

SKRIPSI
TINJAUAN KRIMINOLOGI TENTANG KEJAHATAN
PENIPUAN BERBASIS ONLINE
(Studi Kasus Subdit V Cyber Crime Reskrimsus Polda Sulsel)



Oleh:

Fira Nur Rezki Hasanuddin

04020190102

Diajukan sebagai Tugas Akhir dalam rangka penyelesaian studi

FAKULTAS HUKUM
UNIVERSITAS MUSLIM INDONESIA
MAKASSAR
2023

HALAMAN JUDUL

**TINJAUAN KRIMINOLOGI TENTANG KEJAHATAN PENIPUAN
BERBASIS ONLINE**

(STUDI KASUS SUBDIT V CYBER CRIME RESKRIMSUS POLDA SULSEL)

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:

FIRA NUR REZKI HASANUDDIN

04020190102

**FAKULTAS HUKUM
UNIVERSITAS MUSLIM INDONESIA
MAKASSAR
2023**

PERSETUJUAN PEMBIMBING

Diterangkan bahwa Skripsi mahasiswa :

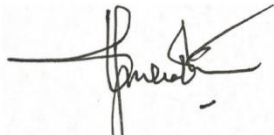
Nama Mahasiswa : Fira Nur Rezki Hasanuddin
NIM : 04020190102
Bagian : Hukum Pidana
Dasar Penetapan : 0397/H.05/FH-UMI/IX/2022
Judul Skripsi : Tinjauan Kriminologi Tentang Kejahatan
Penipuan Berbasis Online

Telah diperiksa dan disetujui untuk diajukan dalam Ujian Skripsi.

Makassar, 7 Februari 2023

Komisi Pembimbing

Pembimbing 1



Prof. Dr. Hj. Mulyati Pawennei, SH., MH.
NIPs. 19611201 198703 2 003

Pembimbing 2



Dr. Salmawati, SHi.,MH.
NIPs. 104171451

Mengetahui,

Ketua Bagian Hukum Pidana



Prof. Dr. Hj. Mulyati Pawennei, SH., MH
NIPs. 19611201 198703 2 003

PERSETUJUAN UJIAN SKRIPSI

Pimpinan Fakultas Hukum Universitas Muslim Indonesia memberikan

Persetujuan untuk mengikuti Ujian Skripsi Kepada :

Nama Mahasiswa : Fira Nur Rezki Hasanuddin

NIM : 04020190102

Bagian : Hukum Pidana

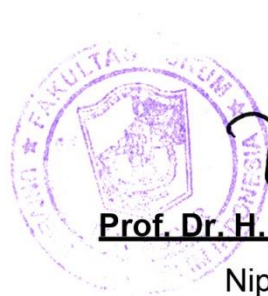
Dasar Penetapan : 0397/H.05/FH-UMI/IX/2022

Judul Skripsi : Tinjauan Kriminologi Tentang Kejahatan Penipuan
Berbasis Online

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

Makassar, 7 Februari 2023

Dekan Fakultas Hukum
Universitas Muslim Indonesia Makassar




Prof. Dr. H. La Ode Husen.SH..MH.

Nips. 104 86 0192

PENGESAHAN SKRIPSI
TINJAUAN KRIMINOLOGI TENTANG KEJAHATAN PENIPUAN
BERBASIS ONLINE
(STUDI KASUS SUBDIT V CYBER CRIME RESKRIMSUS POLDA SULSEL)

Di susun dan di ajukan oleh :

FIRA NUR REZKI HASANUDDIN

04020190102

Telah dipertahankan di hadapan Panitia Ujian Skripsi
Pada Program Studi Sarjana Ilmu Hukum Fakultas Hukum

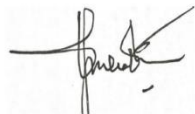
Universitas Muslim Indonesia
Pada, 20 Februari 2023

Dan dinyatakan di terima

Makassar, 20 Februari 2023

Panitia Ujian

Ketua



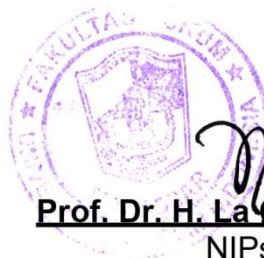
Prof. Dr. Hj. Mulyati Pawennei. SH..MH.
NIPs. 19611201 198703 2 003

Anggota



Dr. Salmawati .SHi.MH
NIPs. 104171451

Dekan



Prof. Dr. H. La Ode Husen. S.H.. M.H
NIPs.104860192

HALAMAN PENGESAHAN PENGUJI

Nama Mahasiswa : Fira Nur Rezki Hasanuddin

NIM : 04020190102

Program Studi : Ilmu Hukum

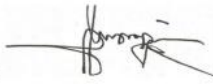
Bagian : Hukum Pidana

Judul Skripsi : **TINJAUAN KRIMINOLOGI TENTANG KEJAHATAN PENIPUAN BERBASIS ONLINE (STUDI KASUS SUBDIT V CYBER CRIME RESKRIMSUS POLDA SULSEL)**

Dasar Penetapan : 0397/H.05/FH-UMI/IX/2022

Telah diterangkan dihadapan Majelis Ujian Skripsi Pada Hari Senin 20

Februari 2023 dan dinyatakan **LULUS** Oleh:

1. Prof. Dr. Hj. Mulyati Pawennei, S.H., M.H. (..... )
(Pembimbing Ketua)

2. Dr. Salmawati, S.Hi., M.H. (..... )
(Pembimbing Anggota)

3. Hj. Fauziah Basyuni, S.H., M.H. (...  ...)
(Penguji I)

4. Arsyid Zakariah, S.H., M.H. (..... )
(Penguji II)



PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini :

Nama Mahasiswa : Fira Nur Rezki Hasanuddin

NIM : 04020190102

Bagian : Hukum Pidana

Judul Skripsi : Tinjauan Kriminologi Tentang Kejahatan

Penipuan Berbasis Online (Studi kasus Sybdit V
Cyber Crime Reskrimsus Polda Sulsel)

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

Makassar, 20 Februari 2023

Penulis

Fira Nur Rezki Hasanuddin

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Alhamdulillah, puji syukur penulis panjatkan kehadiran Allah SWT yang telah memberikan rahmat dan Karunia-Nya, tak lupa pula shalawat dan salam kita kirimkan kepada junjungan Nabi Besar Muhammad SAW beserta para Sahabatnya sehingga penulis senantiasa diberikan kemudahan dan kesabaran dalam menyelesaikan skripsi yang berjudul “Tinjauan Kriminologi Tentang Penipuan Berbasis Online”, sebagai syarat untuk menyelesaikan pendidikan dan memperoleh gelar sebagai Sarjana Hukum di Fakultas Hukum Universitas Muslim Indonesia.

Pada kesempatan ini, penulis ingin mengucapkan terima kasih yang tak terhingga kepada kedua orangtua tercinta, Hasanuddin Hasan, S.H. dan Hj. Saleha yang telah memberikan motivasi serta mencurahkan kasih sayang, perhatian, pengorbanan, doa, dan jerih payahnya sehingga penulis dapat menyelesaikan tugas akhir ini. Selanjutnya penulis ucapkan terimakasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr. H. Basri Modding, S.E, M.Si. selaku Rektor Universitas Muslim Indonesia
2. Bapak Prof. Dr., H. Laode Husen S.H., M.H. selaku Dekan Fakultas dan Wakil Dekan Hukum Universitas Muslim Indonesia
3. Prof. Dr. Hj. Mulyati Pawennei, S.H., M.H dan Dr. Salmawati, S.Hi., M.H. selaku pembimbing I dan pembimbing II penulis yang telah banyak memberikan arahan, kritikan, dan bimbingan kepada

penulis agar penulis dapat menyelesaikan tulisan ini.

4. Hj. Fauziah Basyuni, S.H.,M.H. dan Arsyid Zakariah, S.H.,M.H. selaku penguji I dan penguji II penulis yang telah memberi saran yang sangat bermanfaat untuk menyempurnakan penulis skripsi ini.
5. Para dosen Fakultas Hukum Universitas Muslim Indonesia yang dengan penuh kesabaran, keikhlasan dan ketulusan mereka dalam memberikan ilmu yang sangat bermanfaat kepada penulis.
6. Segenap Bapak dan Ibu Dosen, dan Karyawan Fakultas Hukum Universitas Muslim Indonesia yang telah berjasa mendidik penulis, senantiasa membantu dan memberikan banyak kemudahan.
7. Kepada Panit 2 unit 2 dan Banit Subdit V yang telah memberikan kesempatan dan memudahkan alur perjalanan untuk melakukan penelitian ditempat tersebut.
8. Teruntuk sahabat-sahabatku khususnya kak Didi, Riska, Indy, Lia, Rani, dan Kardhasian Family yang selalu menemani dalam penulisan skripsi ini.
9. Kepada teman-teman yang tidak sempat saya sebutkan satu persatu, penulis ucapkan banyak terima kasih atas bantuan, dan dukungannya. Semoga kebaikan yang diberikan kepada penulis dibalas oleh allah SWT berkali lipat.

Makassar, 20 Februari 2023

Fira Nur Rezki Hasanuddin

ABSTRAK

Fira Nur Rezki Hasanuddin (04020190102) “Tinjauan Kriminologi Tentang Penipuan Berbasis Online (Studi Kasus Subdit V Cyber Crime Reskrimsus polda Sulsel)”. Dibimbing oleh ibu Mulyati Pawennei selaku pembimbing I dan ibu Salmawati selaku pembimbing II

Penelitian ini bertujuan untuk mengetahui faktor yang mempengaruhi maraknya cyber crime yang dikhususkan pada kejahatan penipuan berbasis online, efektivitas penegakan hukum dalam upaya penanggulangan tindak pidana cyber crime, dan kendala-kendala yang dihadapi oleh aparat kepolisian dalam upaya penanggulangannya.

Penelitian ini dilaksanakan di Kepolisian Negara Republik Indonesia Daerah Sulawesi Selatan (Polda Sulsel). Metode penelitian yang digunakan adalah studi lapangan melalui wawancara langsung kepada narasumber yang berkaitan dengan tulisan ini, penulis juga melakukan penelitian kepustakaan dengan mengumpulkan data dari berbagai literatur yang ada, berupa buku, artikel- artikel yang diperoleh dari penelusuran internet, termasuk aturan perundang-undangan yang terkait dengan permasalahan dalam penelitian ini.

Hasil yang penulis peroleh dari penelitian ini menunjukkan, yaitu faktor-faktor yang menyebabkan terjadinya penipuan berbasis online yakni: faktor ekonomi, faktor lingkungan, faktor sosial budaya, dan faktor intelektual. Upaya yang dilakukan pihak kepolisian dalam menanggulangi kejahatan penipuan berbasis online yakni: upaya preventif yang dilakukan untuk mencegah terjadinya pelanggaran aturan di masyarakat dan upaya represif tindakan yang dilakukan setelah pelanggaran aturan terjadi.

Rekomendasi dari penelitian ini agar Pemerintah juga harus memperhatikan aturan-aturan terkait informasi dan transaksi elektronik guna mengurangi celah hukum yang dapat timbul dan sebaiknya pemerintah memperhatikan alat dan akses untuk celebriti yaitu alat untuk mengangkat data dari handphone, yang saat ini hanya 1 buah akses celebriti di cyber crime polda sulsel, sementara penggunaannya sangat penting untuk pembuktian pelaku kejahatan khususnya kejahatan dunia maya.

DAFTAR ISI

PERSETUJUAN PEMBIMBING	ii
BAB I PENDAHULUAN	1
A. Latar Belakang Masalah.....	1
B. Rumusan Masalah	5
C. Tujuan Penelitian.....	6
D. Manfaat penelitian	6
BAB II TINJAUAN PUSTAKA.....	7
A. Tinjauan Kriminologi.....	7
1. Pengertian Kriminologi	7
2. Ruang Lingkup Kriminologi	9
B. Tindak Pidana Kejahatan	11
1. Pengertian Kejahatan	11
2. Jenis Kejahatan	13
C. Tindak Pidana Cyber Crime	17
1. Definisi cyber Crime	17
2. Karakteristik Cyber Crime	18
3. Bentuk-Bentuk Cyber Crime.....	19
D. Tindak Pidana Cyber Crime Di Indonesia	22
E. Tindak Pidana Penipuan	27
1. Pengertian Penipuan.....	27
2. Unsur-unsur Tindak Pidana Penipuan	29
BAB III METODE PENELITIAN.....	31
A. Tipe Penelitian.....	31
B. Lokasi Penelitian	31
C. Jenis Dan Sumber Data	31
D. Populasi dan Sampel	32
E. Teknik Pengumpulan Data	32
F. Analisis Data	33
BAB IV HASIL PENELITIAN DAN PEMBAHASAN	34
A. Faktor-faktor Yang Menyebabkan Terjadinya Kejahatan Penipuan Online	34
1. Faktor Ekonomi	35
2. Faktor Lingkungan.....	36

3. Faktor Sosial Budaya	37
4. Faktor Intelektual	38
B. Upaya Penanggulangan Kejahatan Penipuan Online oleh Pihak Kepolisian	39
1. Upaya Preventif	39
2. Upaya Represif	40
3. Pelaksanaan Undang-Undang Informasi dan Transaksi Terhadap Kejahatan <i>Cyber Crime</i>	41
4. Kendala yang dihadapi Aparat Kepolisian Dalam Upaya Penanggulangan <i>Cyber Crime</i>	53
BAB V PENUTUP	59
A. Kesimpulan	59
B. Saran	59
DAFTAR PUSTAKA	60

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi informasi yang makin pesat seiring berjalannya waktu membuat teknologi dan informasi menjadi hal yang *central* dalam masyarakat. Dalam hal ini juga menjadi kebutuhan pokok bagi masyarakat untuk meningkatkan produktivitas keseharian mereka dengan akses yang cepat dalam memperoleh informasi, yang membuat kemajuan teknologi informasi dan komunikasi menjadi mengubah pola hidup masyarakat dan memicu terjadinya perubahan social, budaya, ekonomi, pertahanan, keamanan, dan penegakan hukum.

Teknologi informasi dan komunikasi telah dimanfaatkan dalam kehidupan sosial masyarakat, dan telah memasuki berbagai faktor kehidupan baik sektor pemerintah, bisnis, perbankan, pendidikan, kesehatan, dan kehidupan pribadi. Manfaat teknologi informasi dan komunikasi selain memberikan dampak positif juga disadari memberi peluang untuk dijadikan sarana melakukan kejahatan baru (*cyber crime*). Dikatakan bahwa teknologi informasi dan komunikasi bagaikan pedang bermata dua, dimana selain memberikan kontribusi positif bagi peningkatan kesejahteraan, kemajuan, dan Peradaban manusia, juga

menjadi sarana potensial dan sarana efektif untuk melakukan perbuatan melawan hukum.¹

Telah banyak kasus kejahatan yang terjadi di dunia maya ini yang tentu saja merugikan dan memberikan dampak yang negatif, *cybercrime* ini tidak hanya meliputi Indonesia tetapi juga global.

Beberapa kasus kejahatan yang terjadi dipicu oleh maraknya penggunaan email, ebanking, ecommerce di Indonesia. Semakin maraknya kasus *cybercrime* yang terjadi terutama di Indonesia telah menarik perhatian pemerintah untuk segera memiliki undang-undang yang bisa digunakan untuk bisa menjerat para pelaku kejahatan di dunia maya. Pemerintah Indonesia sendiri telah mengesahkan undang-undang *cybercrime* yaitu *cyber law* kedalam undang-undang RI. No. 19 tahun 2016 tentang perubahan atas UU RI Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), diharapkan dengan adanya Undang-undang ITE tersebut dapat mengatasi, meminimalisir dan membuat jera pelaku kejahatan di dunia maya.

Pasal 28 ayat (1) Undang-undang RI. No. 19 tahun 2016 tentang perubahan atas Undang-undang RI. No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) berbunyi:

“Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik”.

Pasal 45A ayat (1) Undang-undang RI. No. 19 tahun 2016 tentang perubahan atas Undang-undang RI. No. 11 tahun 2008 tentang

¹ Siswanto. 2009. Hukum informasi dan Transaksi Elektronik Studi Kasus Prita Mulyasari. Jakarta: Rineka Cipta, hlm 40

Informasi dan Transaksi Elektronik (ITE) berbunyi:

“ Setiap orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,00 (satu miliar rupiah).

Cyber crime dapat diartikan sebagai kegiatan ilegal dengan perantara komputer yang dapat dilakukan melalui jaringan elektronik global.

Pada jaringan computer seperti internet, masalah Kriminalitas menjadi semakin kompleks karena ruang lingkupnya yang luas. Kriminalitas dalam internet atau *cyber crime* pada dasarnya adalah suatu tindak pidana yang berkaitan dengan *cyber space*, baik yang menyerang fasilitas untuk di dalam *cyber space* ataupun kepemilikan pribadi.

Bermacam-macam kejahatan yang dapat timbul dari “permainan” internet, seperti penipuan, penghinaan, pornografi, bahkan kejahatan terhadap keamanan negara, seperti pembocoran rahasia Negara. *Money laundering* dan terorisme juga dapat dilakukan melalui internet, terutama dengan penyertaan dan pemufakatan jahat. Sehubungan dengan itu, Asas berlakunya hukum pidana terutama Asas universalitas semestinya diperluas terhadap beberapa bentuk delik baru tersebut.

Tindak pidana penipuan tindak pidana atau kejahatan terhadap harta benda. Tindak pidana tersebut diatur dalam KUHP masuk Buku 2-Kejahatan Bab XXV Pasal 378.

Pasal 378 KUHP mengatur tindak pidana penipuan dalam arti luas (bedrog). Adapun bunyi pasal tentang Penipuan tersebut sebagai berikut: “Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun.”

Tindak Pidana penipuan termuat dalam QS: Al-Baqarah Ayat 9 yang berbunyi:

يُخَادِعُونَ اللَّهَ وَالَّذِينَ آمَنُوا وَمَا يَخْدَعُونَ إِلَّا أَنفُسَهُمْ وَمَا يَشْعُرُونَ ﴿٩﴾

Terjemahan:

“Mereka menipu Allah dan orang-orang yang beriman, padahal mereka hanyalah menipu diri sendiri tanpa mereka sadari”.

Kejahatan dalam internet ini dapat dibedakan menjadi tiga bagian yaitu pelanggaran, akses, pencurian data, dan penyebaran informasi untuk tujuan kejahatan seperti melakukan penipuan melalui internet.

Penipuan melalui internet atau penipuan berbasis *online* merupakan kejahatan yang marak terjadi saat ini. Pengguna internet yang semakin meningkat ternyata membuka kesempatan yang lebih besar bagi para penipu *online* untuk mendapatkan uang atau keuntungan dari internet. Ada banyak sekali pengguna internet yang mencari peluang melalui bisnis *online*, dan ini memberikan ide bagi para *Scammer* (pelaku penipuan berbasis online) untuk meraup keuntungan.

Ada banyak modus penipuan di dunia maya, mulai dari toko *online* hingga penawaran bisnis *online*. Penipuan yang berkedok bisnis *online* dapat tersamar dengan sangat baik, makan orang yang sudah sering bermain internet tidak sadar bahwa dia sedang tertipu. Penipuan bisnis *online* bisa dilakukan dengan berbagai modus, yang biasa digunakan oleh pelaku untuk menjerat korbannya seperti modus penipuan bisnis online berupa pembajakan account biasanya pelaku akan membajak akun akun yang dianggap menguntungkan, seperti akun media social tokoh ternama sudah mampu dibajak maka aksi penipuan bisa dilancarkan dengan menggunakan akun dari seseorang yang terkenal sehingga mudah dipercaya saat ditawarkan produk, atau atau yang lebih parah disuruh mentransfer sejumlah uang. Modus penipuan bisnis online yang paling sering dijumpai pada saat bertransaksi seperti barang yang tidak terkirim atau tidak sampai ke penerima, atau barang yang sampai kepada konsumen tidak sama dengan barang yang diperjualbelikan.

Untuk itu penulis mengangkat skripsi dengan judul : **Tinjauan Kriminologis Terhadap Kejahatan Penipuan Berbasis Online.**

B. Rumusan Masalah

1. Faktor-faktor apakah yang menyebabkan terjadinya kejahatan penipuan berbasis *online*?
2. Upaya apakah yang dilakukan pihak kepolisian dalam menanggulangi kejahatan penipuan berbasis online?

C. Tujuan Penelitian

Berdasarkan uraian latar belakang dan pokok permasalahan sebagai mana telah dikemukakan di atas maka penelitian ini bertujuan untuk:

1. Untuk mengetahui dan menganalisis faktor yang menyebabkan kejahatan penipuan berbasis *online*
2. Untuk mengetahui dan menganalisis penanggulangan kejahatan penipuan berbasis online yang dilakukan oleh pihak kepolisian.

D. Manfaat Penelitian

1. Manfaat teoritis

Hasil penelitian ini dapat bermanfaat pengembangan ilmu pengetahuan pada umumnya dan menambah bahan pustaka mengenai *freuderipenipuan* berbasis *online* perlindungan hukumnya.

2. Manfaat praktik

sebagai sumbangan pemikiran untuk penyelesaian masalah terhadap kasus kejahatan *freuderipenipuan* berbasis *online* sehingga dapat memberikan masukan kepada aparat penegak hukum di dalam penyelesaian kasus-kasus tindak pidana yang memanfaatkan teknologi sebagai alat pengopersiannya.

BAB II

TINJAUAN PUSTAKA

A. Kriminologi

1. Pengertian Kriminologi

Kriminologi termasuk cabang ilmu pengetahuan yang berkembang pada tahun 1850 bersama-sama dengan ilmu sosiologi, antropologi, dan psikologi.

Asal mula perkembangan Kriminologi tidak dapat disangkal berasal dari penyelidikan C. Lombroso (1876). Bahkan Lombroso menurut Pompe dipandang sebagai salah satu tokoh revolusi dalam sejarah hukum pidana, disamping Cesare Baccaria. Namun ada pendapat lain yang mengemukakan bahwa penyelidikan secara ilmiah tentang kejahatan justru bukan dari Lombroso melainkan dari Adolphe Quetelet, seorang Belgia yang memiliki keahlian dibidang matematika. Bahkan, dari dialah berasal “ *statistic kriminil* ” yang kini dipergunakan terutama oleh pihak kepolisian di semua Negara dalam memberikan deskripsi tentang perkembangan kejahatan di negaranya.²

Nama Kriminologi pertama kali ditemukan oleh P. Topinard (1830-1911) seorang antropologi Perancis.³ Intinya adalah bahwa Kriminologi merupakan ilmu yang mempelajari tentang kejahatan.

² Romli Atasasmita, 2010, *Teori dan Kapita Selekta Kriminologi*, Refika Adatama, Bandung, Hal 9.

³ As. Aalam & Amir Ilyas, 2010, *Pengantar Kriminologi*, Pustaka Refleksi, Makassar, Hal 1

Nama kriminologi yang ditemukan oleh P.Topinard (1830-1911) seorang ahli antropologi Prancis, secara harafiah kriminologi berasal dari kata "*crimen*" yang berarti kejahatan atau penjahat dan "*logos*" berarti ilmu pengetahuan, maka Kriminologi dapat berarti ilmu yang mempelajari tentang penjahat dan kejahatan. Beberapa sarjana memberikan pengertian berbeda terhadap Kriminologi, Michael dan Adler berpendapat bahwa :

Kriminologi adalah keseluruhan mengenai perbuatan dan sifat para penjahat, lingkungan mereka dan cara mereka secara resmi diperlakukan oleh lembaga-lembaga penerbit masyarakat dan oleh para masyarakat. Sedangkan Wood mengatakan :

Kriminologi meliputi keseluruhan mengenai perbuatan yang diperoleh berdasarkan teori atau pengalaman, yang berkaitan dengan perbuatan jahat dan penjahat termasuk di dalamnya reaksi dari masyarakat terhadap perbuatan jahat dan para penjahat.⁴

Selanjutnya Moeljatno berpendapat bahwa kriminologi adalah untuk mengerti apa sebab-sebab sehingga seseorang berbuat jahat. Apakah memang karena bakatnya adalah jahat ataukah didorong oleh keadaan masyarakat disekitarnya (*milieu*) baik keadaan sosiologi maupun ekonomi ataukah ada sebab-sebab lain lagi. Jika sebab-sebab itu diketahui, maka disamping pemidanaan, dapat diadakan tindakan-tindakan yang tepat, agar orang tadi tidak lagi berbuat demikian atau

⁴ Topo Santoso & Eva Achjani Zulfa, 2001, Kriminologi, Raja Grafindo Persada, Jakarta, Hal 12.

agar orang-orang lain tidak akan melakukannya. Karena itulah terutama dinegeri-negeri angelsaks, kriminologi di bagi menjadi tiga bagian :

1. *Criminal biology*, yang menyelidiki di orang itu sendiri akan sebab-sebab dari perbuatannya, baik dalam Jasmani maupun Rohani.
2. *Criminal sosiologi*, yang mencoba mencari sebab-sebab dalam lingkungan masyarakat dimana penjahat itu berbeda (dalam milieunya)
3. *Criminal policy*, yaitu tindakan-tindakan apa yang disekitarnya harus dijalankan supaya orang laon tidak berbuatdemikian.

2. Ruang Lingkup Kriminologi

Menurut Sutherland, kriminologi terdiri dari tiga bagian utama, yaitu: ⁵

- a) Etiologi kriminal, yaitu usaha secara ilmiah untuk mencari sebab-sebab kejahatan
- b) Penologi, yaitu pengetahuan yang mempelajari tentang sejarah lahirnya hukuman, perkembangan serta arti dan faedahnya
- c) Sosiologi hukum (pidana), yaitu analisis ilmiah terhadap kondisi-kondisi yang mempengaruhi perkembangan hukum pidana.

Sedangkan Menurut A.S. Alam ruang lingkup pembahasan kriminologi mencakup tiga hal pokok⁶, yaitu :

⁵ I. S. Susanto, 1991, *Diktat Kriminologi Fakultas Hukum Universitas Diponegoro Semarang*, Semarang, Hal 10.

⁶ Moeljatno, 2008, *Asas-Asas Hukum Pidana*, Rineks Cipta, Jakarta, Hal 14.

1. Proses pembuatan hukum pidana dan acara pidana (*making laws*).

Pembahasan dalam proses pembuatan hukum pidana (*process of making laws*) meliputi :

- 1) Definisi kejahatan
- 2) Unsur-unsur kejahatan..
- 3) Relativitas pengertian kejahatan
- 4) Pengolongan kejahatan
- 5) Statistic kejahatan

2. Etiologi kriminal, yang membahas teori-teori yang menyebabkan terjadinya kejahatan (*breaking of laws*). Sedangkan yang dibahas dalam etiologi kriminal (*breaking of laws*) meliputi :

- 1) Aliran-aliran (mazhab-mazhab) kriminologi
- 2) Teori-teori kriminologi
- 3) Berrbagi perspektif kriminologi

3. Reaksi terhadap pelanggaran hukum, (*reacting toward the breaking of laws*). Reaksi dalam hal ini bukan hanya ditujukan kepada pelanggar hukum berupa tindakan represif tetapi juga reaksi terhadap calon pelanggar hukum berupa upaya-upaya pencegahan kejahatan (*criminal prevention*). Selanjutnya yang dibahas dalam bagian ketiga adalah perlakuan terhadap pelanggar-pelanggar hukum (Reacting Toward The Breaking Laws) meliputi :

- a. Teori-teori penghukuma

- b. Rehabilitatif. Secara umum dapat disimpulkan bahwa kriminologi mempelajari tentang kejahatan yaitu norma-norma yang ada dalam peraturan pidana, yang kedua yaitu mempelajari pelakunya yang sering disebut penjahat. Dan yang ketiga bagaimana tanggapan atau reaksi masyarakat terhadap gejala-gejala yang timbul dalam masyarakat .

B. Tindak Pidana Kejahatan

1. Pengertian Kejahatan

Kejahatan adalah suatu persoalan yang selalu melekat dimana masyarakat itu ada. Kejahatan selalu akan ada seperti penyakit dan kematian yang selalu berubah seperti halnya dengan musim yang berganti-ganti dari tahun ketahun. Segala daya upaya dalam menghadapi kejahatan dapat menekan atau mengurangi meningkatnya jumlah kejahatan dan memperbaiki penjahat agar dapat kembali sebagai warga masyarakat yang baik.

Kejahatan adalah suatu nama atau cap yang diberikan orang untuk menilai perbuatan-perbuatan tertentu sebagai perbuatan jahat. Dengan demikian, maka si pelaku disebut sebagai penjahat. Pengertian tersebut bersumber dari manusia, sehingga ia memiliki pengertian yang sangat relative, yaitu tergantung pada manusia yang memberikan penilaian itu. Tentang definisi dari kejahatan itu sendiri tidak terdapat kesatuan pendapat antara para sarjana, R.Soesilo⁷ membedakan

⁷ A.S. Alam & Lya, 2010, *Pengantar Kriminologi*, Pustaka Refleksi, Makassar, Hal 1-2.

pengertian kejahatan secara yuridis dan pengertian kejahatan secara sosiologi.

Ditinjau dari segi yuridis, pengertian kejahatan adalah suatu perbuatan tingkah laku yang bertentangan dengan undang-undang. Ditinjau dari segi sosiologi, maka yang dimaksud dengan kejahatan adalah perbuatan atau tingkah laku yang selain merugikan si penderita, juga sangat merugikan masyarakat yaitu berupa hilangnya keseimbangan, ketentraman dan ketertiban.

Selanjutnya adapun beberapa definisi kejahatan menurut beberapa pakar:

1. **J.M. Bemmelem** memandang kejahatan sebagai suatu tindakan anti sosial yang menimbulkan kerugian, ketidakpatutan dalam masyarakat, sehingga dalam masyarakat terdapat kegelisahan, dan untuk menentramkan masyarakat, Negara harus menjatuhkan hukuman kepada penjahat.
2. **M.A. Elliot** mengatakan bahwa kejahatan adalah suatu problem dalam masyarakat modern atau tingkah laku yang melanggar hukum dapat dijatuhi hukuman penjara, hukuman mati dan hukuman denda dan seterusnya.
3. **W.A. Bonger** mengatakan bahwa kejahatan adalah perbuatan yang sangat anti sosial yang memperoleh tantangan dengan sadar dari negara berupa pemberian penderitaan.

4. **Paul Moedikdo Moeliono** kejahatan adalah perbuatan pelanggaran norma hukum yang ditafsirkan atau patut ditafsirkan masyarakat sebagai perbuatan yang merugikan, menjengkelkan sehingga tidak boleh dibiarkan (negara bertindak)
5. **J.E. Sahetapy** dan **B. Marjono Reksodiputro** dalam bukunya “Paradoks dalam Kriminologi” menyatakan bahwa, kejahatan mengandung konotasi tertentu, merupakan suatu pengertian dan penamaan yang relative, mengandung variabilitas dan dinamik serta bertalian dengan perbuatan atau tingkah laku (baik aktif maupun pasif), yang dinilai oleh sebagian mayoritas atau minoritas masyarakat sebagai suatu perbuatan anti sosial, Suatu pemerkosaan terhadap skala nilai sosial dan atau perasaan hukum yang hidup dalam masyarakat sesuai dengan ruang dan waktu.

2. Jenis Kejahatan

Kejahatan dapat digolongkan atas beberapa penggolongan sebagai berikut : Penggolongan kejahatan yang didasarkan pada motif pelaku.

Hal ini dikemukakan menurut pandangan Bonger⁸ sebagai berikut :

- a) Kejahatan ekonomi (*ecomomic crimes*), misalnya penyelundupan.
- b) Kejahatan seksual (*ecomomic crimes*), misalnya perbuatan zina, pasal 284 KUHP.

⁸ A.S. Alam, 1985, *Kejahatan dan Sistem Pemindaan*, Fakultas Hukum UNHAS, Ujung Pandang Hal. 5

- c) Kejahatan politik (*politic crimes*), misalnya pemberontakan partai komunis Indonesia, DI/TII dan lain sebagainya
- d) Kejahatan diiri (*moscellaneus crimes*), misalnya penganiayaan yang motifnya dendam.

1. Penggolongan kejahatan yang ditulis oleh A.S. Alam didasarkan kepada berat ringannya suatu ancaman pidana yang dapat dijatuhkan, yaitu:

- a. Kejahatan, yakni semua pasal-pasal yang disebut di dalam Buku II KUHP, seperti pembunuhan, pencurian dan lain-lain.
- b. Pelanggaran, yakni semua pasal-pasal yang disebut di dalam Buku III KUHP misalnya saksi di depan persidangan memakai jimat pada waktu ia harus memberikan keterangan dengan sumpah, dihukum dengan hukuman kurung selama-lamanya 10 hari dan denda Rp. 750, penggolongan kejahatan untuk kepentingan statistik, oleh sebagai berikut:

- a) Kejahatan terhadap orang (*crimes against person*), misalnya pembunuhan, penganiayaan dan lain-lain.
- b) Kejahatan terhadap harta benda (*crimes against property*), misalnya pencurian, perampokan dan lain-lain.
- c) Kejahatan terhadap kesusilaan umum (*crimes against publicdecency*), misalnya perbuatan cabul.

2. Penggolongan kejahatan untuk membantu teori penggolongan didasarkan akan adanya kelas-kelas kejahatan dan beberapa menurut

proses penyebab kejahatan itu, yaitu cara melakukan kejahatan teknik- teknik dan organisasinya dan timbul kelompok-kelompok yang mempunyai nilai nilai tertentu. Kelas-kelas tersebut sebagaimana ditulis oleh A.S. Alam⁹ sebagai berikut :

- a) *Profesional crimes*, yaitu kejahatan yang dilakukan sebagai mata pencaharian tetapnya dan mempunyai keahlian tertentu untuk proses itu, misalnya pemalsuan uang, tanda tangan dan pencopetan.
- b) *Organized crimes*, yaitu suatu kejahatan yang teroganisir, misalnya pemerasan, perdangan narkoba dan obat-obatan terlarang.
- c) *Occasional crimes*, yaitu suatu kejahatan karena adanya suatu kesepakatan, misalnya pencurian di rumah secara bersama.

3. penggolongan kejahatan yang dilakukan oleh nilai-nilai sosiologi yang dikemukakan oleh A.S. Alam sebagai berikut:

- a) *Violent personal crimes*, yaitu kejahatan kekerasan terhadap orang, misalnya pembunuhan (murder), pemerkosaan (rape) dan penganiayaan (assault).
- b) *Occasional property crimes*, yaitu kejahatan harta benda karena kesepakatan, misalnya pencurian kendaraan bermotor, pencurian di toko- toko besar.
- c) *Occupational crimes*, yaitu kejahatan karena kedudukan atau jabatan, misalnya korupsi.

⁹ .*Ibid*, Hal 7

- d) Politic crimes, yaitu kejahatan politik, misalnya pemberontakan sabotase, perang gerilya dan lain-lain.
- e) Public order crimes, yaitu kejahatan terhadap ketertiban umum yang biasa disebut dengan kejahatan tanpa korban, misalnya pemabukan, wanita melacurkan diri.
- f) Conventional crimes, yaitu kejahatan konvensional, misalnya perampokan (robbery), pencurian kecil-kecilan (larceny), dan lain-lain.
- g) Organized crimes, yaitu kejahatan yang terorganisir, misalnya perdagangan wanita untuk pelacuran, perdagangan obat bius.
- h) Professional crimes, yaitu kejahatan yang dilakukan sebagai profesinya, misalnya pemalsuan uang, pencopet, dan lain-lain.

Selanjutnya untuk mengetahui kejahatan yang terjadi di masyarakat, diperlukan adanya statistik kejahatan. Statistik kejahatan merupakan statistik yang paling sempurna. Adapun hal-hal yang menyebabkan kesulitan di dalam menyusun statistik kejahatan¹⁰ adalah sebagai berikut :

- a. Tidaklah mungkin mengetahui dengan pasti jumlah kejahatan yang terjadi di dalam setiap daerah peradilan pada suatu waktu tertentu.

¹⁰ .Ibid. Hal 13

- b. Kadang-kadang suatu tindakan dicap sebagai kejahatan, sebaliknya bukan kejahatan oleh peneliti lain.
- c. Merupakan kenyataan sehari-hari bahwa banyak kejahatan yang terjadi tanpa diketahui oleh yang berwenang.

C. Tindak Pidana Cyber Crime

1. Definisi Cyber Crime

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

- a) Penggunaan komputer untuk melaksanakan perbuatan penipuan, pencurian atau penyembunyian yang dimaksud untuk memperoleh keuntungan keuangan, keuntungan bisnis, kekayaan atau pelayanan;
- b) Ancaman terhadap komputer itu sendiri, seperti pencurian perangkat keras atau lunak, sabotase dan pemerasan.¹¹

Sistem teknologi informasi berupa internet telah dapat menggeser paradigma para ahli hukum terhadap definisi kejahatan

¹¹ Sahariyanto, Budi. 2012. Tindak Pidana Teknologi Informasi (Cyber crime) Urgensi Pengaturan dan Celah Hukumnya. Jakarta: Rajawali Pers. Hlm 10.

komputer, pada awalnya para ahli hukum terfokus pada alat/perangkat keras yaitu komputer. Namun dengan adanya perkembangan teknologi informasi berupa jaringan internet, maka fokus dari identifikasi terhadap definisi cyber crime lebih diperluas lagi yaitu seluas aktivitas yang dapat dilakukan di dunia *cyber*/maya melalui sistem informasi yang digunakan. Jadi tidak sekedar pada komponen hardware-nya saja kejahatan itu dimaknai sebagai cyber crime, tetapi sudah dapat diperluas dalam lingkup dunia yang dijelajah oleh sistem teknologi informasi yang bersangkutan. sehingga lebih tepat jika pemaknaan dari cyber crime adalah kejahatan teknologi informasi, juga sebagai kejahatan mayantara.¹²

Pada dasarnya cyber crime meliputi semua tindak pidana yang berkenaan dengan sistem informasi itu sendiri, serta sistem informasi yang merupakan sarana untuk penyampaian/pertukaran informasi kepada pihak lainnya.¹³

2. Karakteristik Cyber Crime

Kejahatan dibidang teknologi informasi dapat digolongkan sebagai white colour crime karena pelaku cyber crime adalah orang yang menguasai penggunaan internet beserta aplikasinya atau ahli di bidangnya. Kejahatan tersebut sering kali dilakukan secara transnasional atau melintasi batas negara sehingga dua kriteria kejahatan melekat sekaligus dalam kejahatan cyber ini, yaitu white colour crime dan transnational crime.

¹² .Ibid Hal 11.

¹³ .Ibid Hal 12

Berdasarkan beberapa literature serta praktiknya, cyber crime memiliki beberapa karakteristik, yaitu:¹⁴

- a) Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah siber/cyber space, sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.
- b) Perbuatan tersebut dilakukan dengan menggunakan peralatan apa pun yang terhubung dengan internet.
- c) Perbuatan tersebut mengakibatkan kerugian materiil maupun inmateriil (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
- d) Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
- e) Perbuatan tersebut sering dilakukan secara transnasional/melintasi batas negara

3. Bentuk-Bentuk Cyber Crime

Kejahatan computer dapat diklasifikasikan sebagai berikut:

- a) Kejahatan yang menyangkut data atau informasi computer.
- b) Kejahatan yang menyangkut software atau program computer.

¹⁴ .Ibid Hal 13

- c) Pemakaian fasilitas computer tanpa wewenang untuk kepentingan yang tidak sesuai dengan tujuan pengelolaan atau operasinya.
- d) Tindakan-tindakan yang mengganggu operasi computer.
- e) Tindakan merusak peralatan computer atau peralatan yang berhubungan dengan computer atau sarana penunjangannya.

Secara umum terdapat beberapa bentuk kejahatan yang berhubungan erat dengan penggunaan teknologi informasi yang berbasis utama computer dan jaringan telekomunikasi, antara lain:¹⁵

a. Unauthorized acces to computer system and service

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.

b. 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.

c. Data forgery

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet.

¹⁵ .Ibid hal 15

d. *Cyber espionage*

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain. dengan memasuki sistem jaringan computer pihak sasaran.

e. *Cyber sabotage and extortion*

Kejahatan ini dilakukan dengan membuat gangguan perusakan atau penghancuran terhadap suatu data, program computer atau sistem jaringan computer yang terhubung dengan internet.

f. *Offense against intellectual property*

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Seperti peniruan tampilan pada web page suatu situs milik orang lain secara illegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain dan sebagainya.

g. *Infrengmentsofprivacy*

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan seseorang pada formulir data pribadi yang tersimpan secara computerized, yang apabila diketahui oleh orang lain akan dapat merugikan korbannya secara materiil maupun immaterial seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

D. Tindak Pidana Cyber Crime Di Indonesia

Kejahatan (cyber crime) yang marak di Indonesia meliputi penipuan kartu kredit, penipuan perbankan, *defacing*¹⁶, *cracking*¹⁷, transaksi seks, pornografi, judi online, penyebaran berita bohong melalui internet dan terorisme. Terdapat beberapa jenis kasus cyber crime yang banyak terjadi di Indonesia berdasarkan modusnya, yaitu:

1. Pencurian Nomor Kredit

Menurut Rommy Alkatiry, penyalahgunaan kartu kredit milik orang lain di internet merupakan kasus cyber crime terbesar yang berkaitan dengan dunia bisnis internet di Indonesia. Penyalahgunaan kartu kredit milik orang lain memang tidak terlalu rumit dan bisa dilakukan secara fisik atau online. Nama dan kartu kredit orang lain yang diperoleh di berbagai tempat (restaurant, hotel, atau segala tempat yang melakukan transaksi pembayaran dengan kartu kredit) dimasukkan di aplikasi barang di internet.¹⁸

2. Memasuki, Memodifikasi, atau Merusak Homepage (hacking)

Seiring tahun berlalu, kasus hacking atau peretasan semakin sering terjadi. Kasus peretasan umumnya bertujuan untuk mengambil data-

¹⁶Defacing merupakan bagian dari kegiatan hacking web atau program application, yang menfokuskan target operasi pada perubahan tampilan dan konfigurasi fisik dari web atau program aplikasi tanpa melalui source code program tersebut. Diakses di Profesiti.blogspot.com/p/category-cybercrime pada tanggal 15 Oktober 2022, pukul 14:23 Wita

¹⁷Cracking merupakan kegiatan membobol suatu sistem computer dengan tujuan mengambil informasi penting. Diakses di cybercrime4c.blogspot.com/2013/06/apa-yang-dimaksud-cracking pada tanggal 15 Oktober 2022 pukul 14:10 Wita

¹⁸Suhariyanto, Budi. Loc cit.hlm 18

data tertentu yang dimiliki target. Tapi ada juga peretasan yang bertujuan menghancurkan data atau sistem tertentu sehingga berdampak seperti kerusakan digital.¹⁹

Menurut John. S. Tumiwa pada umumnya tindakan hacker Indonesia belum separah aksi di luar negeri. Perilaku hacker Indonesia masih sebatas masuk ke suatu situs komputer orang lain yang ternyata rentan penyusupan dan memberitahukan kepada pemiliknya untuk berhati-hati. Di luar negeri *hacker* sudah memasuki system perbankan dan merusak data base bank.²⁰

3. Penyerangan Situs atau e-mail melalui Virus atau Spamming

Spamming merupakan system pengiriman pesan/berita iklan secara massal dan seringkali *Spammers* (pelaku *spamming*) mengirimkan spam-nya secara bertubi-tubi dalam jumlah yang banyak dan tanpa kehendak si penerima.

Spam dikirimkan oleh pengiklan dengan biaya operasional yang sangat rendah, karena spam tidak memerlukan senarai²¹ (maling list) untuk mencapai para pelanggan yang diinginkan. Karena hambatan masuk rendah maka banyak *spammer* yang muncul dan jumlah pesan yang tidak diminta menjadi sangat tinggi. Akibatnya, banyak pihak yang

¹⁹ <http://tekno.kompas.com/read/2014/12/29/09190067/7.Kasus.Hacking.Paling.Heboh.di.2014> yang diakses pada tanggal 15 Oktober 2022, Pukul 14:02 Wita

²⁰ Suhariyanto, Budi. Op cit.hlm 18

²¹ Senarai atau list merupakan struktur data yang terdiri atas rangkaian elemen sejenis yang saling berhubungan atau bersifat reruntunan (sequence). Diakses di <http://slideplayer.info/slide/4106324/>

dirugikan, selain pengguna internet itu sendiri, ISP (penyelenggara jasa internet atau internet *service provider*), dan masyarakat umum juga merasa tidak nyaman. *Spam* sering mengganggu dan terkadang menipu penerimanya.²²

Berikut ini beberapa contoh kasus spam yang terjadi di Indonesia:

a) Kasus penipuan yang dialami beberapa korban yang juga merupakan konsumen dan juga pengguna situs jual beli di dunia maya, seperti:²³

1) Kasus yang bersumber dari postingan F David Talalo, diforum fotografer. net, dimana korban memberikan informasi mengenai dirinya yang telah menjadi korban penipuan.

“Baru baru ini saya tergiur dengan iklan penawaran kamera digital SLR disitus tokobagus.com disitu ditawarkan oleh seorang pengiklan bernama charleszhangyg berdomisili di medan, kamera Nikon D200 body only hanya seharga 2,8jt. Pengiklan menyertakan alamat lengkap beserta nama toko - Miracle Komputer di Shopping Centre YUKI Suka Ramai Lt.2 no.29 dan nomor telepon 061-76503903. Bodohnya, saya terlanjur mentransfer uang sejumlah 2,8jt ke rekening milik bpk.Syukran. Baru kemudian setelah itu konfirmasi dari pihak

²²<https://bigswamp.wordpress.com/2011/03/02/kasus-kasus-cyber-crime-part-1-spamming/> yang diakses pada tanggal 4 Januari 2017, Pukul 14:35 Wita

²³ <http://berbagi100persen.blogspot.co.id/2013/06/kasus-spamming.html> yang diakses pada tanggal 19 Oktober 2022, Pukul 14:27 Wita

mall dimedan menyatakan bahwa toko itu sudah tutup. Barang tidak sampai, nota pembelian pun tidak difax. “

2) Kasus yang bersumber dari facebook toko bagus yang beralamat facebook.com/tokobagus, dimana korban memberikan informasi mengenai dirinya yang telah menjadi korban penipuan.

"Saya ditipu, saya kemaren membeli BB torch 9800 dan sudah mentransfer sejumlah Rp.800.000,- Ke BRI dengan NO REK 530601012007534 AN. RICKY EDISYAH PUTRA dengan nomor HP 085760868349 setelah uang ditransfer HP tidak aktif dan barang pun tidak diterima, saya sangat kecewa setelah belanja OL di situs tokobagus.com"

a) Kasus penipuan yang akibat spamming melalui email hingga mengalami kerugian milyaran rupiah seperti kasus berikut ini.²⁴

Penipuan yang terjadi terhadap seorang rektor Universitas Swasta di Jakarta dengan kerugian sejumlah 1,8 miliar. Kasus tersebut bermula ketika pada tanggal 3 september 2007 rektor tersebut menerima sebuah email yang berisi penugasan seorang warga Nigeria yang bernama Prince Shankamoye yang membawa barang senilai US\$ 25 Juta Ke Indonesia. Barang yang bernilai mahal tersebut milik seorang pengusaha Jerman yang telah mengalami kecelakaan pesawat di Perancis, namun terdapat syarat untuk mendapatkan barang berharga tersebut dimana rektor tersebut diminta untuk menyetorkan uang senilai Rp 1,8miliar untuk biaya administrasi.

²⁴ <http://berbagi100persen.blogspot.co.id/2013/06/kasus-spamming.html> yang diakses pada tanggal 19 Oktober 2022, Pukul 14:27 Wita

Untuk lebih meyakinkan sang korban, Prince ShankaMoye menggunakan sebuah tipu muslihat dimana pelaku mengetahui secara detail mengenai pekerjaan sang rektor, "Dia tahu betul pekerjaan saya. Dia tahu saya pernah kerja di PBB dan membantu proyek kemanusiaan. Makanya saya tertarik dan percaya." kata rektor yang minta agar nama dan universitasnya dirahasiakan ini di Polda Metro Jaya, Jakarta, Rabu (26/9/2007). Setelah masuk perangkap si pelaku, rektor tersebut mentransfer sejumlah uang ke rekening Moye. Rektor tersebut diperintahkan untuk mentransfer uang Rp 56,7Juta ke BCA Cabang Mandala pada 6 September 2007.

Kemudian pada hari yang sama, rektor tersebut bertemu dengan Moye dan dimintai uang Rp 350 juta. Pertemuan tersebut berlanjut, Rektor dan Moye bertemu kembali pada 7 September di Hotel Mulia, Senayan Jakarta. Korban mengatakan "Sudah menjual 2 rumah dan hasil kerja 40 tahun musnah. Saya terlalu mengebu-gebu mendapatkan barang itu. Saya ingin membangun kampus yang membutuhkan dana besar, ".Setelah uang Rp 1,8 miliar selesai ditransfer, karena barang berharga yang dijanjikan tidak kunjung didapatkan, rektor tersebut akhirnya melaporkan modus penipuan ini ke Polda Metro Jaya. Karena itu, melihat sejarah kasus spamming di Indonesia dari jumlah presentasi dari tahun ke tahun semakin mengkhawatirkan dan melihat macam-macam kerugian atau dampak yang ditimbulkan maka wajar apabila jenis kejahatan ini dikriminalisasikan.

4. Defacing

Defacing merupakan kegiatan mengubah halaman situs/website pihak lain, seperti yang terjadi pada situs menkominfo dan partai Golkar serta BI beberapa waktu lalu dan situs KPU saat pemilu 2004. Tindakan deface ada yang semata-mata iseng, unjuk kebolehan, pamer kemampuan membuat program, tapi ada juga yang melakukannya untuk mencuri data dan dijual kepada pihak lain.²⁵

E. Tindak Pidana Penipuan

1. Pengertian Penipuan

Dalam Kamus Besar Bahasa Indonesia, disebutkan bahwa tipu berarti kecoh, daya cara, perbuatan atau perkataan yang tidak jujur (bohong, palsu, dsb), dengan maksud untuk menyesatkan, mengakali, atau mencari untung. Penipuan berarti proses, perbuatan, cara menipu, perkara menipu (mengecoh). Dengan demikian maka berarti bahwa yang terlibat dalam penipuan adalah dua pihak yaitu orang menipu disebut dengan penipu dan orang yang ditipu disebut sebagai tertipu. Jadi penipuan dapat diartikan sebagai suatu perbuatan atau membuat, perkataan seseorang yang tidak jujur atau bohong dengan maksud untuk menyesatkan atau mengakali orang lain untuk kepentingan dirinya atau kelompok (Ananda S, 2009 : 364).

²⁵ Suhariyanto, Budi. Op cit. Hal 140.

Selanjutnya dalam pengertian yuridis, pengertian penipuan termasuk kedalam rumusan tindak pidana didalam KUHP, namun demikian rumusan penipuan dalam KUHP bukan merupakan suatu definisi melainkan hanyalah untuk menetapkan unsur-unsur suatu perbuatan sehingga dapat dikatakan sebagai penipuan dan pelakunya dapat dipidana.

Pasal 378 menyatakan bahwa *“Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hak, mempergunakan nama palsu atau sifat palsu ataupun mempergunakan tipu muslihat atau susunan kata-kata bohong, menggerakan orang lain untuk menyerahkan suatu benda atau mengadakan suatu perjanjian hutang atau meniadakan suatu piutang, karena salah telah melakukan penipuan, dihukum dengan hukuman penjara selama-lamanya empat tahun”*.²⁶

Lamintang mengatakan bahwa “Kejahatan penipuan atau “bedrog” diatur di dalam Pasal 378- 395 KUHP, Buku II Bab ke XXV”.²⁷ Di dalam Bab ke XXV tersebut dipergunakan perkataan “Penipuan” atau “Bedrog”, karena sesungguhnya didalam bab tersebut diatur sejumlah perbuatan- perbuatan yang ditujukan terhadap harta benda, dalam mana oleh si pelaku telah dipergunakan perbuatan-perbuatan yang bersifat menipu atau dipergunakan tipu

²⁶ Republik Indonesia, Kitab Undang-Undang Hukum Pidana.

²⁷ P.A.F. Lamintang, 1997, *Dasar-Dasar Hukum Pidana Indonesia* (Bandung: PT. Citra Aditya Bakti). Hal. 262.

muslihat.²⁸

2. Unsur-unsur Tindak Pidana Penipuan

Menurut ahli hukum pidana Azni Zainal Abiudin Farid (1961 : 135), bahwa unsur-unsur tindak pidana penipuan yang terkandung dalam pasal 378 tersebut yaitu:

- a). Membujuk (menggerakkan hati) untuk
- b). Menyerahkan (*afgifte*) suatu barang atau supaya membuat suatu hutang atau menghapus suatu hutang
- c). Dengan menggunakan upaya-upaya atau cara-cara
 1. memakai nama palsu
 2. memakai kedudukan palsu
 3. memakai tipu muslihat
 4. memakai rangkaian kata-kata bohong
- d). Dengan maksud hendak menguntungkan diri sendiri atau orang lain dengan membawa hukum

Sedangkan unsur-unsur tindak pidana penipuan menurut Moeljatno (2002:70) adalah sebagai berikut:

- a). Ada seseorang yang dibujuk atau digerakka untuk menyerahkan suatu barang atau membuat hutang atau menghapus piutang. Barang itu diserahkan oleh yang punya dengan jalan tipu muslihat. Barang yang diserahkan itu tidak selamanya harus kepunyaan sendiri, tetapi juga kepunyaan orang lain.

²⁸ Ibid. Hal 262.

- b). Penipu itu bermaksud untuk menguntungkan dirinya sendiri atau orang lain tanpa hak. Dari maksud itu ternyata bahwa tujuannya adalah untuk merugikan orang yang menyerahkan barang itu.
- c). Yang menjadi korban penipuan itu harus digerakkan untuk menyerahkan barang itu dengan jalan:
 - 1). Penyerahan barang itu harus akibat dari tindakan tipu daya.
 - 2). Si penipu harus memperdaya si korban.

BAB III

METODE PENELITIAN

A. Tipe Penelitian

Jenis penelitian yang akan digunakan dalam penelitian ini adalah penelitian Hukum empiris, yaitu penelitian dengan adanya data lapangan sebagai sumber data utama, seperti hasil wawancara dan observasi. Penelitian empiris digunakan untuk menganalisis hukum yang dilihat sebagai perilaku masyarakat yang berpola dalam kehidupan masyarakat yang selalu berinteraksi dan berhubungan dalam aspek kemasyarakatan.²⁹

B. Lokasi Penelitian

Penelitian ini dilakukan di kota Makassar, yaitu di POLDA Sulawesi Selatan . Pemilihan lokasi pelaksanaan penelitian ini berdasarkan pada pertimbangan bahwa POLDA Sulawesi Selatan unit Reskrimsus merupakan institusi yang menangani kasus Penipuan Online.

C. Jenis dan Sumber Data

Jenis dan sumber data yang di gunakan dalam penelitian ini adalah senagai berikut:

1. Data primer, adalah data yang diperoleh langsung dari lokasi

²⁹ Bambang Sunggono, Metode Pnelitian Hukum (Jakarta: PT Raja Granfindo Persada, 2003, Hal 43.

penelitian

2. Data Sekunder, adalah data yang diperoleh melalui studi kepustakaan.

D. Populasi dan Sampel

Populasi adalah keseluruhan atau himpunan obyek penelitian dengan ciri yang sama. Populasi dapat himpunan orang, benda (hidup atau mati), gejala-gejala, tingkah laku, pasal perundang-undangan, kasus-kasus hukum, waktu atau tempat, alat-alat pengajaran, cara-cara dan sebagainya, dengan ciri dan sifat yang sama.

Berdasarkan jenis data yang diperlukan maka dalam penelitian ini, yang dijadikan partisipan oleh peneliti adalah objek yang dijadikan sumber data dalam penelitian yang bentuknya dapat berupa manusia, benda-benda, dokumen-dokumen dan sebagainya. Dengan demikian berdasarkan permasalahan yang ada dalam penelitian ini, maka yang menjadi sumber data yaitu Penyidik Cyber Crime Reskrimsus Polda Sulsel.

Sampel adalah bagian dari jumlah dan karakteristik yang dimiliki oleh populasi tersebut (sugiyono, 2008). Adapun sampel dari penelitian tersebut adalah 2 orang Penyidik Cyber Crime Reskrimsus Polda Sulsel dan 2 orang korban tindak penipuan online.

E. Teknik Pengumpulan Data

Teknik pengumpulan data yang penulis lakukan terbagi atas dua,

yaitu:

1. teknik wawancara, yaitu pengumpulan data secara langsung melalui Tanya jawab berdasarkan daftar pertanyaan yang telah disiapkan dan melakukan wawancara untuk memperoleh data dan informasi yang diperlukan.
2. teknik Stadi dokumen, yaitu teknik pengumpulan data dengan cara membaca dan mencatat dokumen dokumen arsip yang berkaitan dengan penelitian yang dikaji.

F. Analisis Data

Seluruh data yang diperoleh dari data primer dan Sekunder penulis selanjutnya diklasifikasikan dan dianalisis untuk menghasilkan kesimpulan dari data-data yang didapatkan sesuai dengan permasalahan yang dibahas. Metode yang digunakan dalam analisis data adalah analisis kualitatif, yaitu menguraikan data secara bermutu dalam bentuk kalimat yang teratur, runtun, logis, tidak tumpang tindih, dan efektif sehingga memudahkan interpretasi data dan analisis.

Selanjutnya kesimpulan-kesimpulan tersebut atau data-data yang diperoleh dari hasil analisis digunakan untuk mengkaji dan membahas permasalahan yang diteliti oleh penulis. Hal ini dimaksudkan untuk memperoleh pembahasan dan kesimpulan yang relevan dan tepat serta sesuai dengan permasalahan yang diteliti.

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

A. Faktor-faktor Yang Menyebabkan Terjadinya Kejahatan Penipuan Online

Telah dikemukakan sebelumnya dalam tinjauan pustaka bahwa terdapat faktor-faktor yang turut mempengaruhi maraknya *cyber crime* yaitu:

- a. Kurangnya kesadaran hukum masyarakat
- b. Masalah keamanan
- c. Aparat penegak hukum
- d. Undang-undang.

Kemajuan teknologi turut melatarbelakangi meningkatnya *cyber crime*. Selain adanya dampak positif, perkembangan teknologi juga memberikan dampak negatif. Menurut Didik M Arief Mansur dan Elisatris Gultom, munculnya kejahatan dengan menggunakan internet sebagai alat bantu yang lebih banyak disebabkan oleh faktor keamanan si pelaku dalam melakukan kejahatan.³⁰

Berikut ini akan dipaparkan faktor-faktor yang turut mempengaruhi efektivitas penegakan hukum dan upaya penanggulangan *cyber crime*, berdasarkan hasil penelusuran data referensi, maka penulis akan memfokuskannya pada beberapa faktor ekonomi, faktor

³⁰ Didik M Mansur dan Allsatris Gultom, *Cyber law – Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung, 2005. Hal 95

lingkungan, factor sosial budaya dan faktor intelektual.

1. Faktor Ekonomi

Salah satu yang mendorong terjadinya kejahatan ini adalah rendahnya tingkat pendidikan dari orang yang melakukan kejahatan ini, sehingga mengakibatkan pasaran tenaga kerja tidak dapat menyerap keahliannya dengan alasan rendahnya tingkat pendidikan. Hal tersebut mengakibatkan pelaku kejahatan menjadi pengangguran. Karena menjadi pengangguran dan kesulitan untuk memenuhi kebutuhan sehari-hari maka pelaku kejahatan tersebut terdorong untuk mencari jalan pintas guna mendapatkan penghasilan demi memenuhi kebutuhannya. Bukannya mencari pekerjaan yang halal tapi justru lebih tergiur untuk melakukan kejahatan demi mendapatkan uang. Salah satu kejahatan yang cenderung mudah dilakukan yaitu seperti melakukan penipuan online berbasis cyber. Selain itu juga pelaku melakukan pemerasan, bahkan sampai pada tingkat pembobolan atau pencurian mengingat media yang digunakan cukup mudah diakses dan sulit dilacak.

Dengan demikian, perkembangan cyber crime di Indonesia merupakan fakta sosial yang harus dicegah, ditindak dan ditanggulangi. Dengan bertambahnya pengguna internet maka kemungkinan terjadinya cyber crime akan semakin terbuka apalagi terdorong oleh tuntutan ekonomi yang mendesak.

2. Faktor Lingkungan

Hubungan antara faktor ekonomi dan factor lingkungan sangat kuat, di mana pelaku yang awalnya tidak mempunyai pekerjaan akhirnya mulai belajar dari orang yang telah atau pernah melakukan cyber crime, yang masih memiliki hubungan keluarga ataupun pertemanan, karena berasal dari lingkungan atau daerah yang sama.

Lingkungan pergaulan turut menentukan pembentukan mental dan karakter seseorang. Seseorang yang pada awalnya bukan merupakan pelanggar hukum, akibat bergaul pada lingkungan yang sering melakukan pelanggaran hukum maka orang tersebut cenderung terdorong oleh lingkungannya dan akan menjadi pelanggar hukum. Fakta ini memperkuat teori asosiasi diferensial³¹ yang dikemukakan oleh Sutherland. Seseorang yang melakukan kejahatan cenderung diakibatkan oleh kondisi lingkungan sosialnya dimana pelaku telah belajar atau mendapat pelajaran dari lingkungannya bahwa tingkah laku kriminal atau perbuatan melanggar hukum lebih baik dan menguntungkan daripada tingkah laku non-kriminal atau melakukan perbuatan taat pada hukum.

³¹ Teori asosiasi diferensial atau differential association dikemukakan pertama kali oleh Edwin H Sutherland pada tahun 1934 dalam bukunya Principle of Criminology. Sutherland dalam teori ini berpendapat bahwa perilaku kriminal merupakan perilaku yang dipelajari dalam lingkungan sosial. Sumber: http://www.kompasiana.com/ariansyahekasaputra/teori-asosiasi-diferensial-differential-association-theory-dalam-kriminologi_54f96eaaa3331178178b4d9b Di akses pada 26 Desember 2022 Pukul 12:21 Wita

3. Faktor Sosial Budaya

Yang menjadi salah satu penyebab terjadinya cyber crime berdasarkan faktor sosial budaya dapat dilihat dari

berbagai aspek, yaitu:

1) Kemajuan teknologi informasi

Pesatnya kemajuan teknologi informasi di dunia ini sudah pasti tidak dapat dibendung oleh siapapun. Semua orang membutuhkan teknologi informasi, bahkan mayoritas masyarakat dunia internasional sudah menganggapnya sebagai suatu kebutuhan primer. Saat ini teknologi informasi memainkan peranan penting dalam kesejahteraan manusia, termasuk pertumbuhan ekonomi, politik, budaya, dan aspek kehidupan lainnya.

2) Sumber Daya Manusia (SDM)

Sumber daya manusia memiliki peranan penting sebagai operator yang mengendalikan sebuah alat, karena operator memiliki peranan penting sebagai pengontrol atau pengendali alat. Selanjutnya tergantung dari si operator apakah alat itu akan digunakan sebagai sarana untuk melakukan hal-hal yang bermanfaat untuk kelangsungan hidup manusia, atau sebaliknya, digunakan sebagai sarana perbuatan menyimpang yang dapat membawa kerugian bagi kelangsungan hidup manusia lainnya.

Di Indonesia sendiri sumberdaya pengelola teknologi informasi sudah banyak namun masih sebatas pengguna saja belum mampu

untuk memproduksi sendiri karena masih dibatasi oleh biaya penelitian dan kurangnya apresiasi terhadap peneliti-peneliti terkait di bidang teknologi dan informasi.

3) Munculnya fenomena komunitas baru.

Dengan adanya teknologi sebagai suatu sarana elektronik untuk mencapai suatu tujuan, di antaranya internet sebagai suatu media untuk berkomunikasi, secara sosiologis terbentuklah komunitas baru di internet atau dunia maya yang saling menghubungkan para pengguna dalam berkomunikasi. terdapat dua sisi yang saling melatarbelakangi, yaitu sisi komunitas di antara para pelaku cyber crime dimana mereka saling berkomunikasi untuk keperluan modus operandi mereka, serta sisi lainnya di mana pelaku cyber crime melakukan modus operandi mereka dengan menggunakan social media seperti Facebook atau Instagram dan Whatsapp untuk mendapatkan korban.

4. Faktor Intelektual

Faktor intelektual memiliki hubungan yang erat dengan faktor-faktor yang telah penulis sebutkan di atas. Faktor intelektual ini dilatarbelakangi oleh kemampuan orang yang terlebih dahulu menjadi pelaku cyber crime, yang kemudian mengajarkan atau menularkan kemampuannya kepada orang lain yang berada disekitarnya atau memiliki keadaan yang sama dengannya. Bahkan terkadang pelaku cyber crime masih tergolong newbie atau pemula

yang baru mulai melakukan tindakan-tindakan kejahatan dari tingkatan terkecil hingga terbesar akibat didorong dengan faktor intelektual yang cenderung disalahgunakan.

B. Upaya Penanggulangan Kejahatan Penipuan Online oleh Pihak Kepolisian

Dalam menanggulangi terjadinya kasus cyber crime, pihak kepolisian telah melakukan berbagai upaya penanggulangan cyber crime. Berdasarkan wawancara penulis dengan IPDA Syamsul Bahri selaku panit 2 unit 2 di Cyber crime Reskrimsus Polda Sulsel pada Kamis 29 Desember 2022 yang menyatakan bahwa pihak kepolisian telah melakukan upaya-upaya penanggulangan yang bersifat preventif dan represif.

1. Upaya Preventif

Dalam melakukan upaya preventif ini pihak kepolisian khususnya unit cyber crime Polda Sulsel telah melakukan berbagai upaya seperti memberikan himbauan ke masyarakat melalui media elektronik maupun media sosial dengan menyebarkan broadcast berupa himbauan-himbauan terkait cyber crime untuk di forward ke masyarakat luas. Selain itu dilakukan juga penerangan ke masyarakat melalui media surat kabar dan radio, serta pada saat mengisi acara talkshow pihak kepolisian tidak henti-hentinya memberikan himbauan ke masyarakat.

Pihak kepolisian juga menjalankan fungsi teknis yang khusus

menangani kasus cyber crime, yaitu dengan melakukan penegakan aturan, melakukan penjagaan di lokasi-lokasi yang diduga sering terjadi kasus cyber crime dan melakukan patroli cyber rutin di dunia maya seperti media-media sosial untuk mencari para pelaku kejahatan dunia maya.

2. Upaya Represif

Dalam melakukan upaya represif ini, pihak kepolisian dalam hal ini, subdit cyber telah mengambil tindakan dengan memproses setiap kasus cybercrime yang ditangani sesuai dengan aturan yang berlaku.

Pihak kepolisian bekerja sama dengan stakeholder yang ada yaitu bagaimana menangkap pelaku yang tertangkap tangan melakukan kejahatan ataupun melalui laporan masyarakat kemudian mendatangi tempat kejadian perkara (TKP) guna melakukan penangkapan dan penahanan terhadap tersangka kasus cyber crime, setelah dilakukan penangkapan kemudian diproses dikepolisian dan sebelum dilimpahkan berkas perkaranya ke kejaksaan terlebih dahulu diadakan konferensi pers dengan media dimana pihak media hadir untuk mewawancarai tersangka dan petugas yang menangani kasus tersebut. Lalu hasil wawancara tersebut disiarkan atau disebarkan kemasyarakat luas, sehingga masyarakat akan mengetahui kasus-kasus yang ditangani oleh aparat kepolisian khususnya kepolisian Polda Sulsel.

3. Pelaksanaan Undang-Undang Informasi dan Transaksi Elektronik Terhadap Kejahatan Cyber Crime

Undang-undang ITE (Informasi dan Transaksi Elektronik) merupakan salah satu peranti hukum di bidang cyberspace atau dunia maya yang diharapkan dapat mengakomodir segala persoalan yang menyangkut kejahatan atau pelanggaran di dunia maya (cyber crime). Undang-undang ITE berperan sangat penting dalam pemberantasan tindak pidana cyber crime di Indonesia. Selain memuat perlindungan hukum terhadap pemakai jasa internet juga memuat ancaman sanksi terhadap pelaku kejahatan cyber crime.

Dalam menghadapi cyber crime, hukum positif di Indonesia masih bersifat *lex locus delicti*. Namun beda halnya dengan situasi dan kondisi pelanggaran hukum yang terjadi atas cyber crime dimana pelaku kejahatan cyber dan korban berada di tempat yang berbeda. Wilayah kejahatan dunia maya yang begitu luas namun mudah diakses menyebabkan maraknya terjadi kejahatan.

Kepolisian Republik Indonesia (POLRI) sebagai salah satu alat kelengkapan negara dalam menegakkan hukum tidak dapat lagi tinggal diam setelah lahirnya UU no. 11 tahun 2008 tentang informasi dan transaksi elektronik. Aparat penegak hukum dalam hal ini penyidik kepolisian harus bergerak secara aktif untuk menindak kejahatan di dunia maya. Aparat kepolisian harus dapat menangani kasus-kasus kejahatan yang terjadi di dunia maya.

Berikut ini akan dipaparkan beberapa kasus cyber crime yang telah ditangani oleh Kepolisian Daerah Sulawesi Selatan tahun 2020 - 2022:

Tabel 1. Jumlah Kasus Cyber Crime yang ditangani Polda Sulsel

No	KASUS	TAHUN 2020	TAHUN 2021	TAHUN 2022
1.	Pornografi dan/atau Pelanggaran Kesusilaan	7	5	6
2.	Penghinaan / Pencemaran Nama Baik	110	53	25
3.	Pemerasan dan/atau Pengancaman	6	6	4
4.	Penipuan Online dan Pinjaman Online	67	74	61
5.	Penyebaran Berita Bohong dan Penyesatan	8	13	9
6.	Hacking	9	7	6

Sumber : Data Penanganan Kasus Subdit Cyber Crime Polda Sulsel

- a. Pornografi dan/atau Pelanggaran Kesusilaan Melalui Media Elektronik (Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 27 Ayat 1)

Saat ini masalah pornografi dan pornoaksi sangat memprihatinkan, dan memiliki dampak negatif yang sangat nyata. Orang-orang yang menjadi korban kejahatan kesusilaan ini tidak hanya perempuan dewasa tetapi banyak korban yang masih anak-anak baik perempuan maupun laki-laki. Para pelakunya pun bukan hanya orang yang tidak dikenal, atau orang yang tidak mempunyai hubungan kekeluargaan dengan korban, diantaranya pelaku masih memiliki hubungan darah, atau hubungan

semenda, hubungan profesi, hubungan kerja, hubungan tetangga, bahkan sampai pada hubungan pendidikan dengan korban.³²

Masalah pornografi dan pornoaksi di Indonesia telah melampaui ambang toleransi dan merusak akhlak bangsa. Namun sangat disayangkan penyelesaian terhadap masalah pornografi yang menyangkut kesusilaan ini belum sesuai dengan yang diharapkan. Kenyataan itu dapat dilihat berdasarkan tabel 1 di atas dimana jumlah kasus pornografi dan/atau pelanggaran kesusilaan melalui media elektronik yang ditangani oleh unit cyber crime Polda Sulsel yaitu sekitar 18 kasus dari rentan waktu 2020 hingga 2022. Jumlah tersebut penulis nilai sangat minim mengingat banyaknya pornoaksi bahkan pelanggaran kesusilaan yang beredar di internet khususnya pada media sosial. Hal tersebut beralasan mengingat kurangnya pengetahuan dari masyarakat tentang pentingnya menjaga etika baik itu tingkah laku maupun penyebaran pict berupa gambar, suara, dan video pada media sosial yang tidak bermuatan atau mengandung unsur pelanggaran kesusilaan.

Pelanggaran kesusilaan pada media elektronik dan dunia maya merupakan perbuatan yang dilarang sebagaimana diatur dalam Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pasal 27 ayat (1) yang berbunyi sebagai berikut.

“Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi

³² Suhariyanto, Budi. *Op Cit.* hal 104

Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.”

Pasal tersebut memiliki sanksi pidana yang ditentukan dalam Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 45 ayat (1), yang berbunyi:

“Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.1.000.000.000,00 (satu miliar rupiah).”

- b. Penghinaan/Pencemaran Nama Baik di Internet (Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 27 ayat 3 UU ITE)

Seiring dengan perkembangan teknologi, maka kejahatan pun berkembang mengikuti perkembangan teknologi tersebut. Jika dahulu orang hanya bisa melakukan penghinaan dan pencemaran nama baik lewat tulisan surat atau perkataan lisan, sekarang dengan adanya media internet seseorang bisa juga melakukan penghinaan dan/atau pencemaran nama baik melalui media internet.³³

Penghinaan dan pencemaran nama baik di dunia maya ini merupakan masalah yang sangat populer dan paling sering terjadi di internet khususnya pada media-media sosial dimana banyak orang-orang yang mem-posting status bahkan komentar-komentar yang berisi

³³ *Ibid.* hal 116

penghinaan bahkan termasuk pencemaran nama baik. Polda sulsel telah menangani kasus penghinaan dan pencemaran nama baik sebanyak 188 kasus sejak tahun 2020 hingga 2022.

IPDA Syamsul Bahri panit 2 Unit 2 Cyber Crime Polda Sulsel menyatakan bahwa walaupun jumlah kejadian penghinaan dan pencemaran nama baik cukup sering terjadi di dunia maya namun penanganannya dinilai cukup menyulitkan dimana kebanyakan pelaku menggunakan nama samaran atau identitas palsu (akun fake) dalam menjalankan kejahatannya. Selain itu polisi kesulitan mengidentifikasi apakah status atau komentar yang di post memuat unsur penghinaan tanpa adanya laporan dari korban.

Penghinaan/pencemaran nama baik di internet dimuat dalam Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pasal 27 ayat (3) yang berbunyi:

“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.”

Pasal tersebut memiliki sanksi pidana yang ditentukan dalam Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 45 ayat (3) dan ayat (5), yang berbunyi:

“Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen elektronik yang memiliki muatan

penghinaan dan/atau pencemaran nama baik sebagaimana dimaksud dalam Pasal 27 ayat (3) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).”

- c. Pemerasan dan/atau Pengancaman Melalui Internet (Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 27 ayat 4 dan Pasal 29)

Dengan adanya media internet yang memiliki berbagai bentuk variasi program dalam berkomunikasi seperti email, blog, web, dan facebook, dapat digunakan sebagai sarana kejahatan berupa pemerasan dan/atau pengancaman. Hal tersebut dapat disebabkan karena identitas pengguna internet sangat sulit untuk diidentifikasi karena pengguna media sosial rentan untuk memanipulasi identitasnya demi kepentingannya masing-masing.

Dengan fenomena tersebut maka intensitas dan variasi kejahatan berupa terror sangat mudah dilakukan dan memiliki banyak sasaran yang potensial. Terror-terror tersebut dapat berupa pengancaman atau pemerasan. Di Sulawesi selatan sendiri kejahatan ini belum banyak terjadi mengingat kasus yang terlapor dan ditangani oleh Polda Sulsel dalam rentan tahun 2020-2022 sebanyak 16 kasus saja, hal tersebut dapat dikatakan bahwa kasus pemerasan dan pengancaman melalui media elektronik/internet masih minim terjadi di kawasan Sulawesi selatan.

Pemerasan dan/atau pengancaman yang dilakukan melalui

media internet diatur dalam Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pasal 27 ayat (4) yang berbunyi:

“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.”

Dan Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik 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 tersebut memiliki sanksi pidana yang ditentukan dalam Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 45 ayat (4), yang berbunyi:

“Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman sebagaimana dimaksud dalam Pasal 27 ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.1.000.000.000,00 (satu miliar rupiah).”

Dan Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 45B yang berbunyi:

“Setiap Orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak

Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).”

- d. Penipuan Online (Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 28 ayat 1)

Penipuan online dapat dilakukan dengan motivasi, yaitu untuk menguntungkan dirinya sendiri atau paling tidak untuk merugikan orang lain.³⁴

Berdasarkan tabel 1 yang telah dipaparkan sebelumnya Polda Sulsel telah menangani kasus penipuan online melalui media elektronik sebanyak 202 kasus.

IPDA Syamsul Bahri panit 2 unit 2 cyber crime Polda Sulsel mengungkapkan bahwa kejahatan ini terjadi dikarenakan korban cenderung mudah ditipu ataupun dibodohi oleh pelaku.

Perbuatan kejahatan penipuan online di dunia maya diatur dalam undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pasal 28 ayat (1) yang berbunyi :

“ Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik”

Adapun beberapa kasus yang terjadi di daerah Polda Sulsel, dalam Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi

³⁴ *Ibid.* hal 122

Elektronik :

- 1) Penipuan arisan online, Terhadap ATIK ANJANI KLAIN AMORITA dengan pelaku Pr. PHOEBEB ADELINE MI VANNY yang diduga telah melakukan modus membuat sebuah arisan online dengan menawarkan keuntungan namun arisan tersebut tidak berjalan. Pelaku mulai membuat arisan online kemudian mengajak para peserta/member untuk bergabung dengan arisan online tersebut melalui whatsapp dengan kata kata “arisan tembak 5jt/bulan namun arisan tersebut hanya berjalan 5 hari saja dan pelaku mengatakan bahwa tidak dapat melanjutkan arisan lagi dan tidak mau berurusan dengan arisan lagi dan tidak dapat membayar member/peserta arisan online tersebut. Akibat dari perbuatan pelaku yang telah melakukan penipuan terhadap korban, korban mengalami kerugian sebesar Rp. 5.350.000,.

e. Penyebaran Berita Bohong dan Penyesatan Melalui Media Elektronik

(Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 28 Ayat 2)

semakin sering terjadi menanggapi gejala sosial kemasyarakatan yang ada di lapangan. Dengan terbukanya akses informasi dan fasilitas-fasilitas penyebaran informasi di internet, maka kemungkinan perbuatan berita bohong dan penyesatan terhadap SARA di dunia maya akan marak terjadi.

Sulawesi selatan sendiri memiliki beberapa suku dan etnis serta beberapa penganut agama yang berbeda sehingga kerukunan antar perbedaan harus tetap dijaga. Dalam menjaga kerukunan tersebut tidak dipungkiri akan muncul isu-isu SARA untuk memecah belah persatuan masyarakat khususnya masyarakat Sulawesi Selatan. Mengingat media

yang digunakan cukup mudah diakses maka pihak kepolisian harus tanggap terhadap isu-isu SARA yang beredar di Internet. Kepolisian Daerah Sulawesi Selatan telah menangani sebanyak 30 kasus sejak tahun 2020- 2022.

Isu SARA merupakan hal yang sensitif sehingga harus cepat ditangani guna mampu menghindari terjadinya bentrokan yang mengatas namakan perbedaan.

Perbuatan profokasi terhadap SARA di dunia maya diatur dalam Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 28 ayat (2) yang berbunyi:

“Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA).”

Dan diancam dengan sanksi pidana dalam Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pasal 45A ayat (2) yang berbunyi:

“Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA) sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.1.000.000.000,00 (satu miliar rupiah).”

- f. Hacking (Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 30)

Salah satu bentuk kejahatan elektronik yang sering ditemukan adalah hacking atau cracking. Kejahatan ini dapat dilakukan dari dan dalam negeri. Semua tindakan yang dapat merugikan kepentingan orang yang dilindungi Indonesia, baik atas tindakan yang dilakukan dengan cara menggunakan atau mengakses komputer dan sistem elektronik lainnya, baik yang dimiliki secara privat atau yang dimiliki dan dilindungi oleh pemerintah, secara tanpa izin atau tanpa hak. Tujuannya adalah memperoleh, mengubah, merusak, atau menghilangkan informasi demi keuntungannya.³⁵

Oleh karena itu, hacking merupakan salah satu kegiatan yang bersifat negatif. Meskipun pada awalnya memiliki tujuan mulia, yaitu untuk memperbaiki sistem keamanan yang telah dibangun dan memperkuatnya, tetapi dalam perkembangannya hacking digunakan untuk keperluan- keperluan lain yang bersifat merugikan. Hal ini tidak terlepas dari penggunaan internet yang semakin meluas sehingga penyalahgunaan kemampuan hacking juga mengikuti luasnya pemanfaatan internet. Terdapat tahapan-tahapan hacking yang dapat dikonstruksikan sebagai kejahatan, yaitu:³⁶

- 1) Mengumpulkan dan mempelajari informasi yang ada mengenai

³⁵ *Ibid.* Hal 128

³⁶ *Ibid.* Hal 129

sistem operasi komputer atau jaringan komputer yang dipakai pada target sasaran.

- 2) Menyusup atau mengakses jaringan komputer target sasaran.
- 3) Menjelajahi sistem komputer (dan mencari akses yang lebih tinggi)
- 4) Membuat backdoor dan menghilangkan jejak.

Pada dasarnya perbuatan mengakses ke suatu sistem jaringan tanpa izin tersebut dapat dikategorikan sebagai perbuatan tanpa wewenang masuk dengan memaksa ke dalam rumah atau ruangan yang tertutup sehingga dianggap suatu kejahatan.

Terkait dengan kejahatan hacking ini Polda Sulsel telah menangani 22 kasus yang menyangkut keamanan privasi. Kasus-kasus tersebut ditangani berdasarkan laporan dari korban. Begitu banyaknya kejahatan hacking yang terjadi namun hanya sedikit yang dapat diproses hukum dikarenakan korban tidak menyadari bahwa sistem perangkat elektroniknya sedang dibobol selain itu pelaku tidak meninggalkan jejak sama sekali dalam melancarkan aksinya sehingga kegiatan hacking tidak dapat dideteksi.

Perbuatan hacking ini diatur dalam Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik 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 apapun.

- (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
- (3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Adapun sanksi yang dikenakan dari perbuatan hacking diatur dalam Undang-undang RI No. 19 Tahun 2016 tentang perubahan atas Undang-undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pasal 46, yang berbunyi:

- (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.600.000.000,00 (enam ratus juta rupiah).
- (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp.700.000.000,00 (tujuh ratus juta rupiah).
- (3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah).

Dalam penanganan cyber crime di wilayah hukum Polda Sulsel terdapat 6 (enam) jenis kejahatan siber yang telah ditangani oleh unit cyber crime reserse kriminal khusus Polda Sulsel dengan rincian berdasarkan tabel 1 dengan jumlah total kasus 476 yang telah atau sementara ditangani unit cyber crime.

Dari total 476 kasus yang telah maupun sedang dalam penanganan Reskrimsus Polda Sulsel sebagian besar sekitar 65,5%

merupakan pelanggaran terhadap Pasal 28 ayat (1) Undang-Undang ITE yang merujuk pada perbuatan menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam hal ini melakukan penipuan untuk merugikan orang lain dan menguntungkan diri sendiri maupun kelompok.

4. Kendala yang Dihadapi Aparat Kepolisian Dalam Upaya Penanggulangan Cyber Crime

Dalam upaya penanggulangan cyber crime oleh aparat kepolisian terdapat beberapa kendala yang menghambat upaya penanggulangan cyber crime, penulis kemudian membaginya ke dalam 4 aspek berdasarkan hasil wawancara dan penelusuran referensi, yaitu:

a. Aspek Penyidik

Penyidik kepolisian memiliki peran penting dalam upaya penanggulangan cyber crime, dimana kemampuan penyidik sangat dibutuhkan untuk mengungkap kasus- kasus cyber crime.

Adanya unit cyber crime dilingkungan kepolisian membuktikan bahwa dibutuhkannya penyidik khusus yang memiliki kemampuan di bidang informasi dan transaksi elektronik guna menangani kejahatan-kejahatan di dunia maya. oleh karena itu dibutuhkannya pendidikan khusus untuk memberikan pengetahuan terkait cyber kepada para penyidik yang khusus menangani masalah cyber crime.

b. Aspek Alat Bukti

Alat bukti dalam kasus cyber crime berbeda dengan alat bukti kejahatan lainnya dimana sasaran atau media cyber crime merupakan data-data atau sistem komputer / internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelaku kejahatan. Selain itu saksi korban dalam kasus cyber crime berperan sangat penting dimana jarang sekali terdapat saksi dalam kasus cyber crime dikarenakan saksi korban yang berada di luar daerah atau bahkan berada di luar negeri yang mengakibatkan penyidik sulit untuk melakukan pemeriksaan saksi dan pemberkasan hasil penyelidikan. Penuntut umum juga tidak mau menerima berkas perkara yang tidak dilengkapi dengan berita acara pemeriksaan saksi khususnya saksi korban dan harus dilengkapi dengan berita acara penyempahan saksi karena kemungkinan besar saksi tidak dapat hadir di persidangan dikarenakan jarak kediaman saksi yang cukup jauh. Hal tersebut mengakibatkan kurangnya alat bukti yang sah jika berkas perkara tersebut dilimpahkan ke pengadilan untuk disidangkan sehingga terdakwa beresiko akan dinyatakan bebas.

Hal serupa dialami oleh penyidik reskrimsus cyber crime Polda Sulsel dimana sangat kesulitan menangani kasus cyber crime terkait aspek alat bukti karena terkadang alat bukti yang berupa data-data tersebut telah diubah atau dihapus, namun beda halnya ketika pelaku cyber crime tertangkap tangan dalam melakukan aksi

kejahatannya dimana alat bukti dapat langsung diamankan dan disita oleh petugas kepolisian.

c. Aspek Fasilitas

Dalam mengungkap kasus-kasus cyber crime dibutuhkan fasilitas yang mampu menunjang kinerja aparat kepolisian. Fasilitas tersebut berupa laboratorium forensik komputer yang digunakan untuk mengungkap data-data yang bersifat digital serta merekam dan menyimpan bukti-bukti yang berupa soft copy (gambar, program, html, suara, dan lain sebagainya).

Komputer forensik merupakan salah satu cabang ilmu forensik yang berhubungan dengan bukti hukum yang ditemukan dalam komputer maupun media penyimpanan secara digital. Computer forensik dikenal sebagai digital forensics. Adapun tujuannya ialah untuk mengamankan dan menganalisis bukti digital, serta memperoleh berbagai fakta yang objektif dari sebuah kejadian atau pelanggaran keamanan dari sistem informasi. Berbagai fakta tersebut akan menjadi bukti yang akan digunakan dalam proses hukum. Contohnya, melalui Forensik Internet, kita dapat mengetahui siapa saja orang yang mengirim email kepada kita, kapan dan dimana keberadaan pengirim. Dalam contoh lain kita bisa melihat siapa pengunjung website secara lengkap dengan informasi IP Address, komputer yang dipakainya dan keberadaannya serta

kegiatan apa yang dilakukan pada website kita tersebut.³⁷

Kemampuan forensik digital menggunakan fasilitas yang hanya dimiliki oleh laboratorium forensik computer sedangkan alat yang berada di subdit cyber crime Polda Sulsel hanya 1 (satu) akses celebre yang berfungsi mengangkat data yang telah terhapus pada perangkat. Terkait dengan hal tersebut unit cyber crime Polda Sulsel belum memiliki fasilitas berupa laboratorium forensik komputer, yang mengakibatkan terkendalanya upaya penanggulangan cyber crime di wilayah hukum Polda Sulsel.

BRIPTU Abdiansyah mengungkapkan bahwa fasilitas subdit cyber crime masih minim atau belum maksimal karena terbatasnya jumlah akses celebre yang hanya satu dan dipergunakan oleh subdit cyber crime dan Polres-polres jajaran di wilayah hukum Polda Sulsel

d. Aspek Jurisdiksi

Dalam sistem hukum pidana yang berlaku saat ini, hukum pidana pada umumnya hanya berlaku di wilayah negaranya sendiri (asas teritorial) dan untuk warga negaranya sendiri (asas personal/nasional aktif). Hanya delik-delik tertentu yang dapat digunakan asas nasional pasif dan asas universal. Asas-asas berlakunya hukum pidana menurut tempat yang

³⁷ <http://www.seputarpengetahuan.com/2014/11/komputer-forensik-pengertian-dan-tujuan>
diakses pada tanggal 17 Juni 2017 Pukul 22:57 Wita

konvensional/tradisional (yurisdiksi fisik) tentunya menghadapi tantangan sehubungan dengan masalah pertanggungjawaban cyber crime.³⁸

Penanganan cyber crime tidak akan berhasil jika aspek yurisdiksi diabaikan. Karena pemetaan yang menyangkut kejahatan dunia maya menyangkut juga hubungan antar kawasan, antar wilayah, dan antar negara. Sehingga penetapan yurisdiksi yang jelas mutlak diperlukan.

Yurisdiksi tersebut telah diatur dalam Pasal 2 undang-undang informasi dan transaksi elektronik nomor 11 tahun 2008, yaitu:³⁹

“Undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau diluar wilayah hukum Indonesia dan merugikan kepentingan Indonesia”.

Undang-undang ini memiliki jangkauan yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia (WNI) maupun warga negara asing (WNA) atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan teknologi informasi untuk informasi dan transaksi elektronik dapat bersifat lintas teritorial atau universal. Yang

³⁸ Barda Nawawi Arief, *Op cit.* Hal 107

³⁹ Undang-undang nomor 11 tahun 2008

dimaksud dengan “merugikan kepentingan indonesia” adalah meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia.⁴⁰

⁴⁰ *Ibid.*

BAB V

PENUTUP

A. Kesimpulan

1. Faktor-faktor yang menyebabkan terjadinya penipuan online, yaitu: faktor ekonomi, faktor lingkungan, faktor sosial budaya, dan faktor intelektual
2. Upaya yang dilakukan pihak kepolisian dalam menanggulangi kejahatan penipuan berbasis online yaitu: Upaya Preventif merupakan upaya pencegahan yang dilakukan untuk mencegah terjadinya pelanggaran aturan di masyarakat dan Upaya Represif merupakan tindakan yang dilakukan setelah pelanggaran aturan terjadi.

B. Saran

1. Pemerintah juga harus memperhatikan aturan-aturan terkait informasi dan transaksi elektronik guna mengurangi celah hukum yang dapat timbul dan sebaiknya pemerintah memperhatikan alat dan akses untuk celebrite yaitu alat untuk mengangkat data dari handphone, yang saat ini hanya 1 buah akses celebrite di cyber crime polda sulsel, sementara penggunaannya sangat penting untuk pembuktian pelaku kejahatan khususnya kejahatan dunia maya.
2. Perlunya untuk meningkatkan kemampuan penyidik khususnya pada aparat kepolisian dengan memberikan pendidikan khusus terkait masalah cyber crime.

DAFTAR PSTAKA

Al-Qur'an dan Terjemahan :

Al Qur'an dan Terjemahan Al-Baqarah : Departemen Agama Republik Indonesia

Literatur :

Alam & Amir Ilyas A.S, 2010, *Pengantar Kriminologi*, Pustaka Refleksi, Makassar.

Alam A.S, 1995, *Kejahatan dan Sistem Pemindanaan*, Fakultas Hukum UNHAS, Ujung Pandang.

Ariani Yakti Widyastuti Rr, 2018, *Penipuan Menggunakan Media Internet Berupa Jual-Beli Online*, Bogor.

Barda Nawawi Arief, 1996, *kebijakan hukum pidana*, Bandung: Citra Aditya Bakti.

Bambang Sunggono, *Metode Penelitian Hukum* (Jakarta: PT Raja Grafindo Persada, 2003, Hal 43

Didik M Mansur dan Allsatris Gultom, *Cyber law – Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung, 2005

Moeljatno, 2008, *Asas-Asas Hukum Pidana*, Rineks Cipta, Jakarta.

Lamintang P.A.F, 1997, *Dasar-Dasar Hukum Pidana Indonesia* (Bandung: PT. Citra Aditya Bakti).

Romli Atasasmita, 2010, *Teori dan Kapita Selekta Kriminologi*, Refika Adatama, Bandung.

Republik Indonesia, Kitab Undang-Undang Hukum Pidana.

Siswanto, 2009, *Hukum Informasi Dan Transaksi Elektronik Studi Kasus Prita Mulyasari*, Jakarta: Rineka Cipta.

Sahariyanto, Budi, 2012, *Tindak Pidana Teknologi Informasi (Cyber Crime) urgensi pengaturan dan Celah Hukumnya*, Jakarta: Rajawali Pers.

Susanto. I.S., 1991, *Diklat Kriminologi Fakultas Hukum Universitas Diponegoro Semarang*, Semarang.

Topo Santoso & Eva Achjani Zulfa, 2001, *Kriminologi*, Raja Grafindo Persada, Jakarta.

Muhammad Solihin S. 2011. *Tinjauan Kriminologis Terhadap Cyber Crime*. Skripsi. Fakultas Hukum Universitas Hasanuddin

Muhammad Fauzan Aries. 2012. *Tinjauan Kriminologis Terhadap Cyber Crime (Data Kasus Pada Subdit II Fismondey DitReskrimsus Polda Sulselbar Tahun 2011)*. Skripsi. Fakultas Hukum Universitas Hasanuddin

Peraturan Perundang-undangan:

Kitab Undang-undang Hukum Pidana, Buku 2-Kejahatan BAB XXV

Undang-Undang RI. No. 19 tahun 2016 tentang perubahan atas Undang-undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Internet:

<http://tekno.kompas.com/read/2014/12/29/09190067/7.Kasus.Hacking.Paling>. Diakses pada tanggal 15 Oktober 2022, pukul 14:02 Wita

cracking merupakan kegiatan membobol suatu sistem computer dengan tujuan mengambil informasi penting. Diakses di cybercrime4c.blogspot.com/2013/06/apa-yang-dimaksud-cracking. Pada tanggal 15 oktober 2022, pukul 14:10 Wita

Defacing merupakan bagian dari kegiatan hacking web atau program application, yang menfokuskan target operasi pada perubahan tampilan dan konfigurasi fisik dari web atau program aplikasi tanpa melalui source code program tersebut. Diakses di Profesiti.blogspot.com/p/category-cybercrime pada tanggal 15 oktober 2022, pukul 14:23 Wita

Senarai atau list merupakan struktur data yang terdiri atas rangkaian elemen sejenis yang saling berhubungan atau bersifat reruntunan (sequence). Diakses di <http://slideplayer.info/slide/4106324/>.

Teori asosiasi diferensial atau differential association dikemukakan pertama kali oleh Edwin H Sutherland pada tahun 1934 dalam bukunya *Principle of Criminology*. Sutherland dalam teori ini berpendapat bahwa perilaku

kriminal merupakan perilaku yang dipelajari dalam lingkungan sosial.Sumber: <http://www.kompasiana.com/ariansyahekasaputra/teori-asosiasi-diferensial-differential-association-theory-dalam> di akses pada tanggal 17 juni 2017 pukul 12:21 Wita

<https://bigswapmp.wordpress.com/2011/03/02/kasus-kasus-cyber-crime-part1-spamming/> yang diakses pada tanggal 4 januari 2017, pukul 14:35 Wita

<http://www.seputarpengetahuan.com/2014/11/komputer-forensik-pengertian-dan-tujuan> yang di akses 19 Desember 2022, pukul 22:57 Wita

<http://berbagi100persen.blogspot.co.id/2013/06/kasus-spamming.html>. Yang diakses pada tanggal 19 Oktober 2022, pukul 14:27 Wita