuk penipuan
- 2) Pasal 333 KUHP dapat dikenakan pada kasus *deface* atau *hacking* serta data *interference* (mengganggu data komputer) dan *system interference* (mengganggu sistem komputer), yang membuat sistem milik orang lain.
- 3) Pasal 334 KUHP yang dikenakan untuk kasus *carding*.
- 4) Pasal 407 KUHP (kejahatan pornografi) dapat dikenakan untuk penyebaran pornografi maupun website porno yang banyak beredar dan mudah diakses di internet.
- 5) Pasal 426 dan 427 KUHP (perjudian) dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di internet.

<sup>151</sup> Renny Ns Koloay, "Perkembangan Hukum Indonesia Berkenaan dengan Teknologi Informasi dan Komunikasi" *Jurnal Hukum Unsrat*, 22 No. 5, (12 Januari 2016).

<sup>152</sup> Yurizal, *Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia*, (Malang: Media Nusa Creative, 2018), 41

- 6) Pasal 433 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media internet.
  - 7) Pasal 482 dan 483 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui e-mail yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan.
2. Undang-Undang No. 19 Tahun 2016 atas Perubahan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Menghadapi *cyber crime*, hukum positif di Indonesia masih bersifat *lex locus delicti*. Namun beda halnya dengan situasi dan kondisi pelanggaran hukum yang terjadi atas *cyber crime* dimana pelaku kejahatan *cyber* dan korban berada di tempat yang berbeda. Wilayah kejahatan didunia maya yang begitu luas namun mudah diakses menyebabkan maraknya terjadi kejahatan. Kepolisian Republik Indonesia (POLRI) sebagai salah satu alat kelengkapan negara dalam menegakkan hukum tidak dapat lagi tinggal diam setelah lahirnya Undang-Undang No.19 Tahun 2016 perubahan Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Aparat penegak hukum dalam hal ini menyelidiki kepolisian harus bergerak secara aktif untuk menindak kejahatan didunia maya. Aparat kepolisian harus dapat menangani kasus-kasus kejahatan yang terjadi di dunia maya.<sup>153</sup> Undang-Undang Nomor 19 Tahun 2016 Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

---

<sup>153</sup>M.Ramli, Ahmad. *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*, (Bandung: PT. Refika Aditama. 2006),98.

1. Tindak pidana yang berhubungan dengan aktivitas illegal, yaitu:
  - a. Distribusi atau penyebaran, transmisi, dapat diaksesnya konten illegal, yang terdiri dari
    - Kesusilaan (pasal 27 ayat (1) UU ITE)
    - Perjudian (pasal 27 ayat (2) UU ITE)
    - Penghinaan dan/atau pencemaran nama baik (pasal 27 ayat (3) UU ITE)
    - Pemerasan dan/atau pengancaman (pasal 27 ayat (4) UU ITE)
    - Berita bohong yang menyesatkan dan merugikan konsumen (pasal 28 ayat (1) UU ITE);
    - Menimbulkan rasa kebencian berdasarkan SARA (Pasal 28 ayat (2) UU ITE);
    - Mengirimkan informasi yang berisi ancaman kekerasan atau menakutkan yang ditujukan secara pribadi (pasal 29 UU ITE);
  - b. Dengan cara apapun melakukan akses ilegal (pasal 30 UU ITE)
  - c. Intersepsi atau penyadapan illegal terhadap informasi atau dokumen elektronik dan sistem elektronik (pasal 31 UU 19/2016);

Tindak pidana yang berhubungan dengan gangguan yaitu: gangguan terhadap informasi atau dokumen elektronik (pasal 32 UU ITE), gangguan terhadap sistem elektronik (pasal 33 UU ITE).

## **BAB V**

### **PENUTUP**

#### **A. Kesimpulan**

Sesuai dengan pembahasan penulis dari bab-bab sebelumnya terkait tinjauan yuridis tindak pidana *cyber crime* di Indonesia, maka dapat ditarik kesimpulan sebagai berikut:

1. Ketentuan Tindak pidana *cyber crime* di Indonesia memiliki beberapa aturan hukum yang berlaku dan dapat dikenakan bagi para pelaku *cyber crime* terutama untuk kasus yang menggunakan komputer sebagai sarannya seperti yang terdapat dalam pasal 332, 333, 334, 407, 426, 433, 483KUHP, Undang-Undang No 19 tahun 2016 perubahan atas Undang-Undang No. 8 tahun 2011 tentang Informasi dan Transaksi Elektronik, Undang-Undang No.28 Tahun 2014 tentang Hak Cipta, Undang-Undang No. 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme, Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi, dan Undang-Undang No. 27 tahun 2022 tentang Perlindungan Data Pribadi.

2. Kendala yang dihadapi yaitu perangkat hukum yang ada di sebagian kalangan saat ini dianggap masih belum memadai, pengetahuan teknis, kemampuan dan pengalaman para penyidik di bidang IT dalam menangani kasus-kasus *cyber crime* serta kemampuan teknis yang dibutuhkan dalam melakukan pelacakan terhadap pelaku *cyber crime* masih sangat minim, faktor sistem pembuktian yang menyulitkan para penyidik, sarana fasilitas komputer forensik yang dibutuhkan oleh penyidik masih belum memadai, serta keterbatasan

anggaran operasional yang kurang menjadi faktor signifikan dalam mengungkap kasus kejahatan siber, dengan keterbatasan anggaran berdampak langsung pada peralatan yang digunakan maupun minimnya biaya operasional pihak kepolisian untuk mendeteksi pelaku *cyber crime*.

3. Upaya penanganan tindak pidana *cyber crime* yang dapat dilakukan, yaitu melalui upaya non hukum seperti pendekatan teknologi, pendekatan budaya, /cultural, pendekatan edukatif/moral/moral religius, hingga pendekatan global seperti kerja sama internasional, Dan upaya hukum lain yang bisa dilakukan yaitu melakukan penegakan hukum terhadap tiga unsur sistem hukum, yakni struktur hukum (*legal structure*) substansi hukum (*legal substance*) dan budaya hukum (*legal culture*). Serta pendekatan sosial seperti informasi himbuan mengenai modus-modus kejahatan *cyber crime*, jalur pendidikan, pembinaan, dan menyiapkan penyidik polri untuk di didik agar mampu menyelidiki *cyber crime* serta meningkatkan upaya penyidikan, serta membangun dan mengefektifkan kerja sama internasional dalam memberantas tindak pidana *cyber crime*, serta peningkatan kualitas sarana dan kebijakan dalam menangani kejahatan ini sangat dibutuhkan dan juga terkait hal-hal pencegahan *cyber crime* itu sendiri.

### **B. Saran**

Pemerintah harus memberi pemahaman kepada masyarakat terhadap etika dan tanggung jawab dalam berinteraksi di dunia *cyber*. Perlu adanya peningkatan kesadaran literasi masyarakat tentang keamanan *cyber*. Serta membangun platform digital security di Indonesia. Institusi kepolisian juga perlu menjalin kolaborasi dengan berbagai pihak perguruan tinggi untuk meningkatkan kualitas

penguasaan teknologi informasi melalui berbagai macam bentuk kemitraan yang berkelanjutan disamping mendapatkan SDM yang terdidik dan terlatih yang dapat mendukung penyelidikan *cyber crime*. selain itu juga diperlukan kerjasama dengan berbagai negara dalam menangani kasus *cyber crime* untuk menelusuri para pelaku *cyber crime*.



## DAFTAR PUSTAKA

- Ahmad, M.Ramli. *Cyber Law Dan HAKI dalam Sistem Hukum Indonesia*, Bandung: PT. Refika Aditama. 2006.
- Arief, Barda Nawawi. *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta: Rajawali Pres, 2006.
- Arief, Barda Nawawi. *Pornografi, Pornoaksi Dan Cybersex/Cyberporn*. Semarang: Pustaka Magister, 2007.
- Arikunto, Suharsimi. *Prosedur Penelitian Suatu Pendekatan*, Jakarta: Rineke Cipta, 2002
- Aswan, *Tindak Pidana Penipuan Berbasis Transaksi Elektronik*, Makassar: Guepedia, 2019.
- Atmasasmita, Romli. *Reformasi Hukum Hak Asasi Manusia & Penegakan Hukum*, Bandung: Mandar Maju, 2001
- Hamzah, Andi. *Aspek-aspek Pidana Dibiidang Komputer*, Jakarta: Sinar Grafika, 1987.
- Hidayat, Arief. *Kajian Kritis Hukum Lingkungan Di Era Otonomi Daerah*, Semarang : Universitas Diponegoro, 2007.
- Ibrahim, Johnny. *Teori dan Metode Penelitian Hukum Normatif*, Jakarta: Bayumedia Publishing, 2005.
- Ilyas, Amir. *Asas-Asas Hukum Pidana: Memahami Tindak Pidana Dan Pertanggungjawaban Pidana Sebagai Syarat Pemidanaan*, (Yogyakarta: Rangkang Education Yogyakarta & Pukap-Indonesia, 2012.
- Lamintang P.A.F dan Franciscus Theojunior Lamintang, *Dasar-Dasar Hukum Pidana di Indonesia*, Jakarta: Sinar Grafika, 2014.
- Marpaung, Leden. *Asas Teori Praktik Hukum Pidana*, Jakarta: Sinar Grafika, 2008.
- Muladi dan Barda Nawawi Arief. *Teori-Teori Dan Kebijakan Pidana*, Bandung: Alumni, 2005.
- Matra, Ida Bagus. *Filsafat Penelitian dan metode penelitian social*. Yogyakarta: Pustaka Pelajar, 2004.
- Mertokusomo, Sudikno. *Mengenal Hukum*, Yogyakarta: Liberty Yogyakarta, 2003.
- Moeljanto, *Asas-Asas Hukum Pidana*, Jakarta: PT. Rineka Cipta, 2008.
- Mulyadi, Lilik. *Bunga Rampai Hukum Pidana Prespektif, Teoritis Dan Praktik*, Bandung: PT. Alumni, 2008.
- Polancik, Gregor. *Empirical Research Method Poster*, Jakarta: Gema Insani,
- Prakoso, Djoko. *Alat Bukti dan Kekuatan Pembuktian di dalam Proses Pidana*, Yogyakarta: Liberty, 1988.
- Prasetyo, Teguh. *Hukum Pidana*, Jakarta: PT. Raja Grafindo Persada, 2016
- Priyatno, Dwidja. *System Pelaksanaan Pidana di Indonesia*, Bandung: Refika Aditama, 2006.

- Prodjodikoro, Wirjono. *asas-asas hukum pidana di indonesia*, Bandung: PT. Refika Aditama, 2003.
- Raharjo, Agus. *Cyber Crime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* Bandung: Citra Aditya Bakti, 2002.
- Rusianto, Agus. *Tindak Pidana dan Pertanggungjawaban Pidana*, Jakarta: kencana, 2016.
- Sahariyanto, Budi. *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan dan Celah Hukumnya*, Jakarta: Rajawali Pers 2012.
- Shihab, M. Quraish. *Tafsir Al-Mishbah, Surah Al-Ma'idah* Jakarta : Lentera Hati, 2002.
- Sianturi, Kanter. *Asas-Asas Hukum Pidana di Indonesia dan Penerapannya* Jakarta: Alumni AHM-PTHM, 1982.
- Sitompul, Josua. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*, Jakarta: Rajawali Pers, 2012.
- Soekanto, Soerjono. *Pengantar Penelitian Hukum*, Jakarta: Universitas Indonesia Press, 1984.
- S.R. Sianturi, *Asas-Asas Hukum Pidana di Indonesia dan Penerapannya*, Jakarta: PT. Citra Aditya Bakti, 1996.
- Sudarto, *Kapita Selekta Hukum Pidana* Bandung: Alumni, 1981.
- Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D* Bandung: Alfabeta, 2016.
- Suhariyanto, Budi. *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*, Jakarta: PT. Raja Grafindo Persada, 2012.
- Suhariyanto, Budi. *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*, Depok: PT. Raja Grafindo Persada, 2013.
- Sulistiyo, Hermawan. *Cyber Crime: Modus Operandi Dan Penanggulangannya* Cet. 1; Yogyakarta: LaksBang Pressindo, 2007.
- Sunggono, Bambang. *Metode Penelitian Hukum*, Jakarta: PT. Raja Grafindo Persada, 2007.
- Suparni, Niniek. *Cyberspace problematika & Antisipasi Pengaturannya*, Jakarta: Sinar Grafika, 2009.
- Susilo, *Kriminologi (Pengetahuan Tentang Sebab-Sebab Kejahatan)*, Bogor: Politeia, 1985.
- Tomalili, Rahmanuddin. *Hukum Pidana*, Yogyakarta: CV Budi Utama, 2019.
- Uladi dan Barda Nawawi Arief. *Teori-Teori dan Kebijakan Pidana*, Bandung: PT Alumni, 2010.

- Usman, Husaini dan Purnompo Setiady Akbar. *Metodologi Penelitian Sosial*. Jakarta: Bumi Aksara, 2009.
- Usman, Sabian. *Dasar-Dasar Sosiologi* Yogyakarta: Pustaka Belajar, 2009.
- Vago, Steven. *Law And Society: Third Edition*, New Jersey; Prentice Hall, 1991.
- Wahid, Abdul dan Muhammad Labib. *Kejahatan Mayantara (Cyber crime)*, Jakarta: PT. Refika Aditama, 2015.
- Wahyo, Bambang. *Tindak Pidana dan Pemidanaan*, Jakarta: Sinar Grafika, 2000.
- W. Gulo. *Metodologi Penelitian*, Jakarta: Pt. Grasindo, 2005.
- Wiratmono, Joko. "Tinjauan Yuridis Cyber Crime" Skripsi, Surabaya: Universitas Pembangunan Nasional Veteran, 2019, Diakses Pada Tanggal 20 Januari 2023.
- Yurizal, *Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia*, Malang: Media Nusa Creative, 2018.

#### **Jurnal Ilmiah:**

- AMT IT Solutions "6 Kasus Cyber Crime di Indonesia Menyerang Server," <https://amt-it.com/blog/kasus-cyber-crime-di-indonesia/>, Diakses Pada Tanggal 17 Juni 2023, Pukul: 20;30
- Arifah, Dista Amaliah. "Kasus Cyber Crime di Indonesia", *Jurnal Bisnis Dan Ekonomi*. 18, No.2, (September 2011), <https://www.unisbank.ac.id/ojs/index.php/fe3/article/view/2099/767>
- Bahje, Ahmad. "Sejarah dan Problematika Hukum Pidana Materil di Indonesia", *SOSIO-RELIGIA* 5, No.2 (2006).
- Djanggih, Hardianto. "Kebijakan Hukum Pidana dalam Penanggulangan Tindak Pidana Cyber Crime di Bidang Kesusilaan". *Jurnal Media Hukum*, 1, No. 2, (November, 15, 2017), <https://doi.org/10.31219/osf.io/c9m25>.
- Farid, Achmad. "14 Kasus Cyber Crime Yang Mengemparkan Warganet" 11 Oktober 2022, <https://www.exabytes.co.id/blog/kasus-cyber-crime-di-indonesia/>, Diakses Pada Tanggal 17 Juni 2023, Pukul: 23;15.
- Ginjar, Denda. "Urgensi Perlindungan Data Pribadi dalam Menjamin Keamanan Data", *Jurnal Hukum dan HAM West Science*, 1, No.1, (November, 14, 2022), <https://wnj.westsciencepress.com/index.php/jhhws/article/view/7>
- Gunarto, Marcus Priyo "Asas Keseimbangan dalam Konsep Rancangan Undang-Undang Kitab Undang-Undang Hukum Pidana," *MIMBAR HUKUM* 24, No.1 (2012).
- Indah, Febyola dan Arista Quera Sidabutar, Nurul Annisa Nasution. "peran cyber security terhadap keamanan data penduduk negara indonesia" *Jurnal Bidang Penelitian Informatika*, 1, No.1, (Oktober, 22, 2022). <https://ejournal.kreatifcemerlang.id/index.php/jbpi/article/view/78>

- Kartiko, Galuh. "Pengaturan Terhadap Yuridiksi *Cyber Crime* Ditinjau dari Hukum Internasional." *Jurnal universitas trunojoyo Madura*, 8, No.2, (Desember 2013). <https://doi.org/10.21107/ri.v8i2.695>.
- Ketaren, Eliasta. "Cyber Crime, Cyber Space, dan Cyber Law." *Jurnal Times*, 5, No.2, (Februari, 13, 2017).
- Liviani, Isnatul. "Kejahatan Teknologi Informasi (*Cyber Crime*) dan Penanggulangannya dalam Sistem Hukum Indonesia." *Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, 23, No.2, (Desember 2020).
- Muladi, "Kebijakan Kriminal Terhadap *Cyber Crime*", *Majalah Media Hukum*, 1 No.3, (23 Agustus 2003).
- Nugraha, Riko. "Perspektif Hukum Indonesia (*Cyberlaw*) Penanganan Kasus Cyber di Indonesia", *Jurnal Ilmiah Hukum Dirgantara-Fakultas Hukum Universitas Dirgantara Marsekal Suryadarma*, 11, No. 2, (Maret 2021), <https://doi.org/10.35968/jihd.v11i2.767>
- Oktaviani, Asrarina dan Emmilia Rusdiana. "Alternative Pidana Bagi Pelaku Tindak Pidana Peretasan di Indonesia dalam Undang-Undang Informasi dan Transaksi Elektronik." *Jurnal Hukum*, 1, no.1 (januari, 9, 2023), <https://doi.org/10.2674/novum.v0i0.50394>
- Rahajeng Indraswari. "*Yurisdiksi Kriminal Berlakunya Hukum Pidana Nasional Terhadap Cyber Crime di Luar Yurisdiksi Indonesia*". Thesis, (Padang: Universitas Andalas).
- Rahmawati, Ineu. "Analisis Manajemen Resiko Ancaman Kejahatan Siber (*Cyber Crime*) dalam Peningkatan Cyber Defense". *Jurnal Pertahanan dan Bela Negara*. 7, No.2 2017, <https://dx.doi.org/10.33172/jpbh.v7i2.179>
- Rilandi, Nanda Risky. "Tinjauan Yuridis Tindak Pidana Cyber Crime Berdasarkan Hukum Pidana." *Jurnal Hukum dan Social Politik*, 1, No.2, (Mei 12, 2023), <https://doi.org/10.59581/Jhsp-Widyakarya.V1i2.214>.
- Shofian, Jhodi. "*Tinjauan Siyasah Dusturiyah Terhadap Pelaksanaan Kewenangan Cyber Crime Polda Bengkulu dalam Pembentukan Virtual Police*." Thesis, (UIN Fatmawati Sukarno Bengkulu, 2022)
- Siregar, Bonanda Japatani. "Problem dan Pengaturan *Cyber Crime* Melalui Aktifitas Internet dalam Kasus Sara di Pilkada Serentak 2018." *Jurnal Penelitian Pendidikan Sosial Humaniora*, 3, No.1, (Mei, 24, 2018), <https://doi.org/10.32696/jp2sh.v3i1.96>.
- Utin Indah Permata Sari, "Kebijakan Penegakan Hukum dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police di Indonesia." *Jurnal Hukum*, 2, No.1, (Oktober 2021),
- Wardani, Agilia Maya Asia. "*Perlindungan Hukum Terhadap Korban Tindak Pidana Siber (Cyber Crime) (Studi Ditreskrimsus Polda Jateng)*". Doctoral Dissertation, (Purwokerto: Universitas Jenderal Soedirman, 2021)
- Yustitiana, Rhesita. "Pelaksanaan Pengaturan Hukum Tindak Kejahatan Fraud Phising Transaksi Elektronik Sebagai Bagian dari Upaya Penegak Hukum di Indonesia dikaitkan dengan Teori Efektivitas Hukum". *Jurnal Hukum*

*VisioJustisia*,1,No.1,(Juli2021),  
<https://ojs.uph.edu/index.php/vj/article/3802/pdf>

**Perundang-Undangan:**

Undang-Undang Republik Indonesia No. 19 Tahun 2019 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).

Undang-Undang No. 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP)

Undang-Undang No. 28 Tahun 2018 tentang Hak Cipta

Undang-Undang No. Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme

Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi

Undang-Undang No. 32 Tahun 2002 tentang Penyiaran

Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.



## DAFTAR RIWAYAT HIDUP



**Sriwulan**, lahir di Salukarondang pada Tanggal 05 Mei 2001, penulis merupakan anak pertama dari enam bersaudara dari pasangan seorang Ibu bernama Rahmiati dan Ayah Nurdin. Saat ini, penulis bertempat tinggal di Dusun Salukarondang Desa Dandang Kecamatan Sabbang Selatan Kabupaten Luwu Utara Provinsi Sulawesi Selatan. Pendidikan dasar penulis diselesaikan pada Tahun 2013 di SDN 008 Dandang, kemudian di Tahun yang sama menempu Pendidikan di SMPN 1 Sabbang hingga Tahun 2016. Pada saat menempu Pendidikan di SMP, penulis mengikuti kegiatan ekstrakurikuler Pramuka. Pada Tahun 2016 melanjutkan Pendidikan di SMKN 7 Luwu Utara.

Pada Tahun 2019, Penulis melanjutkan Pendidikan di Institut Agama Islam Negeri (IAIN) Palopo melalui jalur UMPTKIN pada Program Studi Hukum Tata Negara (HTN) Fakultas Syariah (*siyazah*). Sebelum menyelesaikan Studi, peneliti membuat tugas akhir berupa Skripsi dengan mengangkat Judul “Tinjauan Yuridis Tindak Pidana *Cyber Crime* di Indonesia” sebagai persyaratan untuk menyelesaikan Studi pada jenjang Strata Satu (S1) dan memperoleh gelar Sarjana Hukum (S.H).