

SKRIPSI
ANALISIS KEBIJAKAN HUKUM TENTANG KEJAHATAN DUNIA MAYA
DALAM SISTEM HUKUM PIDANA DI INDONESIA



Oleh :

ANDI RABIAHTUL ADABYAH. AP
040 2019 0323

Diajukan sebagai Tugas Akhir dalam rangka Penyelesaian Studi

FAKULTAS HUKUM
UNIVERSITAS MUSLIM INDONESIA
MAKASSAR
2023

HALAMAN JUDUL

**ANALISIS KEBIJAKAN HUKUM TENTANG KEJAHATAN DUNIA MAYA
DALAM SISTEM HUKUM PIDANA DI INDONESIA**

SKRIPSI

**Skripsi ini diajukan untuk memenuhi salah satu persyaratan guna
memperoleh gelar Sarjana Hukum pada Fakultas Hukum pada
Program Studi Ilmu Hukum di Universitas Muslim Indonesia**

Oleh :

**ANDI RABIAHTUL ADABYAH. AP
040 2019 0323**

**FAKULTAS HUKUM
UNIVERSITAS MUSLIM INDONESIA
MAKASSAR
2023**

PERSETUJUAN PEMBIMBING

Diterangkan bahwa hasil penelitian mahasiswa :

Nama Mahasiswa : Andi Rabiahtul Adabyah. AP
Stambuk : 04020190323
Bagian : Hukum Pidana
Judul Penelitian : **ANALISIS KEBIJAKAN HUKUM TENTANG
KEJAHATAN DUNIA MAYA DALAM
SISTEM HUKUM PIDANA DI INDONESIA**
Dasar Penetapan : **0396/H.05/FH.UMI/IX/2022**

Telah diperiksa dan disetujui untuk diajukan dalam **Ujian Skripsi**

Makassar, 12 Juli 2023

Komisi Pembimbing

Pembimbing I,

Pembimbing II,



Prof. Dr. H. Hambali Thalib, SH.,MH.
NIP. 195503131981111001



Yuli Adha Hamzah, SH.,MH.,M.Kn
NIPs.104151397

Mengetahui

Ketua Bagian Hukum Pidana



Prof. Dr. H. Mulyati Pawennei, SH.,M. Hum
NIP. 196112011987032003

PERSETUJUAN UJIAN SKRIPSI

Diterangkan bahwa skripsi mahasiswa :

Nama Mahasiswa : Andi Rabiahtul Adabyah. AP
Stambuk : 04020190323
Bagian : Hukum Pidana
Judul Penelitian : **ANALISIS KEBIJAKAN HUKUM TENTANG
KEJAHATAN DUNIA MAYA DALAM
SISTEM HUKUM PIDANA DI INDONESIA**
Dasar Penetapan : **0396/H.05/FH.UMI/IX/2022**

Memenuhi syarat untuk diajukan dalam ujian skripsi sebagai ujian akhir program studi

Dikeluarkan di : Makassar
Pada Tanggal : 12 Juli 2023
Dekan Fakultas Hukum
Universitas Muslim Indonesia



Prof. Dr. La Ode Husen, S.H., M.Hum
NIPs. 104 86 0192

PENGESAHAN SKRIPSI

**ANALISIS KEBIJAKAN HUKUM TENTANG KEJAHATAN DUNIA MAYA
DALAM SISTEM HUKUM PIDANA DI INDONESIA**

Disusun dan diajukan oleh :

ANDI RABIAHTUL ADABYAH. AP

04020190323

Telah dipertahankan dihadapan Panitia Ujian Skripsi
pada Program Studi Sarjana Ilmu Hukum Fakultas Hukum
Universitas Muslim Indonesia
Pada ..02.., Agustus 2023
dan dinyatakan diterima

Makassar, 02 Agustus 2023

Panitia Ujian,

Ketua,

Prof. Dr. H. Hambali Thalib, SH.,MH.
NIP. 195503131981111001

Anggota,

Yuli Adha Hamzah, SH.,MH.
NIPs. 104151397

Dekan Fakultas Hukum
Universitas Muslim Indonesia



Prof. Dr. La Ode Husen, S.H., M.Hum
NIPs. 104 86 0192

HALAMAN PENGESAHAN

Diterangkan bahwa skripsi dibawah ini

Judul Penelitian : **Analisis Kebijakan Hukum Tentang
Kejahatan Dunia Maya Dalam
Sistem Hukum Pidana Di Indonesia**

Nama Mahasiswa : Andi Rabihtul Adabyah. AP

Nomor Stambuk : 04020190323

Program Studi : Ilmu Hukum

Bagian : Hukum Pidana

Dasar Penetapan : **0396/H.05/FH.UMI/IX/2022**

Telah dipertahankan dihadapan majelis Ujian Skripsi dan dinyatakan
LULUS, oleh :

1. Prof. Dr. H. Hambali Thalib, S.H., M.H. (.....)
(Pembimbing Ketua)
2. Yuli Adha Hamzah, SH., MH., M. Kn (.....)
(Pembimbing Anggota)
3. Dr. H. Azwad Rachmat Hambali, SH., MH. (.....)
(Penguji I)
4. Hj. Nurbaya Mangatta, SH., MH. (.....)
(Penguji II)



PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan dibawah ini :

Nama Mahasiswa : Andi Rabiahtul Adabyah. AP
NIM : 04020190323
Bagian : Hukum Pidana
Judul Skripsi/Penelitian : **Analisis Kebijakan Hukum Tentang
Kejahatan Dunia Maya Dalam
Sistem Hukum Pidana Di Indonesia**

Menyatakan dengan sebenarnya bahwa skripsi saya ini benar merupakan hasil karya sendiri, bukan merupakan hasil plagiasi terhadap karya ilmiah orang lain. Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan dari skripsi ini merupakan hasil plagiasi, maka saya bersedia menerima sanksi karena perbuatan tersebut

Makassar, Agustus 2023
Yang menyatakan,

Andi Rabiahtul Adabyah. AP

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Dengan memanjatkan puji syukur kehadiran Allah SWT, karena atas berkat rahmat dan karunia-Nya akhirnya penulis dapat menyelesaikan Skripsi ini.

Penulisan Skripsi dilakukan dalam rangka memenuhi salah satu syarat memperoleh gelar Sarjana Hukum (S.H.) pada Fakultas Hukum Universitas Muslim Indonesia Makassar. Adapun judul Skripsi yang penulis susun adalah “**Analisis Kebijakan Hukum Tentang Kejahatan Dunia Maya Dalam Sistem Hukum Pidana di Indonesia**”.

Penulis berkewajiban untuk menyampaikan ucapan teristimewa dan penghargaan setinggi-tingginya kepada keluarga tercinta khususnya kedua orang tua penulis Ayahanda **Andi Parenrengi** dan **Andi Lilis Suryani** dengan susah dan jerih payahnya mengasuh dan mendidik serta memberikan materi yang tak henti-hentinya baik diwaktu kuliah maupun diwaktu penyelesaian skripsi ini. Serta kakak saya **Andi Yati Apriliani**, adik-adik saya **Andi Khusnul Khatimah** dan **Andi Syahrul Ramadhan** dan Suami saya **Andi Walinono** tercinta yang selalu memberikan motivasi dalam menggapai cita-cita. Selanjutnya diucapkan terima kasih kepada :

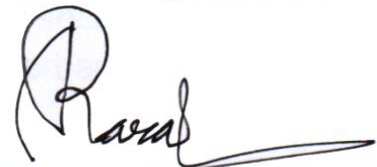
1. Yth. Bapak Prof. Dr. H. Basri Modding, S.E., M.Si. selaku Rektor Universitas Muslim Indonesia di Makassar.

2. Yth. Bapak Prof. Dr. H. La Ode Husein, S.H.,M.H. selaku Dekan Fakultas Hukum Universitas Muslim Indonesia.
3. Yth Ibu Prof. Dr. Hj. Mulyati Pawennei, SH.,MH., selaku Ketua Bagian Hukum Pidana Fakultas Hukum Universitas Muslim Indonesia; yang telah memberikan izin, kesempatan dan fasilitas kepada Penulis selama mengikuti pendidikan Program Sarjana
4. Yth. Bapak Prof. Dr. H. Hambali Thalib, SH.,MH selaku Pembimbing Ketua dan Ibu Yuli Adha Hamzah, SH.,MH., M.Kn selaku Pembimbing Anggota yang memberikan bimbingan, dengan penuh keseriusan, kecermatan.
5. Bapak dan Ibu Dosen serta Asisten Dosen Fakultas Hukum Universitas Muslim Indonesia Makassar yang telah memberikan ilmu yang berguna sejak memasuki bangku kuliah sampai dengan selesainya studi penulis di Fakultas Hukum.
6. Seluruh Karyawan/Karyawati Fakultas Hukum Universitas Muslim Indonesia Makassar yang telah membantu dalam pelayanan administrasi selama mengikuti Pendidikan sampai terlaksananya ujian sarjana.
7. Keluarga besar penulis yang selalu memberikan dukungan serta doa yang berlimpah
8. Pihak lain yang tidak dapat disebutkan namanya satu persatu yang terlibat dan membantu sehingga skripsi ini dapat tersusun dengan baik dan lancar.

Akhir kata saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan kepada semua pihak yang telah membantu. Skripsi ini tidak luput dari adanya kekurangan dan kelemahan baik dalam penyusunannya maupun penulisannya. Untuk itu dengan senang hati penulis menerima segala kritik, saran, maupun komentar untuk menyempurnakannya, dengan tetap menyatakan secara keseluruhan skripsi ini menjadi tanggung jawab penulis.

Semoga dengan hadirnya skripsi ini dapat bermanfaat bagi pengembangan ilmu.

Makassar, 12 Agustus 2023

A handwritten signature in black ink, appearing to read 'Rabihtul Adabyah. AP', with a long horizontal flourish extending to the right.

Andi Rabihtul Adabyah. AP

ABSTRAK

Andi Rabiahtul Adabyah. AP. Analisis Kebijakan Hukum Tentang Kejahatan Dunia Maya Dalam Sistem Hukum Pidana di Indonesia. Di bawah bimbingan (Prof. Dr. H. Hambali Thalib, SH.,MH.) Sebagai Ketua Pembimbing dan (Yuli Adha Hamzah, SH.,MH., M.Kn) Sebagai Anggota Pembimbing

Penelitian ini bertujuan untuk mengetahui dan menganalisis sejauh manakah tindakan Kejahatan Dunia Maya di sebut tindak pidana. Dan untuk mengetahui dan menganalisis bagaimanakah kebijakan mengenai Kejahatan Dunia Maya dalam Hukum Pidana.

Metode Penelitian yang digunakan dalam penulisan hasil penelitian ini adalah metode penelitian Normatif, yaitu bahan hukum yang diperoleh dari peraturan perundang-undangan, buku-buku literatur, artikel hukum, dan bacaan lainnya yang berkaitan dengan masalah yang dibahas. Adapun sumber bahan hukum yang digunakan yaitu bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier.

Hasil penelitian penulis yaitu kemajuan teknologi membawa dampak perubahan sosial dalam masyarakat baik secara positif maupun negatif. Dimana dari sisi negatif memicu lahirnya berbagai kejahatan siber atau yang sering disebut *cybercrime*. Sehingga diperlukan kebijakan mengenai Kejahatan Dunia Maya Kitab Undang-Undang Hukum Pidana (KUHP) menjadi dasar untuk menjangkit *Cyber Crime*, yang memenuhi unsur-unsur dalam pasal-pasal KUHP. Selain KUHP ada juga aturan hukum yang berkaitan dengan hal ini, yaitu Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), dimana aturan tindak pidana yang terjadi di dalamnya terbukti mengancam para pengguna internet.

Adapun saran dari judul yang saya teliti yaitu pemerintah lebih meningkatkan keamanan terhadap data atau informasi yang terdapat dalam jaringan komputer. Dan diharapkan bagi masyarakat dalam menggunakan teknologi dan informasi atau internet sebagai sarana positif.

Kata Kunci : Kebijakan Hukum, Kejahatan Dunia Maya, Hukum Pidana.

DAFTAR ISI

HALAMAN JUDUL.....	ii
PERSETUJUAN PEMBIMBING.....	iii
PERSETUJUAN UJIAN SKRIPSI	iv
PENGESAHAN SKRIPSI	v
HALAMAN PENGESAHAN	vi
PERNYATAAN KEASLIAN SKRIPSI.....	vii
KATA PENGANTAR	viii
ABSTRAK.....	xi
DAFTAR ISI	xii
BAB I PENDAHULUAN	1
A. Latar Belakang Masalah	1
B. Rumusan Masalah	9
C. Tujuan Penelitian	9
D. Kegunaan Penelitian	9
BAB II TINJAUAN PUSTAKA.....	11
A. Kebijakan Hukum Pidana.....	11
B. Kejahatan Dunia Maya (Cyber Crime).....	14
1. Definisi Cyber Crime	15
2. Bentuk- Bentuk <i>Cyber Crime</i>	17
C. Hukum Pidana	25
D. Tindak Pidana	26
1. Definisi Tindak Pidana	26
2. Unsur-unsur Tindak Pidana	30
3. Penyebab Terjadinya Tindak Pidana	33
BAB III METODE PENELITIAN.....	36
A. Tipe Penelitian	36
B. Pendekatan Penelitian	36
C. Sumber Bahan Hukum.....	37

D. Teknik Pengumpulan Bahan Hukum	38
E. Analisis Bahan Hukum	39
BAB IV HASIL PENELITIAN DAN PEMBAHASAN	40
A. Tindakan Kejahatan Dunia Maya (<i>Cybercrime</i>) yang dapat disebut sebagai Tindak Pidana	40
B. Kebijakan Tindak Pidana Kejahatan Dunia Maya di Indonesia.....	48
C. Analisis Penulis	62
BAB V PENUTUP	64
A. Kesimpulan	64
B. Saran	65
DAFTAR PUSTAKA.....	66

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Teknologi Komunikasi dan Informasi adalah aplikasi pengetahuan dan keterampilan yang digunakan manusia dalam mengalirkan informasi atau pesan dengan tujuan untuk membantu menyelesaikan permasalahan manusia agar tercapai tujuan komunikasi. Perkembangan teknologi informasi berawal dari kemajuan dibidang komputerisasi. Penggunaan komputer pada masa awal untuk sekedar menulis, membuat grafik dan gambar serta alat menyimpan data yang luar biasa telah berubah menjadi alat komunikasi dengan jaringan yang lunak dan bisa mencakup seluruh dunia. Dengan kemajuan teknologi maka proses interaksi antar manusia mampu menjangkau lapisan masyarakat dibelahan dunia manapun menjadi semakin terbuka.

Teknologi Informasi adalah suatu teknologi yang digunakan untuk mengolah data, termasuk memproses, mendapatkan, menyusun, menyimpan, memanipulasi data dalam berbagai cara untuk menghasilkan informasi yang berkualitas, yaitu informasi yang relevan, akurat dan tepat waktu, yang digunakan untuk keperluan pribadi, bisnis, dan pemerintahan dan merupakan informasi yang strategis untuk pengambilan keputusan. Teknologi ini menggunakan seperangkat komputer untuk mengolah data, sistem jaringan untuk

menghubungkan satu komputer dengan komputer yang lainnya sesuai dengan kebutuhan, dan teknologi telekomunikasi digunakan agar data dapat disebar dan diakses secara global.

Teknologi informasi mengalami perkembangan yang pesat di era modern, tak terkecuali di Indonesia. Indonesia adalah negara hukum seperti yang tertuang dalam konstitusi, sebagai sebuah negara hukum tentunya negara wajib melindungi setiap warga negaranya dari setiap perbuatan yang dapat merugikan apalagi perbuatan tersebut dapat merusak tatanan kehidupan berbangsa dan bernegara. Seperti halnya kejahatan yang terjadi di dunia maya atau biasa disebut dengan *cybercrime*. Kejahatan yang tidak menganal ruang dan waktu ini mengalami perkembangan yang pesat akhir-akhir ini, kecanggihan teknologi yang disalah gunakan oleh oknum yang tidak bertanggung jawab demi keuntungan pribadi yang menyebabkan negara-negara berkembang kesulitan untuk menindak pelaku kejahatan komputer khususnya pihak kepolisian, disamping dibutuhkan suatu perangkat aturan yang mengatur tentang penyalahgunaan informasi ini juga dibutuhkan sumber daya manusia dan sarana dan prasarana yang mendukung.¹

Kecepatan teknologi informasi yang begitu cepat membuat masyarakat cenderung lebih menerima dibandingkan menyaring

¹ Dheny Wahyudi. (2020). Perlindungan Hukum Terhadap Korban Kejahatan *Cyber Crime* di Indonesia. Jurnal Ilmu Hukum, Universitas Jambi, hlm. 99

terlebih dahulu kebenaran informasi yang diterima, sehingga adanya refleksi pengguna yang semakin berkurang²

Kejahatan yang terjadi di dunia maya lahir akibat dampak negatif dari perkembangan teknologi, kejahatan yang terjadi dari berbagai bentuk dan jenisnya tersebut membawa konsekwensi terhadap perlindungan hukum penggunaannya hal ini penting mengingat bahwa setiap manusia harus dilindungi sesuai dengan harkat dan martabatnya sebagai manusia. Salah satu bentuk wujud tanggung jawab negara atas perlindungan terhadap warga negaranya adalah dengan memberikan jaminan hukum dan tindakan nyata yang melindungi masyarakatnya dari segala bentuk kejahatan atau perbuatan-perbuatan menyimpang lainnya yang mungkin di alami oleh masyarakat baik di dunia nyata ataupun di dunia maya.

Teknologi informasi di yakini membawa keuntungan yang besar bagi negara-negara di dunia. Lahir suatu rezim hukum baru yang dikenal dengan hukum *cyber*, yang diambil dari kata *Cyber Law* adalah istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Istilah lain yang digunakan yaitu Hukum Teknologi Informasi (*Law Of Information Technology*), Hukum Dunia Maya (*Virtual World Law*). Istilah-istilah tersebut lahir mengingat kegiatan internet dan manfaat teknologi informasi berbaris virtual. Istilah hukum *cyber* digunakan dalam tulisan ini dilandasi pemikiran bahwa *cyber* jika

² Noviantini, N., Remaja, I. N. G., & Mariadi, N. N. (2021). Efektivitas Patroli Siber Dalam Mengungkap Kasus Ujaran Kebencian Di Wilayah Hukum Polres Buleleng. *Kertha Widya*, 9(1), 37.

diidentikan dengan "Dunia Maya" akan cukup menghadapi persoalan jika harus membuktikan suatu persoalan yang diasumsikan sebagai "maya", sesuatu yang tidak terlihat dan semu.³

Internet yang merupakan salah satu hasil teknologi informasi adalah sumber daya informasi yang mampu menjangkau seluruh dunia. Di Indonesia kini bahkan muncul desa digital, di mana memanfaatkan internet untuk meningkatkan kesejahteraan masyarakat baik dari aspek ekonomi, aspek kesehatan dan aspek pendidikan.

Indonesia merupakan salah satu negara di dunia yang masyarakatnya kebanyakan sudah menggunakan gadget (alat komunikasi elektronik) seperti telepon seluler atau smartphone dan juga media sosial saat ini Indonesia adalah negara dengan jumlah pengguna internet terbanyak ke-4 di dunia. Jumlah pengguna internet di Indonesia terus meningkat setiap tahunnya. Berdasarkan hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), ada 210,03 juta pengguna internet di dalam negeri pada periode 2021-2022. Jumlah itu meningkat 6,78% dibandingkan pada periode sebelumnya yang sebesar 196,7 juta orang. Hal itu pun membuat tingkat penetrasi internet di Indonesia menjadi sebesar 77,02%.⁴

³ Budi Suhariyanto. (2007). Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya, Depok : PT. Rajagrafindo Persada, halaman 1-2.

⁴ Dimas Bayu. (2022, 9 Juni). Pengguna Internet Indonesia Tembus 210 Juta pada 2022. *DataIndonesia.id*. Diakses pada tanggal 18 Oktober 2022

Besarnya pengguna internet memicu munculnya banyak pihak yang ingin melakukan kejahatan di dunia maya atau yang lebih dikenal dengan *cyber crime*.

Kejahatan siber atau dalam bahasa Inggris disebut *cyber crime* adalah kejahatan yang disebabkan oleh majunya teknologi serta pengembangannya, dan cepatnya arus penyebaran informasi tersebar di internet, yang disebut sebagai "dunia maya". *Cyber crime* merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif yang sangat luas bagi seluruh bidang kehidupan modern saat ini.⁵ Modern disini diartikan sebagai kecanggihan dari kejahatan tersebut sehingga pengungkapannya pun melalui sarana yang canggih pula. Secara singkat, *Cyber crime* merupakan bentuk-bentuk kejahatan yang ditimbulkan karena pemanfaatan teknologi internet.

Tingkat *cyber crime* di Indonesia tergolong cukup tinggi. Berdasarkan laporan State of The Internet 2013, Indonesia berada di urutan kedua dalam daftar lima besar negara asal serangan kejahatan siber atau *cyber crime*. Total kerugian *cyber crime* di Indonesia mencapai Rp 33,29 miliar.⁶ Fakta tersebut menunjukkan bahwa *cyber crime* di Indonesia merupakan kejahatan yang serius dan perlu

⁵ Barda Nawawi Arief. (2007). Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan. Jakarta: Kencana, hlm. 237.

⁶ Fidel Ali Permana. (2015, 12 Mei). Indonesia Urutan Kedua Terbesar Negara Asal "Cyber Crime" di Dunia. Nasional.kompas.com. Diakses pada tanggal 19 Oktober 2022.

peraturan yang memadai untuk mencegahnya, khususnya dalam aspek hukum pidana.

Secara garis besar, kejahatan yang berkaitan dengan teknologi informasi dapat dibagi menjadi dua bagian besar. Pertama, kejahatan yang bertujuan merusak atau menyerang sistem atau jaringan komputer. Dan kedua, kejahatan yang menggunakan komputer dan internet sebagai alat bantu dalam melancarkan kejahatan. Namun, mengingat teknologi informasi (telekomunikasi, komputer dan media) dapat berkembang seiring waktu maka kejahatan jenis diatas dapat berkembang menjadi lebih luas lagi.

Cyber crime adalah bentuk-bentuk kejahatan yang timbul karena memanfaatkan teknologi internet. Seiring dengan kemajuan teknologi informasi, telah muncul beberapa kejahatan dengan karakteristik yang sama sekali baru. Kejahatan tersebut timbul akibat penyalahgunaan jaringan internet, yang membentuk *cyber space* (ruang siber). *Cyber crime* adalah kejahatan yang sering dipersepsikan sebagai kejahatan yang dilakukan dalam ruang atau wilayah siber.

Cyber crime adalah sebuah perbuatan yang tecela dan melanggar kepatutan di dalam kehidupan masyarakat serta melanggar hukum, sekalipun sampai sekarang sukar untuk menemukan norma hukum yang secara khusus mengatur *cyber crime*. Oleh karena itu peran masyarakat dalam upaya menegakan hukum

terhadap *cybercrime* adalah penting untuk menentukan sifat dapat dicela dan melanggar kepatutan masyarakat dari suatu perbuatan *cyber crime*.⁷

Menurut kepolisian Inggris, *Cyber Crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan/atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital. Kejahatan dunia maya merupakan istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran, atau tempat terjadinya kejahatan. Termasuk dalam kejahatan dunia maya, antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit/*carding*, *confidence fraud*, penipuan identitas, pornografi anak, dan sebagainya. Namun istilah ini juga digunakan untuk kegiatan kejahatan di mana komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.⁸

Allah berfirman dalam surah al-Ahzab ayat 58:

وَالَّذِينَ يُؤْذُونَ الْمُؤْمِنِينَ وَالْمُؤْمِنَاتِ بَغَيْرِ مَا اكْتَسَبُوا فَقَدْ احْتَمَلُوا بُهْتَانًا
وَإِثْمًا مُّبِينًا ٥٨

“Dan orang-orang yang menyakiti orang-orang mukmin dan mukminat tanpa kesalahan yang mereka perbuat, maka sesungguhnya mereka telah memikul kebohongan dan dosa yang nyata.”(QS: Al-Ahzab [33]:58).

⁷ Dikdik M. Arief Mansur, dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, Bandung : PT. Grafika Aditama 2005, hlm. 89

⁸ Ricky Adjie Purnama, “Cyber Crime Dalam Perspektif Hukum Positif dan Hukum Islam”(Skripsi Fakultas Syari’ah IAIN SMH Bante, 2007), hlm. 12

Ayat tersebut menegaskan bahwa tindakan perusakan merupakan sesuatu yang dilarang oleh Allah swt. baik dalam bentuk apapun dan di manapun, 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 larangan tersebut mengarah kepada hal-hal yang merugikan dan meresahkan orang lain. Perbuatan *cybercrime* merupakan perbuatan yang dapat menyakiti korbannya. Menyakiti yang dimaksud disini bukanlah menyakiti dalam artian fisik karena *cybercrime* bukanlah perbuatan yang sama sekali tidak menyertakan serangan fisik atau mengakibatkan luka fisik, melainkan *cybercrime* merupakan perbuatan yang dampaknya menyakiti fisikis korbannya.

Indonesia memiliki Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya dalam tulisan ini, disingkat penyebutannya dengan UU ITE) dan dihubungkan dengan Kitab Undang-Undang Hukum Pidana (KUHP) 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 aparaturnya penegak hukum.

Berdasarkan latar belakang masalah yang telah diuraikan diatas maka penulis melakukan penelitian dengan judul “**ANALISIS KEBIJAKAN HUKUM TENTANG KEJAHATAN DUNIA MAYA DALAM SISTEM HUKUM PIDANA DI INDONESIA**”.

B. Rumusan Masalah

1. Sejauh manakah tindakan Kejahatan Dunia Maya (*CyberCrime*) dapat disebut tindak Pidana?
2. Bagaimanakah kebijakan mengenai Kejahatan Dunia Maya (*CyberCrime*) dalam Hukum Pidana?

C. Tujuan Penelitian

1. Untuk mengetahui apakah *cybercrime* merupakan suatu tindak pidana di Indonesia
2. Untuk mengetahui dan menganalisis apakah kebijakan dan peraturan perundang-undangan di Indonesia sudah mengatur tentang tindakan *cybercrime*.

D. Kegunaan Penelitian

1. Manfaat Teoritik

Diharapkan penelitian ini dapat digunakan sebagai bahan kajian bagi kalangan hukum, dalam mengembangkan memperluas ilmu pengetahuan dalam badan hukum, terkhususnya dibidang hukum pidana.

2. Manfaat Praktik

Sebagai bahan masukan terhadap aparat penegak hukum dalam hal pengaturan tindakan *cybercrime* dalam pembaharuan hukum pidana di Indonesia

BAB II

TINJAUAN PUSTAKA

A. Kebijakan Hukum Pidana

Kebijakan hukum pidana pada dasarnya ialah keseluruhan dari peraturan yang menentukan perbuatan apa yang dilarang dan termasuk kedalam tindak pidana, serta bagaimana sanksi yang dijatuhkan terhadap pelakunya dengan tujuan untuk penanggulangan kejahatan. Secara teori, banyak doktrin yang dikemukakan oleh para ahli terkait dengan pengertian kebijakan hukum pidana.

Barda Nawawi, berpendapat bahwa istilah “Kebijakan” diambil dari istilah “*policy*” (Inggris) dan “*politiek*” (Belanda), sehingga “Kebijakan Hukum Pidana” dapat pula di sebut dengan istilah “Politik Hukum Pidana” dan yang sering di kenal dengan istilah “*penal policy*”, “*criminal law policy*” atau “*strafrechtspolitik*”.⁹ Dalam bukunya Barda Nawawi Arief mengutip pendapat dari Marc Ancel yang menyatakan bahwa *Penal Policy* merupakan salah satu komponen dari *Modern Criminal Science* disamping komponen yang lain seperti, “*Criminologi*” dan “*Criminal Law*”.¹⁰ Marc Ancel berpendapat bahwa “*Penal Policy*” ialah:

“suatu ilmu yang memiliki tujuan praktis untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik dan untuk

⁹ Barda Nawawi Arief. (2008). Bunga Rampai Kebijakan Hukum Pidana Perkembangan Konsep KUHP Baru. Cetakan Ke-1, Jakarta: Kencana Prenadamedia Grub, hlm 26;

¹⁰ *Ibid.*, hlm. 23

memberi pedoman tidak hanya kepada pembuat undang-undang, tetapi juga kepada pengadilan yang menerapkan undang-undang dan juga kepada para penyelenggara atau pelaksana putusan pengadilan.”¹¹

Senada dengan Marc Ancel, Prof. Sudarto memberikan pengertian “*Penal Policy*” sebagaimana dikutip oleh Barda Nawawi Arief ialah:

- a. Usaha untuk mewujudkan peraturan-peraturan yang baik sesuai dengan keadaan dan situasi pada suatu saat; ¹²
- b. Kebijakan dari negara melalui badan-badan yang berwenang untuk menetapkan peraturan-peraturan yang dikehendaki yang diperkirakan bisa digunakan untuk mengekspresikan apa yang terkandung dalam masyarakat dan untuk mencapai apa yang dicita-citakan.

Pendapat lainnya berasal dari A. Mulder, “*Strafrechtspolitik* atau *Penal Policy*” ialah garis kebijakan untuk menentukan:

- a. Seberapa jauh ketentuan – ketentuan pidana yang berlaku perlu diubah atau diperbaharui;
- b. Apa yang dapat diperbuat untuk mencegah terjadinya tindak pidana; dan

¹¹ *Ibid.*, hlm. 26;

¹² Sudarto. (1981). *Hukum dan Hukum Pidana*. Bandung: Alumni, hlm. 159;

- c. Cara bagaimana penyidikan, penuntutan, peradilan, dan pelaksanaan pidana harus dilaksanakan.¹³

Dari beberapa pendapat tersebut, maka dapat ditarik kesimpulan bahwa “Kebijakan Hukum Pidana” atau “*Penal Policy*” merupakan suatu peraturan hukum yang dirumuskan dan ditetapkan oleh badan-badan yang berwenang sebagai suatu pedoman (hukum positif) bagi masyarakat maupun penegak hukum yang bertujuan untuk mencegah dan menanggulangi suatu kejahatan atau dengan kata lain suatu tindak pidana. Usaha penanggulangan kejahatan dengan hukum pidana pada hakikatnya juga merupakan bagian dari usaha penegakan hukum (khususnya penegakan hukum pidana), oleh karena itu sering pula dikatakan bahwa kebijakan hukum pidana merupakan bagian pula dari kebijakan penegakan hukum (*law enforcement policy*). Selain bagian dari usaha penegakan hukum, juga merupakan bagian integral dari usaha perlindungan masyarakat (*social welfare*) serta bagian integral dari kebijakan atau politik sosial (*social policy*). Kebijakan sosial (*social policy*) dapat diartikan sebagai usaha yang rasional untuk mencapai kesejahteraan masyarakat dan sekaligus mencakup perlindungan masyarakat, sehingga dalam pengertian “*social policy*” terkandung pula “*social welfare policy*” dan “*social defence policy*”.¹⁴ Secara luas, kebijakan hukum pidana dapat mencakup ruang lingkup kebijakan dibidang hukum pidana materiil,

¹³ Barda Nawawi Arief, *Op. cit.*, hlm 27;

¹⁴ *Ibid.*, hlm. 29-30;

dibidang hukum pidana formal dan dibidang hukum pidana pelaksanaan pidana.

Pada hakekatnya kebijakan untuk membuat peraturan hukum pidana menjadi lebih baik merupakan bagian dari upaya penanggulangan kejahatan. Dengan demikian kebijakan hukum pidana, hakekatnya merupakan bagian dari kebijakan penanggulangan kejahatan (politik kriminal). Dalam perspektif ini (politik kriminal), kebijakan hukum pidana identik dengan pengertian “kebijakan penanggulangan kejahatan dengan hukum pidana”. Oleh karena itu, dengan perkataan yang lain “kebijakan penanggulangan kejahatan dengan hukum pidana” bisa disebut dengan kebijakan kriminalisasi, dimana dalam proses ini (kriminalisasi) menggunakan sarana pidana. Dari sisi tampak bahwa perspektif kebijakan hukum pidana kriminalisasi merupakan bagian dari kebijakan hukum pidana.

B. Kejahatan Dunia Maya (Cyber Crime)

Kriminalisasi cyber crime di Indonesia khususnya dalam UU-ITE dapat dibagi dalam dua kategori, yaitu perbuatan yang menggunakan komputer sebagai sarana kejahatan, dan perbuatanperbuatan yang menjadikan komputer sebagai sasaran kejahatan. Kejahatan yang menggunakan komputer sebagai sarana adalah setiap tindakan yang mendayagunakan data komputer, sistem komputer, dan jaringan komputer sebagai alat untuk melakukan kejahatan di ruang maya bukan ruang nyata. Kejahatan yang

menjadikan komputer sebagai sasaran adalah setiap perbuatan dengan menggunakan komputer yang diarahkan pada data komputer, sistem komputer, atau jaringan komputer, atau ketiganya secara bersama-sama. Perbuatan tersebut dilakukan di ruang maya bukan ruang nyata, sehingga seluruh aktivitas yang dilarang oleh peraturan perundangundangan terjadi di ruang maya¹⁵

2. Definisi Cyber Crime

Istilah *cyber crime* saat ini merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya (*cyber space*) dan tindakan kejahatan yang menggunakan komputer. Ada ahli yang menyamakan antara tindak kejahatan *cyber* (*cyber crime*) dengan tindak kejahatan komputer, dan ada ahli yang membedakan diantara keduanya. Beberapa penggunaan kata untuk merujuk pada *cyber crime* yang umum digunakan dalam berbagai literatur adalah kejahatan dunia maya, kejahatan komputer, kejahatan mayantara, kejahatan dibidang teknologi informasi, dan masih banyak lagi.

Kejahatan komputer atau kejahatan *cyber* atau kejahatan dunia maya (*cybercrime*) adalah sebuah bentuk kriminal yang mana menjadikan internet dan komputer sebagai medium melakukan tindakan kriminal. Masalah yang berkaitan dengan kejahatan jenis ini misalnya hacking, pelanggaran hak cipta,

¹⁵ Widodo, Aspek Hukum Pidana Kejahatan Mayantara, Aswaja Pressindo, Yogyakarta, hlm. 64-66

pornografi anak, dan eksploitasi anak. Juga termasuk pelanggaran terhadap privasi ketika informasi rahasia hilang atau dicuri, dan lainnya.

Dalam definisi lain, kejahatan dunia maya adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit, *confidence fraud*, penipuan identitas, pornografi anak, dan lain-lain. Walaupun kejahatan dunia maya atau *cybercrime* umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional dimana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.¹⁶

Dari definisi diatas, kita bisa mengetahui unsur dari *cyber crime* sebagai berikut :

1. Perbuatan yang bertentangan dengan hukum, etika dan tanpa kewenangan.
2. Menggunakan teknologi tinggi atau digital
3. Dengan teknologi informasi sebagai sasaran atau sarana kejahatan di dunia *cyber*.

¹⁶ Taufan Aditya Pratama. (2019). Pengertian Cyber Crime. Adoc.tips. diakses pada tanggal 23 Oktober 2022

3. Bentuk- Bentuk *Cyber Crime*

Kejahatan dalam dunia maya (*Cyber Crime*) secara sederhana dapat diartikan sebagai jenis kejahatan yang dilakukan dengan mempengaruhi media internet sebagai alat bentuknya. Semakin berkembangnya teknologi dapat dilakukan berbagai macam tindak kejahatan. Adapun macam-macam kejahatan berteknologi dari laporan pihak korban maupun hasil dari identifikasi pakar hukum disesuaikan dan diklasifikasikan dengan undang-undang yang berlaku.¹⁷

Berdasarkan bentuk aktivitas yang dilakukannya, *cyber crime* dapat digolongkan menjadi beberapa bentuk sebagai berikut:

a. *Unauthorized Access to Computer System and Service*

Merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup kedalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. *Probing* dan *port* merupakan contoh kejahatan ini.

b. *Offense Against Intellectual Property.*

Offence Against Intellectual Property yaitu kekayaan yang ditujukan terhadap hak kekayaan intelektual yang dimiliki seseorang di internet. Sebagai contoh adalah peniruan

¹⁷ Dikdik M. Arief Mansur dan Elisatris Gultom. (2005). *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama, hlm. 26.

tampilan web page suatu situs milik orang lain secara illegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

c. *Illegal Contents.*

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

d. *Cyberstalking*

Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya

e. *Denial of Service Attack* atau Serangan DoS

adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

f. *Cybersquatting and Typosquatting*

Cybersquatting merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun *typosquatting* adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain.

g. *Arp spoofing*

Arp spoofing adalah teknik yang cukup populer untuk melakukan penyadapan data, terutama data username/password yang ada di jaringan internal. Intinya adalah dengan mengirimkan paket ARP Reply palsu sehingga merubah data MAC Address: IP yang ada di tabel ARP komputer target. Perubahan data ini menyebabkan pengiriman

paket TCP/IP akan melalui attacker sehingga proses penyesuaian dapat dilakukan.

h. Phishing

Phishing (Indonesia: pengelabuan) adalah suatu bentuk penipuan yang dicirikan dengan percobaan untuk mendapatkan informasi peka, seperti kata sandi dan kartu kredit, dengan menyamar sebagai orang atau bisnis yang terpercaya dalam sebuah komunikasi elektronik resmi, seperti surat elektronik atau pesan instan.

i. *Malware*

Adalah program komputer yang mencari kelemahan dari suatu software. Umumnya *malware* diciptakan untuk membobol atau merusak suatu software atau operating system. *Malware* terdiri dari berbagai macam, yaitu: *virus, worm, trojan horse, adware, browser hijacker, dll.*

j. *Cyber Espionage*

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

k. *Infringements of Privacy*

Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

l. *Data Forgery*

Ini merupakan modus kriminal di dunia maya yang dilakukan dengan memalsukan data dokumen penting yang disimpan sebagai dokumen tanpa kertas melalui internet. kejahatan sejenis ini biasanya menargetkan dokumen e-commerce, seolah-olah ada "typo" yang pada akhirnya akan menguntungkan pelaku, karena korban akan memasukkan data pribadi dan nomor kartu kredit kepada pelaku.

m. *Cyber Sabotage and Extortion*

Merupakan kejahatan yang paling mengesankan. Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

3. Jenis-jenis cyber crime

Berdasarkan motif kegiatan yang dilakukannya, *cybercrime* dapat dibagi menjadi dua jenis sebagai berikut :

1. *Cyber crime* sebagai tindakan murni kriminal

Kejahatan yang murni merupakan tindak kriminal merupakan kejahatan yang dilakukan karena motif kriminalitas. Kejahatan ini biasanya menggunakan internet hanya sebagai sarana kejahatan. Contoh kejahatan semacam ini adalah *carding*, yaitu pencurian nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet. Juga pemanfaatan media internet (*webserver*, *mailing list*) untuk menyebarkan material bajakan. Pengirim e-mail anonim yang berisi promosi (*spamming*) juga dapat dimasukkan dalam contoh kejahatan yang menggunakan internet sebagai sarana. Di beberapa negara maju, pelaku *spamming* dapat dituntut dengan tuduhan pelanggaran privasi.

2. *Cyber crime* sebagai kejahatan "abu-abu"

Cukup sulit menentukan apakah itu merupakan tindak kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk kejahatan. *Probing* atau *portscanning*, misalnya, untuk pengintaian terhadap sistem milik orang lain dengan mengumpulkan informasi sebanyak-banyaknya dari sistem yang diintai, termasuk sistem operasi yang digunakan, *port-port* yang ada, baik yang terbuka maupun tertutup, dan sebagainya.

Berdasarkan sasaran kejahatannya *cybercrime* dapat dikelompokkan menjadi beberapa kategori seperti berikut ini:

1. *Cybercrime* yang menyerang individu (*against person*). Jenis kejahatan ini, sasaran serangannya ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut, contohnya: (a) pornografi, dengan membuat, memasang, mendistribusikan, dan menyebarkan material yang berbau pornografi, cabul, serta mengekspos hal-hal yang tidak pantas; (b) *cyberstalking*, untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya dengan menggunakan e-mail yang dilakukan secara berulang-ulang seperti halnya teror di dunia cyber. Gangguan tersebut bisa saja berbau seksual, religius, dan lain sebagainya; (c) *cyber-tresspass*, dengan yang dilakukan melanggar area privasi orang lain seperti misalnya *web hacking*, *breaking ke PC*, *probing*, *port scanning* dan lain sebagainya.
2. *Cybercrime* menyerang hak milik (*againts property*), yakni *cybercrime* yang dilakukan untuk mengganggu atau menyerang hak milik orang lain. Beberapa contoh kejahatan jenis ini misalnya pengaksesan komputer secara tidak sah melalui dunia cyber, pemilikan informasi elektronik secara tidak sah/pencurian informasi, *carding*, *cybersquatting*, *hijacking*,

data forgery dan segala kegiatan yang bersifat merugikan hak milik orang lain.

3. *Cybercrime* menyerang pemerintah (*againsts government*), ini dilakukan dengan tujuan khusus penyerangan terhadap pemerintah. Kegiatan tersebut misalnya *cyber terrorism* sebagai tindakan yang mengancam pemerintah termasuk juga cracking ke situs resmi pemerintah atau situs militer.

4. Karakteristik *Cyber Crime*

Menurut Abdul Wahid dan M. Labib, cyber crime memiliki beberapa karakteristik, yaitu :¹⁸

1. Perbuatan yang dilakukan secara illegal, tanpa hak atau tindakan etis terjadi diruang/wilayah siber, sehingga tidak dapat dipastikan yuridiksi negara mana yang berlaku terhadapnya;
2. perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang berhubungan dengan internet;
3. perbuatan tersebut mengakibatkan kerugian materiil maupun immateriil yang cenderung lebih besar dibandingkan dengan kejahatan konvensional;
4. pelakunya adalah orang yang menguasai penggunaan internet dan aplikasinya;

¹⁸ Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara (Cyber Crime)*, Jakarta: PT. Refika Aditama, hlm. 76.

5. perbuatan tersebut sering dilakukan secara transnasional.

C. Hukum Pidana

Hukum Pidana adalah keseluruhan dari peraturan-peraturan yang menentukan perbuatan apa yang dilarang dan termasuk ke dalam tindak, serta menentukan hukuman apa yang dapat dijatuhkan terhadap yang melakukannya.

Menurut Prof. Moeljatno, Hukum Pidana adalah bagian daripada keseluruhan hukum yang berlaku di suatu negara, yang mengadakan dasar-dasar dan aturan-aturan untuk:¹⁹

1. Menentukan perbuatan-perbuatan mana yang tidak boleh dilakukan dan yang dilarang, dengan disertai ancaman atau sanksi yang berupa pidana tertentu bagi barang siapa yang melanggar hukum tersebut.
2. Menentukan kapan dan dalam hal-hal apa kepada mereka yang melanggar larangan-larangan itu dapat dikenakan atau dijatuhi pidana sebagaimana yang telah diancamkan.
3. Menentukan dengan cara bagaimana pengenaan pidana itu dapat dilaksanakan apabila ada orang yang disangka telah melanggar larangan tersebut.

Sedangkan menurut Sudarsono, pada prinsipnya Hukum Pidana adalah yang mengatur tentang kejahatan dan pelanggaran

¹⁹ Kamri Ahmad dan Andi Khaedir. Pengantar Ilmu Hukum. Makassar: Umitoha Ukhuwah Grafika, 2019, hlm. 121;

terhadap kepentingan umum dan perbuatan tersebut diancam dengan pidana yang merupakan suatu penderitaan.

Dengan demikian hukum pidana bukanlah mengadakan norma hukum sendiri, melainkan sudah terletak pada norma lain dan sanksi pidana. Diadakan untuk menguatkan ditaatinya norma-norma lain tersebut, misalnya norma agama dan kesusilaan.

D. Tindak Pidana

1. Definisi Tindak Pidana

Pengertian tentang tindak pidana dalam Kitab Undang Undang Hukum Pidana (KUHP) dikenal dengan istilah *Strafbaarfeit* dan dalam kepustakaan tentang hukum pidana sering mempergunakan istilah delik, sedangkan pembuat undang-undang merumuskan suatu undang-undang, mempergunakan istilah peristiwa pidana atau perbuatan pidana atau tindak pidana.²⁰

Para pakar asing hukum pidana menggunakan istilah tindak pidana atau perbuatan pidana atau peristiwa pidana, dengan istilah:

- a. *Strafbaar Feit* adalah peristiwa pidana
- b. *Strafbare Handlung* diterjemahkan dengan Perbuatan Pidana, yang digunakan oleh para sarjana Hukum Pidana Jerman

²⁰ Amir Ilyas. (2012). *Asas-Asas Hukum Pidana Memahami Tindak Pidana Dan Pertanggungjawaban Pidana Sebagai Syarat Pemidanaan (Disertai Teori-Teori Pengantar Dan Beberapa Komentar)*, Yogyakarta: Rangkang Education Yogyakarta & PuKAP-Indonesia, hlm. 18;

- c. *Criminal Act* diterjemahkan dengan istilah Perbuatan Kriminal.

Delik yang dalam bahasa Belanda disebut *Strafaarfeit*, terdiri atas tiga kata, yaitu *straf*, *baar* dan *feit*. Yang memiliki arti:

- a. *Straf* diartikan sebagai pidana dan hukum,
- b. *Baar* diartikan sbagai dapat dan boleh,
- c. *Feit* diartikan sebagai tindak, peristiwa, pelanggaran dan perbuatan.²¹

Lebih lanjut Pompe, mengartikan *Strafaarfeit* sebagai “suatu pelanggaran norma (gangguan terhadap tertib hukum) yang dengan sengaja ataupun dengan tidak sengaja telah dilakukan oleh seorang pelaku, dimana penjatuhan hukuman terhadap pelaku tersebut adalah perlu demi terpeliharanya tertib hukum”.²² Selanjutnya terdapat Simons, merumuskan *strafaarfeit*, sebagai “suatu tindakan melanggar hukum yang telah dilakukan dengan sengaja oleh seseorang yang dapat dipertanggungjawabkan atas tindakannya dan yang oleh undang-undang telah dinyatakan sebagai suatu tindakan yang dapat dihukum”.

Sedangkan Jonkers, merumuskan *Strafaarfeit* sebagai peristiwa pidana yang diartikannya sebagai suatu perbuatan yang melawan hukum (*wederrechtelijk*) yang berhubungan dengan

²¹ *Ibid.*, hlm. 18-19;

²² *Ibid.*, hlm. 34;

kesengajaan atau kesalahan yang dilakukan oleh orang yang dapat dipertanggungjawabkan.²³

Selain ahli hukum pidana dari manca negara, ahli hukum pidana dari Indonesia juga tidak ketinggalan untuk ambil bagian dalam mendefinisikan pengertian *Strafaarfeit*, seperti Moeljatno, yang mengartikan *Strafaarfeit* sebagai perbuatan pidana, dan mendefinisikan perbuatan pidana tersebut sebagai “suatu kelakuan manusia yang diancam pidana oleh peraturan perundang-undangan”.²⁴

Lebih lanjut Moeljatno, menjelaskan bahwa tindak pidana adalah suatu perbuatan yang memiliki unsur dan dua sifat yang berkaitan, unsur-unsur yang dapat dibagi menjadi dua macam, yaitu:

- a. Subyektif adalah berhubungan dengan diri sipelaku dan termasuk ke dalamnya yaitu segala sesuatu yang terkandung dihatinya.
- b. Obyektif adalah unsur-unsur yang melekat pada diri sipelaku atau yang ada hubungannya dengan keadaan-keadaannya, yaitu dalam keadaan-keadaan mana tindakan-tindakan dari sipelaku itu harus dilakukan.²⁵

²³ Adami Chazawi. (2013). Pelajaran Hukum Pidana, Bagian 1: Stelsel Pidana, Teori-Teori Pidana & Batas Berlakunya Hukum Pidana. Jakarta: Raja Grafindo, hlm. 75

²⁴ Ibid., hlm. 72

²⁵ Moeljatno. (1993). Azas-Azas Hukum Pidana. Jakarta: Rineka Cipta, hlm. 69

Selanjutnya Andi Hamzah, dalam bukunya Asas-Asas Hukum Pidana, menyebut “*Strafbaarfeit*” sebagai delik, memberikan definisi yakni suatu perbuatan atau tindakan yang terlarang dan diancam dengan hukuman oleh undang-undang (pidana).²⁶ Selanjutnya S.R. Sianturi, memberikan perumusan mengenai tindak pidana sebagai berikut, “Tindak pidana adalah sebagai suatu tindakan pada, tempat, waktu dan keadaan tertentu yang dilarang (atau diharuskan) dan diancam dengan pidana oleh undang-undang bersifat melawan hukum, serta dengan kesalahan di lakukan oleh seseorang (yang bertanggung jawab)”.²⁷

Dari penjelasan di atas, dapat dipahami bahwa tindak pidana merupakan terjemahan dari *Strafaarfeit*, meskipun demikian terdapat banyak istilah lain yang digunakan untuk memberikan gambaran mengenai tindak pidana tersebut seperti perbuatan pidana maupun delik pidana. Sedangkan mengenai pengertian *Strafaarfeit* dapat diartikan sebagai peristiwa yang dapat dipidana atau perbuatan yang dapat dipidana, sedangkan delik dalam bahasa asing disebut *delict* yang artinya suatu perbuatan yang pelakunya dapat dikenakan hukuman (pidana). Jadi yang dimaksud dengan tindak pidana adalah suatu perbuatan yang dilarang dalam ketentuan perundang-undangan dan dari perbuatan tersebut dapat dijatuhi pidana

²⁶ Andi Hamzah. (1994). Asas-Asas Hukum Pidana, Jakarta: Rineka Cipta, hlm, 72 - 88.

²⁷ S. R. Sianturi. (1982). Asas-Asas Hukum Pidana di Indonesia dan Penerapannya. Jakarta: Alumni. hlm. 207.

2. Unsur-unsur Tindak Pidana

Unsur-unsur tindak pidana dapat dibedakan setidaknya dari dua sudut pandang, yaitu (1) dari sudut pandang teoritis dan (2) dari sudut pandang Undang-undang. Maksud teoritis adalah berdasarkan pendapat ahli hukum, yang tercermin dari pada rumusannya. Sedangkan sudut Undang-undang adalah kenyataan tindak pidana itu dirumuskan menjadi tindak pidana tertentu dalam Pasal-pasal perundang-undangan yang ada.²⁸

a. Unsur-unsur tindak pidana menurut beberapa teoritis

Berdasarkan rumusan tindak pidana menurut Moeljatno, maka unsur tindak pidana adalah perbuatan, yang dilarang (oleh aturan hukum), ancaman pidana (bagi yang melanggar larangan). Dari batasan yang dibuat Jonkers dapat dirincikan unsur-unsur tindak pidana adalah perbuatan, melawan hukum (yang berhubungan dengan), kesalahan (yang dilakukan oleh orang yang dapat), dipertanggungjawabkan. E.Y.Kanter dan SR. Sianturi menyusun unsur-unsur tindak pidana yaitu:²⁹

Ke-1 Subjek

Ke-2 Kesalahan

Ke-3 Bersifat melawan hukum (dari tindakan)

²⁸ Adami Chazawi. (2002). Pelajaran Hukum Pidana II. Jakarta: Rajawali Pers, hlm. 78.

²⁹ E.Y. Kanter. (1992). Azas-azas Hukum Pidana di Indonesia dan Penerapannya. Jakarta: Alumni AHMPH, hlm. 211

Ke-4 Suatu tindakan yang dilarang dan diharuskan oleh UU/PerUU-an dan terhadap pelanggarannya diancam dengan pidana

Ke-5 Waktu, tempat, keadaan (unsure bjektif lainnya).

Sementara K. Wantjik Saleh menyimpulkan bahwa suatu perbuatan akan menjadi tindak pidana apabila perbuatan itu:³⁰

1. Melawan hukum
2. Merugikan masyarakat
3. Dilarang oleh aturan pidana
4. Pelakunya diancam dengan pidana.

Perumusan Simons mengenai tindak pidana, menunjukan unsur-unsur tindak pidana sebagai berikut:³¹

1. *Handeling*, perbuatan manusia, dengan *hendeling* dimaksudkan tidak saja *eendoen* (perbuatan) tetapi juga “*een naitalen*” atau “*niet doen*” (melalaikan atau tidak berbuat)
2. Perbuatan manusia itu harus melawan hukum (*wederrechtelijk*)
3. Perbuatan itu diancam pidana (*Strafbaarfeit Gesteld*) oleh UU

³⁰ K. Wantjik Saleh, (1998) Kehakiman dan Keadilan. Jakarta: Ghalia Indonesia.

³¹ Mustafa Abdullah dan Ruben Achmad. (1983). Intisari Hukum Pidana. Jakarta: Ghalia Indonesia, hlm. 26-27

4. Harus dilakukan oleh seseorang yang mampu bertanggung jawab (*toerekeningsvatbaar*).
 5. Perbuatan itu harus terjadi karena kesalahan.
- b. Unsur rumusan Tindak Pidana dalam Undang-undang

Buku II KUHP memuat rumusan-rumusan perihal tindak pidana tertentu yang masuk dalam kelompok kejahatan dan Buku III adalah pelanggaran. Ternyata ada unsur yang selalu disebutkan dalam setiap rumusan ialah tingkah laku/perbuatan, walaupun ada pengecualian seperti Pasal 335 KUHP. Unsur kesalahan dan melawan hukum terkadang dicantumkan dan seringkali juga tidak dicantumkan. Sama sekali tidak dicantumkan ialah mengenai unsur kemampuan bertanggungjawab. Disamping itu banyak mencantumkan unsur-unsur lain baik sekitar/mengenai objek kejahatan maupun perbuatan secara khusus untuk rumusan tertentu.

Dari rumusan-rumusan tindak pidana tertentu dalam KUHP, maka dapat diketahui adanya delapan unsur tindak pidana, yaitu:

1. Unsur tingkah laku
2. Unsur melawan hukum
3. Unsur kesalahan
4. Unsur akibat konstitutif
5. Unsur keadaan yang menyertai

6. Unsur syarat tambahan untuk dapatnya dituntut pidana
 7. Unsur syarat tambahan untuk memperberat pidana
 8. Unsur syarat tambahan untuk dapat dipidana.
3. Penyebab Terjadinya Tindak Pidana

Dalam KUHP, tindak pidana terbagi dua, yakni untuk semua yang dimuat dalam Buku II, dan pelanggaran untuk semua yang terdapat dalam Buku III. Sehingga tindak pidana merupakan bentuk kejahatan.

Faktor-faktor sosial yang dianggap mempunyai pengaruh terhadap terjadinya suatu pidana, dapat dikategorikan sebagai berikut:³²

1. Faktor ekonomi, meliputi sistem ekonomi, yang tidak saja merupakan sebab utama (*basic causa*) dari terjadinya kejahatan terhadap hak milik, juga mempunyai pengaruh *kriminogenik* karena membangun *egoisme* terhadap macam-macam kejahatan lain dengan cara pola hidup konsumeristis, dan persaingan pemenuhan kebutuhan hidup, perubahan harga pasar, yang mempengaruhi tingkat pencurian, keadaan krisis, pengangguran
2. Faktor-faktor mental, meliputi kurangnya pemahaman terhadap agama, pengaruh bencana, film dan televisi

³² Stepen Huwitz dan Saduran Moeljatno. (1986). Kriminologi. Jakarta: Bina Aksara, hlm. 86

3. Faktor-faktor fisik, keadaan iklim, seperti hawa panas/dingin, keadaan terang/gelap, dan lain-lain dianggap sebagai penyebab langsung dari kelakuan manusia yang menyimpang dan khususnya kejahatan kekerasan berkurang semakin basah dan panas iklimnya
4. Faktor-faktor pribadi, meliputi umur, jenis kelamin, ras dan nasionalitas, alkoholisme, dan perang berakibat buruk bagi kehidupan manusia.

Secara umum dapat diklasifikasikan hal yang dapat menjadi pemicu terjadi tindak pidana, antara lain:

- a. Keadaan ekonomi yang lemah dan pengangguran
- b. Lemahnya penegakan hukum, dalam hal ini mencakup lemahnya dari sanksi perundang-undangan pidana, dan tidak terpadunya sistem peradilan pidana
- c. Adanya *demonstration effects*, yaitu kecenderungan masyarakat untuk memamerkan kekayaan sehingga menyulut pola hidup konsumtif yang berlomba-lomba mengejar nilai lebih sedangkan kesanggupan rendah
- d. Perilaku korban yang turut mendukung sehingga terjadinya tindak pidana
- e. Lingkungan keluarga yang tidak harmonis dan pergaulan dengan masyarakat yang berintegrasi dengan pola-pola kejahatan dalam masyarakat tentang

- f. Kurangnya pendidikan moral
- g. Penyakit kejiwaan.

Sementara secara sederhana, dalam dunia kriminalitas dikenal dua faktor penting terjadi tindak pidana, yaitu niat dan kesempatan. Kedua faktor saling mempengaruhi dan harus ada untuk terjadinya tindak pidana.

BAB III

METODE PENELITIAN

Adapun Metode Penelitian yang digunakan adalah sebagai berikut :

A. Tipe Penelitian

Tipe penelitian ini termasuk kategori penelitian hukum normatif. Penelitian hukum normatif adalah metode atau cara yang dipergunakan di dalam penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka yang tersedia.

B. Pendekatan Penelitian

Dalam penelitian ini, penulis menggunakan beberapa pendekatan penelitian. Melalui pendekatan tersebut maka penulis akan mendapatkan informasi dari berbagai aspek mengenai permasalahan yang penulis coba untuk diteliti. Pendekatan-pendekatan yang dimaksud antara lain:

1. Pendekatan Perundang-undangan

Pendekatan Perundang-undangan ini dilakukan dengan melakukan pengkajian terhadap Pasal Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik j.o Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), KUHP serta Peraturan yang relevan.

2. Pendekatan Perbandingan

Merupakan pendekatan dengan cara melihat praktik hukum yang ada di masyarakat dan mempelajari penerapan norma dan kaidah yang berlaku. Dengan mengangkat suatu kasus atau peristiwa yang terjadi pada kenyataan yang berhubungan dengan penelitian dan melihat serta mengkajinya dengan lebih seksama dan membandingkannya dengan literatur atau jurnal yang telah ada

C. Sumber Bahan Hukum

Data yang terkumpul merupakan data kualitatif dimana datanya dinyatakan dalam keadaan yang sewajarnya data yang digunakan dalam penelitian ini

1. Data Sekunder merupakan sejumlah data yang diperoleh melalui pustaka yang meliputi buku-buku, artikel, dan dokumen-dokumen serta internet yang berkaitan dengan objek penelitian. Data sekunder dapat dibedakan menjadi:

- a. Bahan Hukum Primer

Bahan hukum primer yaitu bahan-bahan hukum yang mengikat dan terdiri dari:

- a) Undang-Undang Negara Republik Indonesia 1945
- b) Kitab Undang-Undang Hukum Pidana
- c) Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

d) Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Tansaksi Elektronik.

b. Bahan Hukum Sekunder

Adapun data yang penulis jadikan sebagai sumber data sekunder adalah macam-macam buku yang relevan dengan penelitian ini bermacam-macam jurnal yang berkaitan dengan penelitian ini, termasuk dokumen-dokumen yang berkaitan dengan pembahasan dalam penelitian ini.

c. Bahan Hukum Tersier

Bahan hukum tersier yaitu bahan hukum yang merupakan pelengkap yang bersifat memberikan petunjuk atau penjelasan tambahan terhadap bahan hukum primer dan sekunder. Bahan hukum tersier yang terdapat dalam penelitian misalnya Kamus Besar Bahasa Indonesia, Kamus Inggris-Indonesia

D. Teknik Pengumpulan Bahan Hukum

Bahan Hukum dikumpulkan melalui prosedur identifikasi peraturan perundang-undangan, serta klasifikasi dan sistematisasi bahan hukum sesuai permasalahan penelitian. Oleh karena itu, teknik pengumpulan bahan hukum yang digunakan dalam penelitian ini adalah dengan cara membaca, menelaah, mencatat, membuat ulasan bahan-bahan pustaka, maupun penelusuran melalui media internet yang ada kaitannya dengan judul penelitian.

E. Analisis Bahan Hukum

Data yang diperoleh dari penelitian akan dianalisis secara kualitatif dan disajikan secara deskripsi yaitu menjelaskan menguraikan dan menggambarkan sesuai dengan permasalahan yang erat kaitannya dengan penelitian ini, kemudian menarik suatu kesimpulan berdasarkan analisis yang telah dilakukan. Dimana penelitian ini nantinya akan memberikan gambaran secara jelas dan tepat perihal Pengaturan *Cyber Crime* di dalam sistem hukum pidana di Indonesia.

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

A. Tindakan Kejahatan Dunia Maya (*Cybercrime*) yang dapat disebut sebagai Tindak Pidana

Cybercrime mempunyai bentuk beragam, karena setiap negara tidak selalu sama dalam melakukan kriminalisasi. Begitu pula, dalam setiap negara dalam menyebut apakah suatu perbuatan tergolong kejahatan *cybercrime* atau bukan kejahatan *cybercrime* juga belum tentu sama. Secara teoritik, berkaitan dengan konsepsi kejahatan. Muladi mengemukakan bahwa *asas mala in se* mengajarkan bahwa suatu perbuatan dikategorikan sebagai kejahatan karena masyarakat dengan sendirinya menganggap perbuatan tersebut jahat. Sedangkan berdasarkan *asas mala prohibita*, suatu perbuatan dianggap jahat karena melanggar peraturan perundang-undangan.³³ *Asas Mala Prohibita* menghasilkan konsepsi kejahatan dalam arti yuridis (yaitu sebagaimana diatur dalam peraturan perundang-undangan tertulis).

Jonathan Rosenoer menjelaskan tentang bentuk-bentuk *cybercrime* sebagai berikut:

1. *Copyright, include exclusive right, subject matter of copyright, formalities, infringement, source of risk, word wide web sites, hypertext link, graphical element, e-mail, criminal liability, fair use, first amandment, and software rental.*
2. *Trademark*
3. *Defamation*

³³ Muladi, 2002, Demokratisasi , Hak Asasi Manusia, dan Reformasi Hukum di Indonesia, Jakarta, Habibie Center, hlm. 196

4. *Privacy, include common law privacy, constitutinal law, anonymity, and technology expanding privacy right.*
5. *Duty of care*
 - a. *Negligence*
 - b. *Negligent misstatement*
 - c. *Equipment malfunctions*
 - d. *Economic loss may not be recoverable*
 - e. *Contractual limitations of liability.*
6. *Criminal liability; such as; computer fraud and abuse act, wire fraud. Electronic communication privacy act, extortion and threats, expose, sexual exploitation of children, obscene and indent telephone call, copyright stalking.*
7. *Procedural issues, include jurisdiction, venue and conflict of law.*
8. *Electronic contract and digital signature, include electronic agreement enforceable, public key encryption and digital signature.³⁴*

Cybercrime meliputi pelanggaran hak kekayaan intelektual, fitnah atau pencemaran nama baik, pelanggaran terhadap kebebasan pribadi (*privacy*), ancaman dan pemerasan, eksploitasi seksual anak-anak dan pencabulan, kerusakan sistem komputer, pembobolan kode akses, dan pemalsuan tanda tangan digital. Semua perbuatan tersebut dapat dipertanggungjawabkan secara pidana sesuai dengan yurisdiksinya. *Cybercrime* juga dapat berbentuk pemalsuan data, penyebaran virus komputer ke jaringan komputer atau sistem komputer, penambahan atau pengurangan sistem instruksi dalam jaringan komputer, pembulatan angka, kerusakan data, dan pembocoran data rahasia. Ini diuraikan oleh Sue Titus Reid, bahwa

³⁴ Jonathan Rosenoer, 1997, *Cyberlaw: The Law of the Internet*, New York, SpringVerlag, hlm. 45.

cybercrime meliputi “*data diddling, the Trojan horse, the salami technique, superzapping, and date leakage.*”³⁵

The International Hendbook on Computer Crime mengklasifikasikan bentuk-bentuk *cybercrime* sebagai berikut.

1. *Computer-related Economic Crimes*
 - a. *Fraud by Computer Manipulation*
 - b. *Computer Espionage and Software Piracy*
 - c. *Computer Sabotage*
 - d. *Theft of Services*
 - e. *Unauthorized Access to DP Systems and Hacking*
 - f. *The Computer as a Tool for traditional Business Offences*
2. *Computer-related Infringements of Privacy*
 - a. *Use of Incorrect Data*
 - b. *Illegal Collection and Storage of Correct Data*
 - c. *Illegal Disclosure and Misuse of data*
 - d. *Infringements of Formalities of Privacy Laws*
3. *Further Abuses*
 - a. *Offences Against State and Political Interests*
 - b. *The Extension to Offences Against Personal Intergity.*³⁶

Berdasarkan uraian *Handbook on Computer Crime*, *cybercrime* dikategorikan menjadi tiga. Kategori pertama, *cybercrime* adalah kejahatan ekonomi yang terkait dengan komputer, meliputi penipuan dengan manipulasi komputer, pembajakan perangkat lunak komputer, spionase komputer, sabotase, pencurian jasa, akses tidak sah ke dalam sistem atau jaringan komputer, komputer sebagai alat untuk menyerang bisnis tradisional. Kategori ke dua, adalah pelanggaran terhadap keleluasaan pribadi, yaitu penggunaan data yang tidak benar, pengumpulan data secara tidak sah, penyalahgunaan data,

³⁵ Sue Titus Reid, 1985, *Crime and Criminology*, New York, CBS College Publishing, hlm. 56

³⁶ *Ibid.*,

pelanggaran rahasia perusahaan. Sedangkan kategori ke tiga, misalnya melakukan penyerangan terhadap dan kepentingan politik, dan penyerangan terhadap kebebasan pribadi orang per orang.

Selain penggolongan *cybercrime* sebagaimana terjabar di atas, Donn Parker mengklasifikasikan bentuk-bentuk *cybercrime* ke dalam empat klarifikasi berikut.

1. Komputer sebagai Objek

Dalam kategori ini, bentuk-bentuk *cybercrime* termasuk kasus-kasus kerusakan terhadap komputer, data atau program yang terdapat di dalamnya atau kerusakan terhadap sarana-sarana komputer seperti *Air Condutouring* (AC) dan peralatan yang menunjang pengoprasian komputer.

2. Komputer sebagai Subjek

Komputer dapat pula menimbulkan tempat atau lingkungan untuk melakukan kejahatan, misalnya pencurian, penipuan, dan pemalsuan yang menyangkut harta benda dalam bentuk baru yang tidak dapat disentuh (*intangible*), misalnya pulsa elektronik dan guratan-guratan magnetis.

3. Komputer sebagai Alat

Komputer digunakan sebagai alat melakukan kejahatan sehingga sifat peristiwa kejahatan tersebut adalah sangat kompleks dan sulit diketahui. Salah satu contoh adalah seseorang pelaku kejahatan yang mengambil warkat-warkat setoran dari suatu

bank dan menulis nomor rekening pelaku dengan tinta magnetis pada warkat-warkat tersebut kemudian meletakkan kembali ke tempat semula. Nasabah yang akan memasukkan uang akan mengambil dan mengisi warkat yang sudah dibubuhi nomor rekening pelaku kejahatan memproses warkat-warkat nasabah, komputer secara otomatis akan mengredit sejumlah uang pada rekening pelaku kejahatan. Selain itu, pelaku kejahatan menarik uang dengan cek dari rekeningnya sebelum peram nasabah yang menyeter mengajukan complain ke bank.

4. Komputer sebagai simbol

Suatu komputer dapat digunakan sebagai simbol untuk melakukan penipuan atau ancaman, dalam kategori ini termasuk penipuan “Biro Jodoh” yang menyatakan bahwa biro jodoh tersebut memakai komputer untuk membantu si koraban mencari jodoh, akan tetapi ternyata birojodoh tersebut sama sekali tidak memakai komputer untuk keperluan tersebut.

Kejahatan yang berhubungan dengan komputer (*cybercrime*) sudah diatur oleh instrumen internasional. Satu-satunya instrument internasional yang mengatur kejahatan yang berhubungan dengan komputer adalah *Convention on Cybercrime*. Dalam Bab II konvensi tersebut diatur tentang hukum pidana substantive, yaitu sebagaimana terjabar dalam Pasal (*article*) 2 sampai dengan Pasal 11. Sedangkan

Pasal 12-13 mengatur mengenai ketentuan pidana. Ketentuan tersebut adalah sebagai berikut :

1. *Title 1, offences against the confidentiality, integrity and availability of computer data and system.*
 - a. *Illegal access (article 2);*
 - b. *Illegal interception (article 3);*
 - c. *Data interference,*
 - d. *Damaging, deleting, deterioration, alteration or suppression of computer data without right (article 4);*
 - e. *System interference (article 5);*
 - f. *Misuse of devices (access code) (article 6).*
2. *Title 2, Computer Related Offences:*
 - a. *Computer related forgery (article 7);*
 - b. *Computer related fraud (article 8).*
3. *Title 3, Content Related Offences:*
4. *Title 4, Offences Related to Infringement of Copyright and Related Right (article 10).*
5. *Title 5, Ancillary liability and sanction (article 11); (article 12, (article 13).*

Berdasarkan ringkasan ketentuan dalam Convention on Cybercrime dapat dipahami bahwa dalam bagian 1, Pelanggaran terhadap kerahasiaan, ketersediaan dan integritas sistem dan data komputer, terdiri atas perbuatan berikut:

1. Akses tidak sah, yaitu sengaja memasuki atau mengakses komputer tanpa hak (Pasal 2);
2. Intersepsi tidak sah, yaitu sengaja dan tanpa hak mendengar atau menangkap secara diam-diam pengiriman transmisi dan pemancaran (emisi) data komputer yang tidak bersifat public ke, dari atau di dalam sistem komputer dengan menggunakan alat bnatu teknis (Pasal 3);

3. Gangguan atau perusakan data, yaitu sengaja dan tanpa hak melakukan perusakan.
4. Penghapusan, perubahan atau penghapusan data komputer (Pasal 4);
5. Gangguan atau perusakan sistem, yaitu sengaja melakukan gangguan atau rintangan secara serius tanpa hak terhadap berfungsinya sistem komputer (Pasal 5);
6. Penyalahgunaan peralatan, yaitu penyalahgunaan perlengkapan komputer, termasuk program komputer, komputer, *password* kode masuk (*access code*) (Pasal 6).

Kemudian dalam bagian 2, diatur tentang pelanggaran yang berhubungan dengan komputer, yaitu dalam bentuk berikut:

1. Pemalsuan yang berhubungan dengan komputer (Pasal 7), yaitu pemalsuan (dengan sengaja dan tanpa hak memasukkan, mengubah, menghapus data otentik menjadi tidak otentik dengan maksud untuk digunakan sebagai data otentik);
2. Penipuan yang berhubungan dengan komputer (Pasal 8), yaitu penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang atau kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data komputer, atau dengan mengganggu berfungsinya komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain).

Selanjutnya dalam bagian 3 tentang Pelanggaran yang berhubungan dengan isi, yaitu berkaitan dengan delik-delik yang berhubungan dengan pornografi anak (Pasal 9), yaitu meliputi perbuatan:

1. Memproduksi dengan tujuan mendistribusikan melalui sistem komputer;
2. Menawarkan melalui sistem komputer;
3. Mendistribusikan atau mengirim melalui sistem komputer;
4. Memperoleh melalui sistem komputer;
5. Memiliki dalam sistem komputer atau di dalam media penyimpanan data.

Akhirnya dalam bagian 4 tentang Pelanggaran yang berhubungan dengan Hak Cipta (Pasal 10), yaitu delik-delik yang terkait dengan pelanggaran hak cipta. Sedangkan pada bagian 5, diatur tentang pertanggungjawaban pidana dan sanksi; Percobaan dan Pembantuan (Pasal 11); Pertanggungjawaban Korporasi (Pasal 12); Sanksi dan tindakan (Pasal 13).

Berdasarkan ketentuan-ketentuan dalam konvensi tersebut dapat disimpulkan bahwa delik-delik *cybercrime* sudah diatur secara umum dalam konvensi. Meskipun demikian, setiap Negara diberi peluang untuk mengembangkan dan mengharmonisasikan dengan kebutuhan Negara yang bersangkutan tanpa mengesampingkan kepentingan masyarakat internasional. Karena itu, bahasa yang

digunakan bersifat netral, dan bentuk-bentuk kejahatan yang diatur dalam konvensi adalah ketentuan setandar minimum

B. Kebijakan Tindak Pidana Kejahatan Dunia Maya di Indonesia

- a. Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi,
Dalam undang-undang tersebut terdapat beberapa pasal yang mengatur perbuatan yang dilarang yang termasuk tindak pidana *cybercrime*. Sebelum ada Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, undang-undang ini yang digunakan untuk mengancam pidana bagi perbuatan yang dikategorikan dalam tindak pidana *cybercrime*. Namun undang-undang ini hanya mengatur beberapa tindak pidana yang termasuk tindak pidana *cybercrime* yang masih bersifat umum dan luas, dan hanya berkaitan dengan telekomunikasi, sehingga belum dapat mengakomodir tindak-tindak pidana yang berkaitan dengan komputer.

“Pasal 22 yang berbunyi: “Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi :

- 1) Akses ke jaringan telekomunikasi; dan atau
- 2) Akses ke jasa telekomunikasi; dan atau
- 3) Akses ke jaringan telekomunikasi khusus.”

“Pasal 38 yang berbunyi : “Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi”

“Pasal 40 yang berbunyi : “Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun”

Bentuk-bentuk tindak pidana *cybercrime* dalam Undang-undang Nomor 36 tahun 1999 tentang Telekomunikasi adalah Akses Illegal yakni tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi, menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi dan penyadapan informasi melalui jaringan telekomunikasi. Hal ini merujuk pada pengertian *cybercrime* yang diberikan oleh Konferensi PBB yang menyatakan *cybercrime* adalah perbuatan yang tidak sah yang menjadikan komputer atau jaringan komputer, baik pada sistem keamanannya. Telekomunikasi merupakan salah satu bentuk jaringan dan sistem komputer sehingga perbuatan yang dilarang dalam pasal pasal tersebut dapat dikategorikan menjadi tindak pidana *cybercrime*.

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

Tanggal 23 April 2008 telah diundangkan Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Undang-undang ini bukanlah undang-undang tindak pidana khusus, melainkan juga memuat tentang pengaturan mengenai pengelolaan informasi dan transaksi elektronik dengan tujuan pembangunan, namun undang-undang ini juga mengantisipasi

pengaruh buruk dari pemanfaatan kemajuan teknologi ITE tersebut, yakni dengan diaturnya hukum pidana khususnya tentang tindak pidana yang menyerang kepentingan hukum orang pribadi, masyarakat, atau kepentingan hukum Negara dengan memanfaatkan kemajuan teknologi ITE, atau sering disebut tindak pidana *cybercrime*.

Cybercrime merupakan suatu kejahatan dengan memanfaatkan sarana teknologi informasi dengan memanfaatkan adanya celah keamanan serta ketidakhatihatian calon korban. *Cybercrime* diatur di dalam UU ITE³⁷

UU ITE telah menetapkan perbuatan-perbuatan mana yang termasuk tindak pidana di bidang ITE (*cybercrime*) dan telah ditentukan unsur-unsur tindak pidana dan penyerangan terhadap berbagai kepentingan hukum dalam bentuk rumusan-rumusan tindak pidana tertentu. Tindak Pidana *Cybercrime* dalam UU ITE diatur dalam 9 pasal, dari pasal 27 sampai dengan pasal 35. Dalam 9 pasal tersebut dirumuskan 20 bentuk atau jenis tindak pidana ITE. Pasal 36 tidak merumuskan bentuk tindak pidana ITE tertentu, melainkan merumuskan tentang dasar pemberatan pidana yang diletakkan pada akibat merugikan orang lain pada tindak pidana yang diatur dalam Pasal 27 samapai dengan Pasal 34. Sementara ancaman pidananya ditentukan didalam Pasal 45

³⁷ Arifah, D. A. (2011). Kasus cybercrime di indonesia. Jurnal Bisnis Dan Ekonomi, 18(2), 186.

sampai Pasal 52. Adapun rumusan pasal-pasal tersebut adalah sebagai berikut:

“Pasal 27 yang berbunyi :

- 1) 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 yang melanggar kesusilaan.
- 2) 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.
- 3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
- 4) 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 pemerasan dan/atau pengancaman.

“Pasal 28 yang berbunyi:

- 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 yang ditujukan untuk menimbulkan rasa

kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA).”

“Pasal 29 yang berbunyi:

“Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.”

“Pasal 30 yang berbunyi:

- 1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
- 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 apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.”

“Pasal 31 yang berbunyi:

- 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.

- 2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.
- 3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.
- 4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.”

“Pasal 32 yang berbunyi:

- 1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik 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 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 33 yang berbunyi:

“Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.”

“Pasal 34 yang berbunyi:

- 1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
 - a) perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33
 - b) sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33
- 2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.”

“Pasal 35 yang berbunyi:

“Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.”

“Pasal 36 yang berbunyi:

“Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.”

“Pasal 37 yang berbunyi:

“Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.”

Dari uraian rumusan pasal-pasal bentuk-bentuk tindak pidana *Cybercrime* menurut Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dapat diklasifikasikan menjadi 2 bentuk yakni:

- 1) *Cybercrime* yang menggunakan komputer sebagai alat kejahatan, yakni Pornografi Online (*Cyber-Porno*), Perjudian Online, Pencemaran nama baik melalui media sosial, penipuan melalui komputer, pemalsuan melalui komputer, pemerasan dan pengancaman melalui komputer,

penyebaran berita bohong melalui komputer, pelanggaran terhadap hak cipta, *cyber terrorism*

2) *Cybercrime* yang berkaitan dengan komputer, jaringan sebagai sasaran untuk melakukan kejahatan, yakni akses tidak sah (*illegal acces*), mengganggu sistem komputer dan data komputer, penyadapan atau intersepsi tidak sah, pencurian data, dan menyalahgunakan peralatan komputer.

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

Perbuatan yang dilarang dalam Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik sama dengan perbuatan yang dilarang dengan Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik tidak ada penambahan maupun pengurangan tindak pidana tersebut yang diancam pemidanaannya, sehingga bentuk-bentuk *cybercrime* masih sama dengan undang-undang sebelumnya.

d. Kebijakan *cybercrime* 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 itu dapat dikenakan atau dijatuhi pidana sebagaimana yang telah diancamkan, menentukan dengan cara bagaimana pengenaan 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 *cybercrime* .Rancangan undang undang tersebut sudah ada sejak tahun 2000 dan revisi terakhir dari 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 *cybercrime*, 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 *cybercrime*.

Kebijakan kriminalisasi *Cybercrime* (CC) dalam Rancangan Undang- Undang Pemanfaatan Teknologi Informasi (RUU-PTI) tertuang dalam Bab XIV yang berjudul “Ketentuan Pidana” mulai Pasal 35-40. Undang-Undang Pemanfaatan Teknologi Informasi (RUU-PTI) pada intinya memuat perumusan tindak pidana seperti apa yang terdapat dalam Konvensi *Cybercrime* Dewan Eropa (*Council of Europe Cybercrime Convention*) 2001 yaitu:³⁵

Pasal 35:

- Memuat Perumusan delik mengenai “penggunaan nama domain yang bertentangan dengan Hak Kekayaan Intelektual milik orang lain”;
- Dalam Konvensi *Cybercrime*, delik serupa ini termasuk “*infringement of copyright*”.

Pasal 36:

- Memuat perumusan delik mengenai “mengakses data komputer/mediaelektronik lainnya secara melawan hukum”;
- Dalam Konvensi *Cybercrime*, delik ini disebut dengan istilah “*illegal access*”.

Pasal 37:

- Ayat (1) memuat perumusan delik mengenai perbuatan “menahan atau mengintersepsi pengiriman data melalui

komputer/media elektronik lainnya secara melawan hukum”; dan ayat (2)-nya memuat perumusan delik mengenai perbuatan. “mengintersepsi secara melawan hukum pengiriman data melalui komputer/media elektronik yang menghambat komunikasi dalam sistem komputer/jaringan komputer/sistem komunikasi lainnya”;

- Dalam Konvensi *Cybercrime*, delik dalam Pasal 37 di atas, disebut “*illegal interception*” untuk ayat (1) dan termasuk “*interference system*” untuk ayat (2)

Pasal 38:

- Ayat (1) memuat perumusan delik mengenai perbuatan “memasukkan, mengubah, menambah, menghapus atau merusak data komputer/program komputer/data elektronik lainnya secara melawan hukum”. Delik pada ayat (1) itu diperberat ancaman pidananya apabila “mengakibatkan kerugian ekonomi bagi orang lain” ayat (2) dan “mengakibatkan terganggunya fungsi sistem komputer atau sistem media elektronik lainnya ayat (3);
- Dalam Konvensi *Cybercrime*, delik dalam ayat (1) dan ayat (2) tergolong “*data interference*” dan ayat (3) termasuk “*system interference*”.

Pasal 39:

- Memuat perumusan delik mengenai penggunaan kartu kredit/alat pembayaran elektronik lainnya milik orang lain secara melawan hukum dalam transaksi elektronik.
- Delik ini dalam Konvensi *Cybercrime* termasuk “*computer related offences*”, khususnya “*computer related fraud*”.

Pasal 40:

- Ayat (1) memuat ketentuan mengenai perbuatan “membuat, menyediakan, mengirimkan, mendistribusikan, data/ tulisan/

gambar/ rekaman yang isinya melanggar kesusilaan dengan menggunakan komputer/media elektronik lainnya”. Delik pada ayat (1) diperberat ancaman pidananya dalam ayat (2) apabila objeknya adalah anak.

- Dalam Konvensi *Cybercrime*, hanya disebutkan adanya “*child pornography*” seperti pada ayat (2) di atas.

Tindak pidana di atas Pasal 35-40 diancam dengan pidana penjara (maksimumnya berkisar antara 1 (satu) sampai dengan 5 (lima) tahun dan/atau pidana denda (maksimumnya berkisar antara Rp. 100.000.000,00 (seratus juta rupiah) sampai dengan Rp. 500.000.000,00 (lima ratus juta rupiah).

Dalam Upaya Menangani kasus-kasus yg terjadi khususnya yang ada kaitannya dengan *cybercrime*, para Penyidik (khususnya Polri) melakukan analogi atau perumpamaan dan persamaan terhadap pasal-pasal yang ada dalam KUHP Pasal yang dapat dikenakan dalam KUHP pada *cybercrime* antara lain:

a. KUHP (Kitab Undang-Undang Hukum Pidana), pasal-pasal yang terkait:

1. Pasal 362 KUHP tentang pencurian (Kasus *carding*)

Carding dimana pelaku mencuri 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.

2. Pasal 378 KUHP tentang 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.
3. Pasal 311 KUHP Pencemaran nama dengan menggunakan media internet. Modusnya adalah pelaku menyebarkan e-mail kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan e-mail secara berantai melalui mailling list (millis) tentang berita yang tidak benar.
4. Pasal 303 KUHP Perjudian (permainan judi online) dapat dikenakan untuk menjerat permainan judi yang dilakukan secara on-line di internet dengan penyelenggara dari Indonesia
5. Pasal 282 KUHP *Pornografi* dapat dikenakan untuk penyebaran pornografi maupun website porno yang banyak beredar dan mudah diakses di internet.
6. Pasal 282 dan 311 KUHP dapat dikenakan untuk penyebaran foto atau film pribadi seseorang yang vulgar di internet.
7. Pasal 378 dan 262 KUHP dapat dikenakan pada kasus *carding*, karena pelaku melakukan penipuan seolah-olah ingin membeli suatu barang dan membayar dengan kartu

kredit yang nomor kartu kreditnya merupakan hasil curian.

8. Pasal 406 KUHP dapat dikenakan pada kasus *deface* suatu *website*, karena pelaku setelah berhasil memasuki *website* korban, selanjutnya melakukan pengrusakan dengan cara mengganti tampilan asli dari *website* tersebut.

Adapun beberapa peraturan perundang-undangan yang berkaitan dengan masalah komputer, diantaranya adalah sebagai berikut :

1. Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta, Khususnya tentang Program Komputer atau software.
2. Undang-Undang Nomor 25 Tahun 2003 tentang Perubahan atas Undang- Undang Nomor 15 Tahun 2002 tentang Pencucian Uang.
3. Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme.
4. Undang-undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang
5. Undang-undang Nomor 44 Tahun 2008 tentang Pornografi
6. Undang-undang Nomor 35 Tahun 2009 tentang Narkotika

C. Analisis Penulis

Masyarakat seharusnya lebih berhati-hati dalam menggunakan teknologi informasi dalam hal internet karena tindak kejahatan dunia maya di Indonesia saat ini mempunyai bentuk beragam seiring dengan berkembangnya teknologi maka semakin berkembang juga bentuk-bentuk kejahatan yang dapat dilakukan.

Tindak Kejahatan Dunia Maya meliputi pelanggaran hak kekayaan intelektual, fitnah atau pencemaran nama baik, pelanggaran terhadap kebebasan pribadi (privacy), ancaman dan pemerasan, eksploitasi seksual anak-anak dan pencabulan, kerusakan sistem komputer, pembobolan kode akses, pemalsuan tanda tangan digital, pemalsuan data, penyebaran virus, dan pembocoran data rahasia dan masih banyak lagi jenis dan bentuk kejahatan yang terjadi.

Adapun kebijakan mengenai kejahatan dunia maya adalah Undang-undang hukum pidana yang menjadi dasar untuk menjarung kejahatan dunia maya yaitu Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Undang-Undang Nomor 11 Tahun 2009 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, kebijakan kejahatan dunia maya melalui pendekatan KUHP dan masih ada beberapa peraturan perundang-undangan yang berkaitan dengan masalah komputer.

Namun seiring dengan perkembangan kejahatan dunia maya yang terjadi maka kebijakan dunia maya yang berlaku saat ini perlu dilakukan perbaharuan kebijakan dan masyarakat beserta aparat yang menangani kejahatan dunia maya melakukan pencegahan dan meningkatkan keamanan terhadap data atau informasi yang terdapat dalam jaringan komputer.

BAB V

PENUTUP

A. Kesimpulan

- a. Kemajuan teknologi selain membawa dampak perubahan sosial dalam masyarakat. Perubahan sosial tersebut terdiri dari perubahan positif dimana teknologi menjadikan aktivitas dalam masyarakat lebih mudah untuk dilakukan, arus informasi begitu cepat, dan membawa pengaruh dalam sistem politik juga ekonomi. Namun disisi lain juga menimbulkan dampak negative dimana dengan adanya perkembangan teknologi ini memicu lahirnya berbagai kejahatan siber atau yang sering disebut dengan *cybercrime*. Hal ini menjadi suatu tantangan besar yang dihadapi sistem kebijakan hukum di seluruh dunia dalam mengatur masyarakat dalam dunia virtual untuk memberikan perlindungan dan keamanan masyarakat dalam berbagai tindak kejahatan dan menekan tindakan kejahatan yang semakin berkembang.
- b. Undang-Undang Hukum Pidana menjadi dasar untuk menjangkit *Cyber Crime*, yang memenuhi unsur-unsur dalam pasal-pasal Kitab Undang-Undang Hukum Pidana (KUHP). Selain KUHP ada juga aturan hukum yang berkaitan dengan hal ini, yaitu Undang-Undang Nomor 19 tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi

dan Transaksi Elektronik (ITE), dimana aturan tindak pidana yang terjadi di dalamnya terbukti mengancam para pengguna internet.

B. Saran

Mengingat tindak pidana dalam dunia maya akan terus berkembang sesuai dengan perkembangan teknologi dan budaya masyarakat, maka terdapat beberapa saran sehubungan dengan kebijakan hukum tentang kejahatan dunia maya melalui hukum pidana, adalah sebagai berikut:

- a. Sebaiknya, masyarakat luas dalam menggunakan teknologi informasi, dalam hal internet adalah untuk sarana yang positif, yaitu sebagai bahan informasi pengetahuan, sehingga menambah wawasan keilmuan dalam bermasyarakat, berbangsa, dan bernegara.
- b. Sebaiknya pemerintah dalam hal ini aparat penegak hukum dalam menangani *Cyber Crime* melakukan *self protection* terhadap data atau informasi yang terdapat dalam jaringan komputer yang merupakan ujung tombak dari pencegahan dan penanggulangan *Cyber Crime*.

DAFTAR PUSTAKA

Al-Qur'an/Hadist

Departemen Agama RI, (2015) Al-Qur'an dan Terjemahan. Bandung: CV. Darus Sunnah

Buku

Abdul Wahid dan Mohammad Labib. (2005). **Kejahatan Mayantara (Cyber Crime)**. Jakarta: PT. Refika Aditama

Adami Chazawi. (2002). **Pelajaran Hukum Pidana II**. Jakarta: Rajawali Pers.

_____. (2013) **Pelajaran Hukum Pidana, Bagian 1: Stelsel Pidana, Teori-Teori Pemidanaan & Batas Berlakunya Hukum Pidana**, Jakarta: Raja Grafindo

Amir Ilyas. (2012). **Asas-Asas Hukum Pidana Memahami Tindak Pidana Dan Pertanggungjawaban Pidana Sebagai Syarat Pemidanaan (Disertai Teori-Teori Pengantar Dan Beberapa Komentar)**. Yogyakarta:Rangkang Education Yogyakarta & PuKAP-Indonesia.

And i Hamzah. (1994). **Asas-Asas Hukum Pidana**. Jakarta: Rineka Cipta.

Barda Nawawi Arief. (2007). **Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan**. Jakarta; Kencana.

- _____. (2008). **Bunga Rampai Kebijakan Hukum Pidana Perkembangan Konsep KUHP Baru**. Jakarta: Kencana Prenadamedia Grub.
- Budi Suhariyanto. (2007). **Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya**, Depok: PT. Rajagrafindo Persada.
- Dikdik M. Arief Mansur dan Elisatris Gultom. (2005). **Cyber Law Aspek Hukum Teknologi Informasi**. Bandung: Refika Aditama.
- E.Y. Kanter. (1992). **Azas-azas Hukum Pidana di Indonesia dan Penerapannya**. Jakarta: Alumni AHMPH.
- Jonathan Rosenoer.(1997). **Cyberlaw: The Law of the Internet**. New York:SpringVerlag
- K. Wantjik Saleh, (1998) **Kehakiman dan Keadilan**. Jakarta: Ghalia Indonesia.
- Kamri Ahmad & Andi Khaedir. (2019). **Pengantar Ilmu Hukum**. Makassar: Umitoha Ukhuwah Grafika
- Moeljatno. (1993). **Azas-Azas Hukum Pidana**. Jakarta: Rineka Cipta.
- Muladi. (2002). **Demokratisasi Hak Asasi Manusia dan Reformasi Hukum di Indonesia**. Jakarta: Habibie Center
- Mustafa Abdullah dan Ruben Achmad. (1983). **Intisari Hukum Pidana**. Jakarta: Ghalia Indonesia.

Ricky Adjie Purnama, **“Cyber Crime Dalam Perspektif Hukum Positif dan Hukum Islam”**(Skripsi Fakultas Syari’ah IAIN SMH Bante, 2007).

S. R. Sianturi. (1982). **Asas-Asas Hukum Pidana di Indonesia dan Penerapannya**. Jakarta: Alumni.

Stepen Huwitz dan Saduran Moeljatno. (1986). **Kriminologi**. Jakarta: Bina Aksara

Sudarto. (1981). **Hukum dan Hukum Pidana**. Bandung: Alumni.

Sue Titus Reid. (1985). **Crime and Criminology**. New York: CBS College Publishing

Widodo. (2013) **Aspek Hukum Pidana Kejahatan Mayantara**. Yogyakarta:Aswaja Pressindo.

Peraturan Perundang-Undangan

Undang-Undang Negara Republik Indonesia 1945

Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Tansaksi Elektronik.

Website

Ani Mardatila. (2022). **Perkembangan Teknologi Informasi di Indonesia.** Merdeka.com. Di akses dari <https://www.merdeka.com/sumut/perkembangan-teknologi-informasi-di-indonesia-klm.html>, diakses pada tanggal 18 Oktober 2022. Pukul 21.30

Dimas Bayu. (2022). **Pengguna Internet Indonesia Tembus 210 Juta pada 2022.** Dataindonesia.id. Di akses dari <https://dataindonesia.id/digital/detail/apjii-pengguna-internet-indonesia-tembus-210-juta-pada-2022>, diakses pada tanggal 18 Oktober 2022. Pukul 22.33

Fidel Ali Permana. (2015). **Indonesia Urutan Kedua Terbesar Negara Asal "Cyber Crime" di Dunia.** Nasional.kompas.com. Di akses dari <https://nasional.kompas.com/read/2015/05/12/06551741/Indonesia.Urutan.Kedua.Terbesar.Negara.Asal.Cyber.Crime.di.Dunia>, diakses pada tanggal 19 Oktober 2022. Pukul 19.30

Taufan Aditya Pratama. (2019). **Pengertian Cyber Crime.** Adoc.tips. Diakses dari <https://adoc.tips/download/pengertian-cyber-crime.html> diakses tanggal 23 Oktober 2022. Pukul 12.00

Jurnal

Arifah, D. A. (2011). Kasus cybercrime di indonesia. Jurnal Bisnis Dan Ekonomi, 18(2), 186.

Dheny Wahyudi. (2020). Perlindungan Hukum Terhadap Korban Kejahatan *Cyber Crime* di Indonesia. Jurnal Ilmu Hukum, Universitas Jambi, hlm. 99

Noviantini, N., Remaja, I. N. G., & Mariadi, N. N. (2021). Efektivitas Patroli Siber Dalam Mengungkap Kasus Ujaran Kebencian Di Wilayah Hukum Polres Buleleng. Kertha Widya, 9(1), 37.