

**Prosedur Penanganan Tindak Pidana *Cybercrime* dan Problematika
Penumpukan Perkara *Cybercrime* di Polda Jateng**

SKRIPSI

Diajukan untuk Memenuhi Tugas dan Melengkapi Syarat Guna Memperoleh Gelar Strata S.I
Dalam Prodi Ilmu Hukum



Oleh:

SIGID PAMUNGKAS

NIM. 1502056057

**FAKULTAS SYARIAH DAN HUKUM UNIVERSITAS ISLAM NEGERI
WALISONGO SEMARANG 2021**



KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI (UIN) WALISONGO

FAKULTAS SYARIAH DAN HUKUM

Alamat: Jl. Prof. DR. HAMKA Kampus III Ngaliyan Telp./Fax. (024) 7601291, 7624691 Semarang 50185

SURAT KETERANGAN PENGESAHAN SKRIPSI

Nomor: B-6224.12/Un.10.1/D.1/PP.00.9/XII/2021

Pimpinan Fakultas Syari'ah dan Hukum Universitas Islam Negeri (UIN) Walisongo Semarang menerangkan bahwa skripsi Saudara,

Nama : Sigid Pamungkas
NIM : 1502056057
Program studi : Ilmu Hukum (IH)*
Judul : Prosedur Penanganan Tindak Pidana Cybercrime dan Problematika Penumpukan Perkara Cybercrime di Polda Jateng
Pembimbing I : Dr. H. Ali Imron, S.H., M.Ag
Pembimbing II : Novita Dewi Masyithoh S.H., M.H

Telah dimunaqasahkan pada tanggal 28 Desember 2021 oleh Dewan Penguji Fakultas Syari'ah dan Hukum yang terdiri dari:

Penguji I / Ketua Sidang : H. Tolkah, M.A.
Penguji II / Sekretaris Sidang: Novita Dewi Masyithoh S.H., M.H
Penguji III : Hj. Briliyan Erna Wati, SH., M.Hum.
Penguji IV : Dr. M. Harun, S.Ag. MH.

dan dinyatakan **LULUS** serta dapat diterima sebagai syarat guna memperoleh gelar Sarjana Strata 1 (S.1) pada Fakultas Syariah dan Hukum UIN Walisongo.

Demikian surat keterangan ini dibuat dan diberikan kepada yang bersangkutan untuk dipergunakan sebagaimana mestinya.



A.n. Dekan,
Wakil Dekan Bidang Akademik
& Kelembagaan

Dr. H. Ali Imron, SH., M.Ag.

Semarang, 28 Desember 2021
Ketua Program Studi,

Briliyan Erna Wati, S.H., M.Hum.

PENGESAHAN

SKRIPSI

Prosedur Penanganan Tindak Pidana *Cybercrime* dan Problematika Penumpukan Perkara *Cybercrime* di Polda Jateng

Disusun Oleh :

Sigid Pamungkas

NIM 1502056057

Telah dipertahankan di depan majelis penguji skripsi pada tanggal 28 Desember 2021
dan dinyatakan LULUS

Susunan Dewan Penguji

Ketua



H. Tolkah M.A

NIP.196905071996031005

Sekretaris



Novita Dewi Masyitoh, S.H., M.H.

NIP.197910222007012001

Penguji I



Hj. Brilyan Erna Wati, S.H, M.H

NIP.196312191999032001

Penguji II



Dr. M. Harun, S.Ag., M.H

NIP.197508152008011017

Pembimbing I



Dr. H. Ali Imron, S.H., M.Ag

NIP. 197307302003121003

Pembimbing II



Novita Dewi Masyithoh, S.H., M.H.

NIP. 197910222007012001

PERSETUJUAN PEMBIMBING

Lamp : 4 (empat) eksemplar

Hal : Naskah Skripsi

a.n. Sdr. Sigid Pamungkas

Kepada Yth

Dekan Fakultas Syari'ah dan Hukum

UIN Walisongo Semarang

Assalamu'alaikum Wr.Wb

Setelah kami meneliti dan mengadakan perbaikan seperlunya, Bersama ini saya kirimkan naskah skripsi saudara:

Nama : Sigid Pamungkas

NIM : 1502056057

Jurusan : Ilmu Hukum

Judul Skripsi : Prosedur Penanganan Tindak Pidana *Cybercrime* dan Problematika Penumpukan Perkara *Cybercrime* di Polda Jateng.

Selanjutnya kami mohon agar skripsi saudara tersebut segera dimunaqosahkan.

Atas perhatiannya saya ucapkan terima kasih

Wassalamu'alaikum Wr.Wb

Semarang, 16 Desember 2021

Pembimbing I



Dr. H. Ali Imron, S.H., M.Ag.
NIP. 19730730 200312 1 003

Pembimbing II



Novita Dewi Masvithoh, S.H., M.H.
NIP. 19791022 200701 2 001

MOTTO

يَا أَيُّهَا الَّذِينَ آمَنُوا كُونُوا قَوِّمِينَ لِلَّهِ شُهَدَاءَ بِالْقِسْطِ وَلَا يَجْرِمَنَّكُمْ شَنَا نُ قَوْمٍ عَلَىٰ أَلَّا تَعْدِلُوا ۗ أَعْدِلُوا ۗ هُوَ أَقْرَبُ لِلتَّقْوَىٰ وَاتَّقُوا ۗ
اللَّهَ ۗ إِنَّ اللَّهَ خَبِيرٌ بِمَا تَعْمَلُونَ

“.....Hai orang-orang yang beriman hendaklah kamu jadi orang-orang yang selalu menegakkan (kebenaran) karena Allah, menjadi saksi dengan adil. Dan janganlah sekali-kali kebencianmu terhadap sesuatu kaum, mendorong kamu untuk berlaku tidak adil. Berlaku adillah, karena adil itu lebih dekat kepada takwa. Dan bertakwalah kepada Allah, sesungguhnya Allah Maha Mengetahui apa yang kamu kerjakan.....” (Qs. Al-Maidah: 8)

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk:

Ayah dan ibu,

Karena kasih sayang dan perhatian menuntun anak-anaknya menjadi anak yang saleh dan salehah serta berbakti kepada kedua orang tua baik dalam keadaan senang maupun susah.

Kakak-kakak tercinta,

Yudha Prasetyawan dan Diah Ayu Nurita

Kalian adalah inspirasi dan semangat hidup bagi penulis

DEKLARASI

Dengan penuh kejujuran dan tanggungjawab, penulis menuturkan bahwa skripsi ini tidak mengandung bahan yang sudah ditulis pihak lain atau diterbitkan. Begitu juga skripsi ini tidak mengandung suatu gagasan-gagasan pihak lain, kecuali informasi yang tercantum dalam rujukan yang dijadikan referensi.

Semarang, 16 Desember 2021

Deklarator



Sigid Pamungkas
NIM. 1502056057

TRANSLITERASI ARAB-LATIN

Penulisan transliterasi aksara-aksara Arab Latin dalam skripsi ini berlandaskan pada (SKB) Menteri Agama dan Menteri Pendidikan dan Kebudayaan R.I. Nomor: 158 Tahun 1987 dan Nomor: 0543b/U/1987.

A. Konsonan

Daftar aksara bahasa Arab dan transliterasinya ke dalam aksara Latin bisa diamati pada halaman berikut:

Huruf Arab	Nama	Huruf Latin	Nama
ا	Alif	Tidak dilambangkan	Apostrof
ب	Ba	B	Be
ت	Ta	T	Te
ث	Tsa	S	Es
ج	Jim	Jh	Je
ح	Ha	H	Ha
خ	Kha	Kh	Ka dan Ha
د	Dal	D	De
ذ	Zal	Z	Zet
ر	Ra	R	Er
ز	Zai	Z	Zet
س	Sin	S	Es
ش	Syin	Sy	Es dan Ye
ص	Sad	S	Ş (dengan titik di bawah)
ض	Dad	D	De (dengan titik di bawah)
ط	Ta	T	Te (dengan titik di bawah)
ظ	Za	Z	Zet (dengan titik di bawah)
ع	Ain	-	Apostrof terbalik
غ	Gain	G	Ge
ف	Fa	F	Ef
ق	Qaf	Q	Qi

ك	Kaf	K	Ka
ل	Lam	L	El
م	Mim	M	Em
ن	Nun	N	En
و	Wau	W	We
ه	Ha	H	Ha (dengan titik atas)
ء	Hamzah	-	Apostrof
ي	Ya	Y	Ye

Hamzah (ء) yang berada pada awal kata mengikuti vokalnya tanpa diberi tanda apa pun. Bila ia berada pada tengah atau akhir kata maka ditulis dengan tanda (´) B. Vokal

Vokal bahasa Arab, serupa vokal bahasa Indonesia, mencakup vokal tunggal atau monoftong dan vokal rangkap atau diftong. Vokal tunggal bahasa Arab yang simbolnya berbentuk tanda atau harakat, transliterasinya sebagai berikut:

Tanda	Nama	Huruf Lain	Nama
اَ	Fathah	A	A
اِ	Kasrah	I	I
اُ	Dhomah	U	U

Vokal rangkap bahasa Arab yang simbolnya berbentuk gsbungsn antara harokat dan huruf, transliterasinya berbentuk gabungan huruf, yakni:

Tanda	Nama	Huruf Lain	Nama
اهي	Fathah dan Ya	Ai	A dan I
اهو	Fathah dan wa	Au	A dan U

C. Maddah

Maddah atau vokal panjang yang simbolnya berbentuk harakat dan huruf, transliterasinya berbentuk huruf dan simbol, yakni:

Harakat dan Huruf	Nama	Huruf dan Tanda	Nama
اهيَ	Fathah dan Alif atau Ya	ā	a dan garis di atas
يِ	Kasrah dan Ya	ī	i dan garis di atas
وُ	Dommah dan Wau	ū	u dan garis di atas

D. *Tarbūtah*

Transliterasi untuk ta marbūtah ada dua, yakni: ta marbūtah yang hidup atau mendapat harakat fathah, kasrah, dan dlamamah, transliterasinya adalah [t]. Sementara ta marbūtah yang mati atau mendapat hatakat sukun, transliterasinya adalah [h]. Bila pada kata yang berakhir dengan ta marbūtah diikuti oleh kata yang menggunakan kata sandang al dan bacaan kedua kata itu terpisah, maka ta marbūtah itu ditransliterasikan dengan ha [h].

E. *Syaddah (Tasyid)*

Syaddah atau tasydīd yang dalam tata cara tulisan Arab disimbolkan dengan suatu simbol tasydīd (َ َ َ), dalam transliterasi ini disimbolkan dengan perulangan aksara (konsonan ganda) yang diberi (simbol syaddah), maka ia ditransliterasi serupa huruf maddah (ī).

F. Kata Sandang

Kata sandang dalam tata cara tulisan Arab disimbolkan dengan aksara (alif lam ma'rifah). Dalam pedoman transliterasi ini, kata sandang ditransliterasi seperti biasa, al-, baik saat ia diikuti oleh aksara syamsiyah ataupun aksara qamariyah. Kata sandang tidak mengikuti bunyi huruf langsung yang mengikutinya. Kata sandang ditulis terpisah dari kata yang mengikutinya dan dihubungkan dengan garis mendatar (-).

G. *Hamzah* Regulasi transliterasi aksara hamzah menjadi aspostrof (') hanya berlaku bagu hamzah yang berada di tengah dan akhir kata. Namun, jika hamzah berada di awal kata, maka ia tidak disimbolkan, sebab dalam tulisan Arab ia serupa alif.

H. Penulisan Kata Arab yang Lazim digunakan dalam Bahasa Indonesia

Kata, istilah atau kalimat Arab yang ditransliterasi merupakan kata, istilah atau kalimat yang belum diformalkan dalam bahasa Indonesia. kata, istilah atau kalimat yang sudah umum dan merupakan bagian dari perbendaharaan bahasa Indonesia, tidak lagi ditulis berdasarkan sistem transliterasi sebelumnya. Namun, jika kata-kata tersebut merupakan bagian dari sebuah rangkaian teks Arab, maka mereka musti ditransliterasi secara utuh.

I. *Lafẓ Al-Jalālah* (الله) Kata “Allah” yang didahului partikel seperti aksara jarr dan aksara lainnya atau berkedudukan sebagai mudāfilaih (frasa nominal), ditransliterasi tanpa aksara hamzah. Sementara ta marbūtah di akhir kata yang disandarkan pada lafz AlJalālah, ditransliterasi denganhuruf [t].

J. Huruf Kapital

Meskipun tata cara tulisan Arab tidak menggunakan aksara kapital (All Caps), dalam transliterasinya aksara-aksara tersebut dibebani aturan tentang penerapan aksara kapital berpedoman ejaan bahasa Indonesia yang disempurnakan (EYD). Aksara kapital, contohnya, diterapkan untuk menuliskan huruf awal nama seseorang/sesuatu (manusia, lokasi, bulan) dan aksara pertama pada awal kalimat. Jika nama seseorang/sesuatu diawali oleh kata sandang (al-), maka yang ditulis dengan aksara kapital tetap huruf pertama nama seseorang/sesuatu

tersebut, bukan aksara pertama sandangnya. Bila berada pada permulaan kalimat, maka aksara A dari kata sandang tersebut memakai aksara kapital (A1-). Aturan yang serupa juga berlaku untuk aksara pertama dari judul rujukan yang diawali oleh kata sandang al-, baik saat ia ditulis dalam teks ataupun dalam catatan referensi (CK, DP, CDK, dan DR).

ABSTRAK

Manajemen penyidikan tindak pidana *cybercrime* Ditreskrimsus Polda Jateng berperan amat penting dalam penyelesaian penumpukan perkara, dikarenakan sumber daya yang terbatas. Seperti, personel, materi, waktu, dan dana yang harus dimobilisasikan secara terencana, terkendali serta terorganisir sehingga penyidikan yang efisien dan efektif tercipta dan pada hasilnya mewujudkan cita-cita Polisi Republik Indonesia (POLRI) kedepan akan adanya standar operasi prosedur bagi setiap tahapan penyidikan. Seiring dengan keberadaan Peraturan kepala Kepolisian Negara Republik Indonesia Nomor 14 Tahun 2012 Tentang Manajemen Penyidikan Tindak Pidana. Namun, kendala keterbatasan personil seperti tenaga ahli IT dan *cyber forensic*, fakta ini juga diperkuat oleh laporan dari Wakil Direktur Tindak Pidana Ekonomi Khusus Bareskrim Polri. Terbatasnya jumlah personil tenaga ahli. Lebih ironis lagi laporan tingkat kejahatan siber di Indoensia semakin meningkat, dengan keterbatasan personil dan tenaga ahli di pihak kepolisian Indonesia maka penyelesaian kasus tersebut tidak bisa diselesaikan dengan cepat. Akibatnya dirasakan langsung oleh pihak korban atau kejahatan siber. Kendala lain yang krusial adalah terbatasnya dana anggaran operasional, masalah yang cukup krusial selain perangkat hukum, yaitu SDM yang belum mencukupi, anggaran serta sarana dan prasarana untuk menunjang pengungkapan kasus-kasus *cybercrime*. Sedangkan pada kenyataanya dalam satu bulan bisa mencapai 15 kasus. Oleh karena itu, peneliti ingin mengetahui bagaimanakah prosedur penanganan perkara tindak pidana siber di Polda Jateng dan Bagaimana problematika dan penyelesaian penumpukan perkara *cybercrime* di Polda Jateng.

Penelitian ini menggunakan jenis penelitian hukum kualitatif, yang menghasilkan deskriptif data. Dengan pendekatan yuridis empiris (non doktrinal). Sumber data dalam penelitian ini meliputi, data primer berupa sejumlah keterangan atau fakta yang diperoleh dari hasil wawancara dengan Ditreskrimsus Polda Jateng, data sekunder berupa data *cybercrime* di Ditreskrimsus Polda Jateng Tahun 2019–2020. Lokasi penelitian adalah Ditreskrimsus Polda Jateng yang menjadi tempat penelitian dan memperoleh data-data. Tehnik pengumpulan data yang di gunakan melalui wawancara dan dokumentasi. Adapun analisis data menggunakan penyajian data dan reduksi data kesimpulan dan verifikasi data lapangan.

Hasil dari penelitian ini menyimpulkan bahwa penanganan *Cybercrime* oleh Polda Jateng telah sesuai dengan prosedur penanganan perkara tindak pidana *Cybercrime*. Kasus yang berhadapan dengan wilayah luar Indonesia akan mempersulit penyelidikan apabila ada perbedaan pandangan hukum antara negara Indonesia dengan negara lain, karena kemungkinan negara di mana tempat pembuatan website/media sosial pelaku berada di wilayah yang tidak ada perjanjian diplomasi / perjanjian extradisi dengan Indonesia. Kendala yang krusial adalah terbatasnya dana anggaran operasional, masalah yang cukup krusial selain perangkat hukum, yaitu SDM yang belum mencukupi, anggaran serta sarana dan prasarana untuk menunjang pengungkapan kasus-kasus *cybercrime*.

Kata kunci: Tindak Pidana, *CyberCrime*

ABSTRAK

The management of cybercrime investigations ditreskrimsus Polda Jateng plays a very important role in solving the buildup of cases, due to limited resources. Such as, personnel, materials, time, and funds that must be mobilized in a planned, controlled and organized manner so that efficient and effective investigation is created and in the result realizes the ideals of the Police of the Republic of Indonesia (POLRI) In the future there will be standard operating procedures for each stage of the investigation. Along with the existence of the Regulation of the Head of the State Police of the Republic of Indonesia Number 14 of 2012 concerning the Management of Criminal Investigations. However, the constraints of personnel limitations such as IT and cyber forensic experts, this fact is also reinforced by a report from the Deputy Director of Special Economic Crimes Bareskrim Polri. Limited number of skilled personnel. More ironically, reports of cyber crime rates in Indonesia are increasing, with limited personnel and experts on the part of the Indonesian police, the settlement of the case cannot be resolved quickly. The result is felt directly by the victim or cyber crime. Another crucial obstacle is the limited operational budget funds, a problem that is quite crucial in addition to legal tools, namely insufficient human resources, budgets and facilities and infrastructure to support the disclosure of cybercrime cases. In fact, in one month it can reach 15 cases. Therefore, researchers want to know how the procedure for handling cyber crime cases in Jateng Police and solving the buildup of cybercrime cases in Polda Jateng.

This research uses a type of qualitative legal research, which produces descriptive data. With an empirical (non-doctrinal) juridical approach. Data sources in this study include, primary data in the form of a number of information or facts obtained from the results of interviews with the Ditreskrimsus Polda Jateng, secondary data in the form of cybercrime data in the Ditreskrimsus Polda Jateng Year 2019-2020. The location of the research is ditreskrimsus Polda Jateng which became a place of research and obtaining data. Data collection techniques used through interviews and documentation. Data analysis uses data presentation and reduction of conclusion data and field data verification

The results of this study concluded that the handling of Cybercrime by the Jateng Police was in accordance with the procedures for handling cybercrime cases. Cases dealing with overseas territories will complicate the investigation if there are differences in legal views between the Indonesian state and other countries, because of the possibility of a country where the place of creation of the website / social media actors is in the region where there is no diplomacy agreement / extradisi agreement with Indonesia. A crucial obstacle is the limited operational budget funds, a problem that is quite crucial in addition to legal tools, namely insufficient human resources, budgets and facilities and infrastructure to support the disclosure of cybercrime cases.

Keywords: Criminal Offense, *CyberCrime*

KATA PENGANTAR



Puji sukur kehadiran Allah SWT. atas berkah dan rahmat serta hidayahnya, penulis dapat menyelesaikan skripsi ini dengan lancar tanpa kekurangan suatu apa pun. Shalawat serta salam senantiasa tetap tercurahkan kepada nabi Muhammad SAW. sebagai nabi akhir zaman, yang dapat memberi syafaat kelak di hari kiamat.

Penulis menyadari bahwa skripsi ini tidak akan terwujud tanpa ada bantuan dari berbagai pihak. Oleh karena itu, pada halaman ini penulis ingin menyampaikan terima kasih kepada:

1. Rektor UIN Walisongo Semarang,
2. Bapak Dr. H. Mohamad Arja Imroni, M.Ag selaku Dekan Fakultas Syari'ah UIN Walisongo Semarang,
3. Bapak Dr. H. Ali Imron, S.H., M.Ag. selaku pembimbing pertama dalam penulisan skripsi ini,
4. Ibu Novita Dewi Masyithoh, S.H., M.H. selaku pembimbing dua dalam penulisan skripsi ini,
5. Seluruh dosen, karyawan dan civitas akademika Fakultas Syari'ah UIN Walisongo Semarang yang telah berpartisipasi, membantu, serta memberi semangat kepada penulis,
6. Teman-teman dari KKN MIT (Mandiri Inisiatif Terprogam) Yusuf, Saifin, Davi, Rozak, Falih, Erma, Ulpa, Rifka, Hana, Dwi, Arifah, Fajrul, Lita, kalian telah memberi banyak hal bagi penulis
7. Teman-teman di kampus Yusuf, Muhyiddin, Kautsar, Jabirul Fuad, Falih, Ryan, Hilmi, dan masih banyak lainnya yang tidak dapat penulis sebut satu persatu. Kalian telah banyak mewarnai hari-hari penulis dengan berbagai macam diskusi, dan penulis akan senantiasa merindukannya.
8. Semua pihak yang telah memberi motivasi, meminjamkan buku, dan fasilitas-fasilitas lainnya.

Semoga Allah membalas semua amal baik mereka dengan balasan yang lebih. Serta meninggikan derajat mereka baik di dunia ini maupun di akhirat kelak, amien. Jika skripsi

ini benar adanya maka semata-mata karena hidayah Allah SWT. dan jika terdapat kesalahan maka tidak lain adalah dari kekurangan penulis sendiri. Sehingga kritik dan saran sangat penulis harapkan demi tujuan konstruktif. Penulis hanya berharap skripsi ini dapat dijadikan sebagai tambahan referensi bagi generasi penerus, dan semoga bermanfaat bagi pembaca, amin.

Semarang, 16 Desember 2021

Penulis



Sigid Pamungkas

DAFTAR ISI

FAKULTAS SYARI'AH DAN HUKUM.....	ii
SURAT KETERANGAN PENGESAHAN SKRIPSI.....	ii
PENGESAHAN.....	iii
PERSETUJUAN PEMBIMBING	iv
MOTTO	v
PERSEMBAHAN.....	vi
DEKLARASI.....	vii
TRANSLITERASI ARAB-LATIN	viii
ABSTRAK.....	xii
KATA PENGANTAR	xiv
DAFTAR ISI	xvi
BAB I.....	1
PENDAHULUAN	1
A. Latar Belakang Masalah	1
B. Rumusan Masalah.....	6
C. Tujuan dan Manfaat Penelitian	7
D. Telaah Pustaka	8
E. Metode Penelitian	13
1. Jenis penelitian.....	13
2. Pendekatan penelitian	13
3. Lokasi Penelitian.....	14
4. Sumber Data	14
5. Metode Pengumpulan Data.....	17
6. Teknik Pengujian Validitas Data	18
7. Metode Analisis Data.....	19
F. Sistematika Penulisan	20
BAB II	22
TINJAUAN UMUM <i>CYBERCRIME</i>	22

A. Tindak Pidana <i>Cybercrime</i>	22
1. Pengertian <i>Cybercrime</i>	22
2. Kebijakan Kriminal Penanggulangan <i>Cybercrime</i>	26
3. Formulasi Tindak Pidana <i>Cybercrime</i>	29
B. Pertanggungjawaban Pidana atau Pidanaaan	34
C. Yurisdiksi dalam Tindak Pidana <i>Cybercrime</i>	38
D. Penyidikan dalam Tindak Pidana <i>Cybercrime</i>	42
BAB III	46
PROSEDUR PENANGANAN TINDAK PIDANA CYBER CRIME DI DITRESKRIMSUS POLDA JATENG	46
A. Gambaran Umum Ditreskrimsus Polda Jawa Tengah Unit <i>Cybercrime</i>	46
B. Prosedur Penanganan Tindak Pidana <i>Cyber Crime</i> Di Ditreskrimsus Polda Jateng	48
C. Hambatan dan Kendala yang Dihadapi oleh Pihak Kepolisian Republik Indonesia dalam Penegakan Hukum Terhadap Tindak Pidana pada Tahap Penyidikan di Polda Jawa Tengah	66
BAB IV	72
PROBLEMATIKA DAN PENYELESAIAN TERHADAP PENUMPUKAN PERKARA <i>CYBERCRIME</i> DI POLDA JATENG	72
A. Problematika Penumpukan Perkara <i>Cybercrime</i> di Polda Jateng.....	72
B. Penanganan Problem Penumpukan Perkara <i>Cybercrime</i> di Polda Jateng.....	79
BAB V	87
PENUTUP	87
A. Kesimpulan.....	87
DAFTAR PUSTAKA	89

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Era globalisasi ditandai oleh pesatnya perkembangan ilmu pengetahuan dan teknologi, khususnya di bidang informasi, komunikasi dan transportasi, membuat dunia menjadi transparan seolah-olah menjadi sebuah kampung tanpa mengenal batas Negara. Kondisi ini menciptakan struktur baru yaitu struktur global. *Cybercrime* ialah salah satu dimensi atau susunan baru dari kejahatan era sekarang yang memperoleh perhatian yang luas di dunia internasional. Kejahatan ini adalah salah satu bentuk sisi gelap atas kemajuan zaman teknologi yang memiliki dampak negatif sangat besar bagi semua bidang kehidupan modern saat ini. Pada masa globalisasi saat ini pun semua yang menempati permukaan bumi bisa bersinggungan satu dengan yang lain dalam kondisi yang sama. model hubungan mereka sangat ditentukan bagi alat sambungan internet dan komunikasi.

Kemajuan teknologi khususnya di bidang transportasi dan telekomunikasi dianggap menjadi penggerak dan turut mempercepat proses globalisasi di pelbagai aspek kehidupan. Gregory mengemukakan *cybercrime* adalah bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung melalui internet, dan dapat mengeksploitasi komputer lain yang terhubung dengan internet. Keamanan sistem yang memiliki banyak celah dapat menyebabkan seorang hacker memanfaatkan celah keamanan untuk masuk ke dalam sistem, merusak serta mengambil data-data yang tidak seharusnya diketahui oleh pihak luar.¹

¹ Robert. J Gregory, *Psychological Testing: Hisory, Principles, and Applications*, (United States of Amerika: Pearson Education Limited, 2015), hal.112.

Selain menjadi media pemberi akses informasi internet juga adalah merupakan sarana aktivitas komunitas komersial terpesat dan terbesar pertumbuhannya. Sistem jaringan memungkinkan setiap orang dapat mengetahui dan mengirimkan informasi secara cepat dan menghilangkan batas-batas territorial suatu wilayah negara. Setiap negara mesti menempuh kenyataan bahwa informasi dunia saat ini dibangun berlandaskan suatu akses yang ditawarkan bagi majunya bidang teknologi.²

Secara alamiah, manusia tidak mungkin dilepaskan dari kemajuan teknologi yang tujuannya adalah untuk memudahkan kehidupannya. Sebagai alamiah pula, manusia tidak bisa dilepaskan dari hukum yang arahnya adalah untuk melindungi eksistensi.³ Pada mulanya, manusia berhubungan atau komunikasi melalui bertatap muka secara langsung dan saling menyampaikan isyarat tertentu, lalu berkembang dengan memanfaatkan suatu perpaduan kata-kata tertentu yang dapat dipahami satu dengan yang lain. Bersamaan perkembangan manusia dari waktu ke waktu, kebutuhan manusia akan informasi dan komunikasi semakin mendorong manusia untuk mencoba menemukan dan mengembangkan media komunikasi baru yang mutakhir, yang memberikan kemungkinan terhadap manusia untuk melangsukan komunikasi dan persebaran informasi secara tepat dan cepat. Melalui berjalannya metode penemuan dan pengembangan media komunikasi dan informasi lalu menghadirkan sebuah teknologi yang bisa memperlancar gelombang informasi dan komunikasi tanpa terhalang oleh batas, jarak, ruang dan waktu, juga bisa meningkatkan efisiensi serta produktifitas, yang akhirnya biasa dikenal dengan Teknologi Informasi dan Komunikasi (TIK).

Dalam era informasi (*information age*), keberadaan suatu informasi menjadi suatu hal yang sangat penting bagi orang yang akan mencari suatu informasi tertentu

² Ibid, hal115.

³ Edmon Makarim, *Kompilasi Hukum Telematika*. (Jakarta: Raja Grafindo Persada, 2003), hal7.

yang sesuai dengan kebutuhannya, dan tidak kalah penting ketepatan data yang didapat sebagai suatu dalih untuk menggunakan Teknologi Informasi dan Komunikasi (TIK). Dalam hal ini, TIK menjadi suatu media yang menjawab kebutuhan manusia akan pemenuhan suatu informasi dan komunikasi. Teknologi Informasi dan Komunikasi (TIK) telah membawa manusia kepada suatu peradaban baru dengan struktur sosial dan tata nilai yang diatur sedemikian rupa. Dalam pertumbuhannya, sudah dijumpai komputer selaku suatu produk yang muncul dari teknologi informasi dan komunikasi.

Pasal 1 Angka 14 Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, menjelaskan bahwa computer yaitu: suatu alat yang berguna untuk memproses data elektronik, optik, magnetik atau sistem yang menyelenggarakan fungsi aritmatika, logika dan penyimpanan. Penggabungan antara teknologi telekomunikasi, media dan informatika melahirkan suatu sarana yang baru dan biasa disebut dengan internet.⁴

Fenomena *cybercrime* di Indonesia merupakan perbincangan yang selalu menarik minat masyarakat. Dari masyarakat pada umumnya, sampai pada masyarakat yang memang memiliki keterkaitan langsung dengan fenomena *cybercrime*. Dalam memberikan terjemahan *cybercrime* tampaknya belum ada keseragaman pendapat dari pakar yang terkait. Misalnya, ada yang menterjemahkan dengan kejahatan mayantara, kejahatan siber, kejahatan komputer, kejahatan dunia maya, kejahatan virtual, dan sebagainya. Hal ini ditegaskan pula oleh Didik M. Arief Mansur dan Alisatris Gultom dalam bukunya yang berjudul *cyber law*.⁵ Romainnya *cybercrime* di Indonesia dan di negara-negara lain di dunia memaksa banyak elemen dan pihak akan terus bergiat dan berusaha memeranginya dengan beragam macam cara. Salah satu landasannya adalah

⁴ Robert. J Gregory., *Psychological Testing*, hal, 134.

⁵Didik M. Arief Mansur dan Alisatris Gultom, *Cyber Law-Aspek Hukum Teknologi Informasi*, (Refika Aditama, Bandung, 2005), hal, 25.

dengan menggunakan model memahami bagian *cybercrime* dari semua sisi. Keutuhan pemahaman akan pemberantasan *cybercriminal* dan *cybercrime* harus dilaksanakan berdasarkan perencanaan multi dimensional, salah satunya memakai perspektif hukum kriminologi dan pidana. Keadaan ini didasarkan pada sistem pemikiran bahwa tidak mungkin memerangi sesuatu bisa sukses, tanpa pemahaman sesuatu yang akan diperangi.⁶

Masalah perkembangan teknologi komputer, telekomunikasi dan informasi telah berjalan sedemikian rupa sehingga pada saat ini sudah sangat berbeda dengan sepuluh tahun yang lalu. Pemanfaatan tersebut telah mendorong pertumbuhan bisnis yang pesat, karena berbagai informasi dapat disajikan dengan canggih dan mudah diperoleh, dan melalui hubungan jarak jauh memanfaatkan teknologi komunikasi dapat digunakan untuk bahan melakukan bisnis selanjutnya. Pihak-pihak yang terkait dalam transaksi tidak bertemu secara langsung, cukup melalui peralatan komputer dan komunikasi, kondisi yang demikian merupakan pertanda dimulainya era siber dalam bisnis.⁷

Munculnya teknologi-teknologi baru seperti internet dan yang lainnya harus diakui manakah yang lahir dari rahim teknologi. Namun demikian perkembangan positif ilmu pengetahuan dan teknologi informasi juga dibarengi dengan aspek negatif yang melekat padanya yaitu dengan munculnya kejahatan-kejahatan baru yang sangat kompleks disertai dengan modus operandi yang baru sama sekali.⁸ Akhirnya banyak masyarakat yang terkena dampak kejahatan tindak pidana siber dan melaporkan ke kepolisian. Dampak kejahatan dari kejahatan *cybercrime* seperti ujaran kebencian menimbulkan perpecahan di kalangan masyarakat, *hoaks* juga berdampak sangat buruk,

⁶ Widodo, *Memerangi Cybercrime Karakteristik Motivasi dan Strategi Penanganannya dalam Perspektif Kriminologi*, Aswaja Jakarta :Pressindo, 2013), hal, 1.

⁷ Niniek suparni, “*Cyberspace Problematika dan Aplikasi Pengaturannya*” (Jakarta : Sinar Grafika, 2009), hal 1.

⁸ Abdul wahid dan Muhammad Labib, *Kejahatan Mayantra*, (Bandung: Rafikia Aditama, 2005), hal 33-36.

baik psikologis, sosial, maupun fisik. Pornografi yang disebar di media sosial menyebabkan rentan ditiru anak-anak. Sedangkan prostitusi, baik lewat online atau transaksi dunia nyata, banyak melibatkan remaja perempuan sebagai pekerja seks-nya dan dengan media sosial penyebaran penyakit sosial ini mudah sekali berkembang.

Menimbang benar-benar strategisnya babak penyidikan didalam proses peradilan pidana, lantas POLRI mengeluarkan Perkap No 14 tahun 2012 tentang Manajemen Penyidikan Tindak Pidana, adapun aturan dan tujuan pokoknya ialah peraturan ini menyampaikan gambaran umum berkenaan proses penanganan perkara, manajemen penanganan perkara, peran atasan penyidik terhadap prosedur pengendalian perkara. Tidak boleh melupakan prinsip-prinsip dari peraturan yaitu legalitas, professional, proposional, prosedural, transparan, akuntabel, serta efektif dan efisien.⁹

Manajemen penyidikan tindak pidana berlaku amat penting dikarenakan sumber daya yang terbatas, seperti personel, materi, waktu dan dana yang harus dimobilisasikan secara terencana, terkendali serta terorganisir sehingga penyidikan yang efisien dan efektif tercipta dan pada hasilnya mewujudkan cita-cita POLRI kedepan akan adanya standar operasi prosedur bagi setiap tahapan penyidikan yang akan dilaksanakan di seluruh jajaran POLRI.¹⁰

Berbicara mengenai kendala keterbatasan personil seperti tenaga ahli IT dan *cyber forensic*, fakta ini juga diperkuat oleh laporan dari Wakil Direktur Tindak Pidana Ekonomi Khusus Bareskrim Polri. Terbatasnya jumlah personil tenaga ahli. Lebih ironis lagi laporan tingkat kejahatan siber di Indoensia semakin meningkat, dengan keterbatasan personil dan tenaga ahli di pihak kepolisian Indonesia maka penyelesaian kasus tersebut tidak bisa diselesaikan dengan cepat. Akibatnya dirasakan langsung oleh

⁹ R. Haryo Seto L, *Wawancara*, Semarang, 16 November 2020

¹⁰ R. Haryo Seto L, *Wawancara*, Semarang, 16 November 2020

pihak korban atau kejahatan siber. Kualitas fasilitas teknologi informasi di Indonesia memang sudah cukup baik, namun tidak sebanding dengan jaminan keamanan oleh para pengguna.

Kendala lain yang krusial adalah terbatasnya dana anggaran operasional, masalah yang cukup krusial selain perangkat hukum, yaitu SDM yang belum mencukupi, anggaran serta sarana dan prasarana untuk menunjang pengungkapan kasus-kasus *cybercrime*. Sekarang ini anggaran yang ada hanya cukup untuk satu perkara per satu bulan¹¹. Sedangkan pada nyatanya dalam satu bulan bisa mencapai 15 kasus¹². Oleh karena itu, peneliti ingin mengetahui sebenarnya bagaimanakah prosedur penyelesaian perkara tindak pidana siber di Polda Jateng dan faktor-faktor apa saja yang jadi penghambat terselesainya kasus tersebut. Berdasarkan kenyataan di atas maka penulis tertarik untuk meneliti **Prosedur Penanganan Tindak Pidana *Cybercrime* dan Problematika Penumpukan Perkara *Cybercrime* di Polda Jateng**. Apalagi dengan keberadaan Peraturan kepala Kepolisian Negara Republik Indonesia Nomor 14 Tahun 2012 Tentang Manajemen Penyidikan Tindak Pidana.

B. Rumusan Masalah

1. Bagaimana prosedur penanganan tindak pidana *cybercrime* di Polda Jateng?
2. Bagaimana problematika dan penyelesaian penumpukan perkara *cybercrime* di Polda Jateng?

¹¹ Avi, *Penanganan Kasus Cyber Crime Terganjil Regulasi dan Anggaran*, detiknews, <http://repository.ums.ac.id/bitstream/handle/123456789/7445/BAB%20IV.pdf?sequence=4&isAllowed=y>,(diakses pada 2 Mei 2021)

¹² R. Haryo Seto L, *Wawancara*, Semarang, 16 November 2020

C. Tujuan dan Manfaat Penelitian

Sesuai dengan masalah-masalah yang akan dibahas dalam penelitian ini maka tujuan penelitian ini antara lain sebagai berikut:

1. Untuk mengetahui bagaimana Prosedur Penanganan Tindak Pidana *Cybercrime* di Polda Jateng.
2. Untuk mengetahui bagaimana Prosedur Penanganan Problematika Penumpukan *Cybercrime* di Polda Jateng.

Manfaat dari penelitian dan penulisan ini yang harapannya baik secara teoritis maupun secara praktis adalah:

1. Secara teoritis

- a) Sebagai sarana perkembangan ilmu pengetahuan di bidang ilmu hukum, khususnya dalam bidang ilmu hukum pidana.
- b) Untuk memberikan sumbangan pengetahuan secara ilmiah mengenai Hukum Pidana, khususnya tentang manajemen prosedur dan penanganan Ditreskrimsus Polda Jateng dalam penumpukan perkara *cybercrime*.

2. Secara Praktis

Hasil dari penelitian ini dapat bermanfaat dan berguna untuk:

a) Ditreskrimsus Polda Jateng

Sebagai bahan masukan bagi pihak Ditreskrimsus Polda Jateng khususnya bagian *cybercrime* dalam upaya menangani tindak pidana *cybercrime* dalam rangka meningkatkan profesionalisme dan kredibilitas kepolisian dalam melaksanakan perannya sebagai aparat penegak hukum.

b) Mahasiswa

Untuk menambah pengetahuan mengenai Hukum Pidana, khususnya tentang manajemen prosedur dan penanganan Ditreskrimsus Polda Jateng dalam

penumpukan perkara *cybercrime* dan menambah referensi dan bahan masukan untuk penelitian selanjutnya.

c) Masyarakat

Sebagai sarana pengetahuan umum bagi masyarakat agar mengetahui tentang perkara tindak pidana *cybercrime* dan bagaimana cara bila menghadapi kasus *cybercrime*.

D. Telaah Pustaka

1. Skripsi yang dilakukan oleh Adhi Dharma Aryyaguna skripsi berjudul “Tinjauan Kriminologis Terhadap Kejahatan Penipuan Berbasis Online” Departemen Hukum Pidana Fakultas Hukum Universitas Hasanudin Makassar pada tahun 2017.

Penelitian ini dititik beratkan guna mengetahui aspek yang mempengaruhi banyaknya *cyber crime* yang dikhususkan pada kejahatan penipuan berbasis online, efektifnya penegakan hukum dalam usaha menanggulangi tindak pidana *cyber crime*, dan kendala-kendala yang dihadapi oleh petugas kepolisian dalam usaha menanggulungannya. Riset ini dilakukan pada Kepolisian Negara Republik Indonesia Daerah Sulawesi Selatan (Polda Sulsel).¹³

Perbedaan penelitian ini dengan penelitian dalam skripsi ini adalah adalah tentang penitikberatan pembahasan. Penelitian yang dilakukan oleh Adhi Dharma Aryyaguna (2017) menitikberatkan tentang kriminologis Terhadap Kejahatan Penipuan Berbasis Online, sedangkan penelitian yang dilakukan

¹³ Adhi Dharma Aryyaguna, “Tinjauan Kriminologis Terhadap Kejahatan Penipuan Berbasis Online” skripsi Fakultas Hukum Universitas Hasanudin Makassar pada tahun, 2017

sekarang berbicara tentang teknis prosedur dan penanganan kasus yang menyebabkan terjadinya penumpukan kasus.

2. Skripsi yang dilakukan oleh Surya Putra Dharma Bakara skripsi berjudul “Upaya Direktorat Kriminal Khusus Subdit *Cyber Crime* Dalam Menanggulangi Tindak Pidana *Cyber Crime* Yang Berkaitan Dengan Pornoaksi dan Pornografi (STUDI POLDA LAMPUNG)” Fakultas Hukum Universitas Lampung tahun 2016.

Penelitian ini dititik beratkan pada Tindak pidana *cybercrime* yang berkaitan dengan pornografi dan pornoaksi di Provinsi lampung telah sering terjadi diantaranya foto bugil polwan, foto bugil mahasiswi yang beredar di *facebook*, dua vidio adegan tidak senonoh sepasang (ABG) yang di duga mahasiwa perguruan tinggi di lampung. Direktorat Kriminal Khusus Subdit *cybercrime* Polda Lampung berdasarkan tugas dan wewenang yang dimilikinya belum juga mampu untuk melakukan pengungkapan tindak pidana *cybercrime* yang berkaitan dengan pornografi dan pornoaksi dengan baik, yang berakibat sering terjadi tindak pidana *cybercrime* yang berhubungan dengan pornografi dan pornoaksi.¹⁴

Perbedaan penelitian ini dengan penelitian yang sedang dilakukan adalah tentang penitikberatan pembahasan. Penelitian yang dilakukan oleh Surya Putra Dharma Bakara (2016) menitikberatkan tentang Upaya Direktorat Kriminal Khusus Subdit *Cybercrime* Dalam Menanggulangi Tindak Pidana *Cybercrime* Yang Berkaitan Dengan Pornografi dan Pornoaksi, sedangkan penelitian yang dilakukan sekarang berbicara tentang teknis prosedur dan penanganan kasus yang menyebabkan terjadinya penumpukan kasus.

¹⁴ Surya Putra Dharma Bakara, “Upaya Direktorat Kriminal Khusus Subdit Cyber Crime Dalam Menanggulangi Tindak Pidana Cyber Crime Yang Berkaitan Dengan Pornografi dan Pornoaksi (STUDI POLDA LAMPUNG)” *skripsi* Fakultas Hukum Universitas Lampung tahun, (Lampung 2016)

3. Skripsi yang dilakukan oleh Avan Avika skripsi berjudul “Tinjauan Yuridis Terhadap Fenomena *Cyber Bullying* Sebagai Kejahatan di Dunia *Cyber* Dikaitkan Dengan Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008” Fakultas Hukum Universitas Hassanudin Makassar tahun 2016.

Penelitian dititik beratkan pada Tinjauan Yuridis Terhadap Fenomena *Cyber Bullying* Sebagai Kejahatan Di Dunia *Cyber* Dikaitkan Dengan Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008”. Dibimbing oleh Andy Sofyan dan Nur Azisa. Penelitian ini bertujuan (1) untuk mengetahui unsur-unsur dari *Cyber Bullying* sehingga dikatakan sebagai bentuk kejahatan, dan (2) untuk mengetahui bagaimana relevansi Putusan MK Nomor 50/PUUVI/2008 terkait dengan fenomena *Cyber Bullying*. Riset ini memakai penelitian normatif, menggunakan materi hukum primer sebagai perangkat dalam menemukan isu hukum menyinggung fenomena *Cyber Bullying* dikaitkan atas Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008. Sedangkan bahan hukum tersier dan sekunder menjadi penunjang dalam menemukan jalaan penyelesaian hukum dari permasalahan *Cyber Bullying* dan keterkaitannya melalui Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008¹⁵.

Perbedaan penelitian ini dengan penelitian yang sedang dilakukan adalah tentang penitikberatan pembahasan. Penelitian yang dilakukan oleh Surya Putra Dharma Bakara (2016) menitikberatkan tentang Tinjauan Yuridis Terhadap Fenomena *Cyber Bullying* Sebagai Kejahatan di Dunia *Cyber* Dikaitkan Dengan Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008, sedangkan penelitian

¹⁵ Antonius Sanda, “Tinjauan Yuridis Terhadap Fenomena *Cyber Bullying* Sebagai Kejahatan di Dunia *Cyber* Dikaitkan Dengan Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008” *skripsi* Fakultas Hukum Universitas Hassanudin Makassar, (Makassar2016)

yang dilakukan sekarang berbicara tentang teknis prosedur dan penanganan kasus yang menyebabkan terjadinya penumpukan kasus.

4. Jurnal yang dilakukan oleh Dian Ekawati ismail, jurnal ilmiah berjudul “*Cyber Crime di Indonesia*” Fakultas Ilmu Sosial Universitas Negri Gorontalo pada tahun 2009.

Penelitian dititik beratkan pada Perkembangan teknologi khususnya dibidang telekomunikasi dan transportasi dianggap sebagai lokomotif dan turut mempercepat proses globalisasi di pelbagai aspek kehidupan. Setiap negara mesti menghadapi kenyataan bahwa informasi dunia saat ini dibangun berlandaskan suatu jaringan yang ditawarkan bagi majunya bidang teknologi. Selaku media penyedia informasi internet juga menjadikan sarana kegiatan komunitas komersial terpesat dan terbesar perkembangannya dan pertumbuhannya. Beragam kasus pelanggaran hukum melewati media internet sekarang sering terjadi di Indonesia, keadaan Indonesia secara garis besar dalam persoalan *cyber crime* sudah terlalu memprihatinkan dan menyedihkan.¹⁶

Perbedaan penelitian ini dengan penelitian yang sedang dilakukan adalah tentang penitikberatan pembahasan. Penelitian yang dilakukan oleh Dian Ekawati Ismail (2009) menitikberatkan tentang kejahatan *cyber crime* yang terjadi di Indonesia secara universal, sedangkan penelitian yang dilakukan sekarang berbicara tentang teknis prosedur dan penanganan kasus yang menyebabkan terjadinya penumpukan kasus.

¹⁶ Dian Ekawati ismail, “Cyber Crime di Indonesia”, *Jurnal* Fakultas Ilmu Sosial Universitas Negri Gorontalo, (Gorontalo 2009)

5. Jurnal yang dilakukan oleh Antoni, jurnal ilmiah berjudul “Kejahatan Dunia Maya (*Cyber Crime*) dalam Simak Online” Fakultas Syariah dan Hukum UIN Raden Fatah Palembang tahun 2018.

Penelitian ini dititik beratkan pada Perkembangan teknologi informasi yang terjadi dewasa ini telah mencapai pada titik puncak-nya. Hal ini bisa terlihat dengan semakin berkembang pesatnya fitur-fitur yang ada didalam teknologi digital, khususnya teknologi komputer berbasis teknologi internet yang mengakibatkan “dunia” kian mengecil. Waktu dan jarak lebih bisa dihemat menggunakan perkembangan teknologi informasi yang datang saat ini. Segenap aktivitas yang seharusnya membutuhkan rentang waktu yang lama serta perlu ditempuh melalui jarak yang jauh, untuk era ini lebih memungkinkan untuk dikerjakan atau diakses dimana-pun cuma hitungan menit atau hanya hitungan detik saja. Begitu juga halnya dengan teknologi digital yang ada didalam fitur-fitur komputer yang berbasis internet, menyuguhkan pengoperasiannya serba canggih dan otomatis, menggunakan sistem komputerisasi atau format yang bisa dibaca dengan komputer. Selaku penjelmaan teknologi digital tersebut ialah penggunaan Sistem Informasi Manajemen Akademik (SIMAK) online dalam aktivitas belajar dan mengajar yang dipergunakan dalam dunia pendidikan khususnya perguruan tinggi. Dengan sambil dipergunakannya teknologi digital di kampus perguruan tinggi, melahirkan kegiatan civitas akademika dibuat semakin mudah. Akan tetapi beragam persoalan pada sisi lain timbul saat penerapan teknologi digital yang digunakan tersebut, salah satu masalah ialah kemungkinan berjalannya kejahatan (*cybercrime*) seperti: manipulasi data yang sudah dimasukkan ke dalam data digital. Ancaman yang dimaksud dimungkinkan terjadi oleh berbagai pihak yang memiliki niat jahat (*mens rea*) dalam dunia

digital untuk memalsukan atau merubah data-data digital yang telah di entry tersebut.¹⁷

Perbedaan penelitian ini dengan penelitian yang sedang dilakukan adalah tentang penitikberatan pembahasan. Penelitian yang dilakukan oleh Antoni (2018) menitikberatkan tentang kejahatan *cybercrime* secara umum, sedangkan penelitian yang dilakukan sekarang berbicara tentang teknis prosedur dan penanganan kasus yang menyebabkan terjadinya penumpukan kasus.

E. Metode Penelitian

1. Jenis penelitian

Penelitian ini adalah jenis penelitian hukum kualitatif, metode penelitian yang menghasilkan data yang deskriptif, yang bersumber dari tulisan atau pernyataan dan tingkah laku yang dapat diobservasi dari manusia.¹⁸ Penelitian ini membahas tentang problematika prosedur dan penanganan terhadap penumpukan perkara tindak pidana *cybercrime* di polda jateng.

2. Pendekatan penelitian

Pendekatan penelitian yang digunakan dalam penelitian ini adalah pendekatan yuridis empiris (non doktrinal). Metode penelitian yuridis empiris merupakan metode penelitian hukum yang mengkaji ketentuan hukum yang berlaku serta apa yang terjadi dalam kenyataan di masyarakat atau penelitian yang dilakukan terhadap keadaan sebenarnya yang terjadi di masyarakat, dengan maksud menemukan fakta-fakta yang dijadikan data penelitian yang kemudian data tersebut

¹⁷ Antoni, A, "Dunia Maya (Cyber Crime) Dalam Simak Online", *Skripsi* Fakultas Syariah dan Hukum UIN Raden Fatah Palembang, (Palembang 2018)

¹⁸ Burhan Ashshofa, *Metode Penelitian Hukum*, (Jakarta: PT Rineka Cipta, 2013), hal.16.

dianalisis untuk mengidentifikasi masalah yang pada akhirnya menuju pada penyelesaian masalah¹⁹, yaitu mengkaji konsep normatifnya atau peraturan perundang-undangan, hukum dilihat sebagai norma atau *das sollen*, dikarenakan dalam membahas permasalahan penelitian ini menggunakan bahan-bahan hukum yang tertulis (hukum yang dibuat oleh pejabat yang berwenang yang berlaku umum dengan ancaman sanksi yang tegas) dan yang tidak tertulis (hukum yang berlaku di masyarakat) atau baik bahan hukum primer maupun bahan hukum sekunder.²⁰ Pendekatan empiris yaitu hukum sebagai kenyataan sosial atau *das sein*, karena dalam penelitian ini digunakan data primer yang diperoleh dari lapangan atau mengkaji pada kenyataan yang ada tentang prosedur penanganan tindak pidana *cybercrime* dan problematika penumpukan perkara *cybercrime* di Polda Jateng.

3. Lokasi Penelitian

Lokasi penelitian yang menjadi tempat melaksanakan penelitian dan memperoleh data-data adalah Ditreskrimsus Polda Jateng karena menurut Peneliti Ditreskrimsus Polda Jateng adalah kepolisian yang memiliki wewenang untuk melakukan penyelidikan, penyidikan dan penuntutan perkara-perkara tindak pidana *cybercrime*.

4. Sumber Data

Adapun dalam penelitian ini, penulis akan menggunakan sumber data sebagai berikut:

- a. Sumber Data Primer

¹⁹ Bambang Waluyo, *Penelitian Hukum Dalam Praktek*, (Jakarta: Sinar Grafika, 2002) Hal 15-16

²⁰ Soerjono dan Abdurrahman, *Pengantar Penelitian Hukum*, (Jakarta: UI-Press, 1986), hal 10.

Data Primer yaitu data yang diperoleh seorang peneliti langsung dari sumber pertama tanpa perantara pihak lain (langsung dari objeknya). Data primer dalam skripsi ini berupa sejumlah keterangan atau fakta tentang peran Ditreskrimsus Unit *Cybercrime* Polda Jateng dalam Prosedur Penanganan Tindak Pidana *Cybercrime* dan Problematika Penumpukan Perkara *Cybercrime* di Polda Jateng yang diperoleh dari hasil wawancara dengan R. Haryo Seto L SH, M.krim, divisi Siber Ditreskrimsus Polda Jateng.

b. Sumber Data Sekunder

Data sekunder yaitu data yang diperoleh seorang peneliti secara tidak langsung dari sumbernya (objek penelitian), tetapi melalui sumber lain²¹. Dalam penelitian ini, data sekunder berupa data-data *cybercrime* di Saikara Ditreskrimsus Polda Jateng Tahun 2019 – 2020.

c. Bahan Hukum

Penelitian ini menggunakan bahan hukum atau “*source of law*” yang merupakan sesuatu (seperti konstitusi, perjanjian, undang-undang, atau kebiasaan) yang memberikan wewenang untuk undang-undang dan keputusan pengadilan; titik asal untuk hukum atau analisis hukum. Menurut *Black law Dictionary*, bahan hukum dikategorikan menjadi (i) Asal-usul konsep dan ide hukum; (ii) Lembaga pemerintah yang merumuskan aturan hukum; dan (iii) Manifestasi hukum yang diterbitkan (buku, basis data komputer, bentuk mikro,

²¹ Suteki & Galang Taufani, *Metodologi Penelitian Hukum (Filsafat, Teori dan Praktik)*, (Depok: PT Raja Grafindo Persada, 2018), hal.213.

disk optik, dan media lain yang berisi informasi hukum adalah semua sumber hukum).²²

Bahan hukum ada dua macam, yaitu bahan hukum primer dan sekunder. Bahan hukum dimaksud lebih menitikberatkan pada sumber-sumber kepustakaan, sebagaimana dinyatakan oleh Robert Watt:²³ Bahan hukum yang digunakan dalam skripsi ini yaitu bahan hukum primer dan bahan hukum sekunder²⁴.

- 1) Bahan Hukum Primer, yang terdiri dari peraturan perundang-undangan, yurisprudensi atau keputusan pengadilan dan perjanjian internasional, bersifat otoratif yaitu merupakan hasil dari tindakan atau kegiatan yang dilakukan oleh lembaga yang berwenang untuk itu²⁵ meliputi:
 - a. Undang-Undang Dasar Negara Republik Indonesia 1945
 - b. Kitab Undang-Undang Hukum Acara Pidana.
 - c. Undang-undang Nomor 1 tahun 1946 Jo Undang-undang Nomor 73 Tahun 1958 tentang Pembentukan Kitab undang-undang hukum Pidana.
 - d. Undang-Undang No.8 tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP).
 - e. Undang-undang Nomor. 2 tahun 2002 Tentang Kepolisian Negara Republik Indonesia.
 - f. PP No. 27 Tahun 1983 jo PP No.58 Tahun 2010 tentang Pelaksanaan KUHAP.

²²Henry Campbell Black, M. A, *Blacks Law Dictionary*, (ST. Paul, Minn: West Publshing CO, 1968),hal.1400.

²³Robert Watt, *concise legal research*, (NSW: The federation Press, 2001),hal.1.

L.J. Van Apeldoorn, 2005, Pengantar Ilmu Hukum, Cet. 31, (PT. Pradnya Paramita, 2005) hal.3.

²⁵Suteki & Galang Taufani, *Metodologi Penelitian...* ,214.

- g. Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 14 Tahun 2012 tentang Manajemen Penyidikan Tindak Pidana.
 - h. Undang-Undang Nomor 11 Tahun 2008 Tentang Internet & Transaksi Elektronik (ITE).
- 2) Bahan Hukum Sekunder²⁶.

Bahan hukum sekunder adalah bahan-bahan yang erat kaitannya dengan bahan hukum primer dan dapat membantu menganalisis dan memahami bahan hukum primer, meliputi literatur-literatur dan hasil penelitian yang berkaitan dengan masalah yang dibahas dalam penelitian ini.

5. Metode Pengumpulan Data

a. Wawancara

Wawancara (*interview*), digunakan untuk mendapatkan informasi atau keterangan secara langsung dari narasumber di lokasi penelitian.²⁷ Wawancara yang digunakan penulis berbentuk wawancara terstruktur yaitu kepada informan diajukan pertanyaan yang telah disediakan sebelumnya untuk menghindari data yang tidak lengkap. Dalam hal ini informan tidak terbatas dalam memberikan jawaban sehingga memberikan keterangan secara bebas. Informan dalam penelitian ini adalah polisi bidang *Cybercrime* yang sudah ditunjuk oleh Polda Jateng, yaitu Bripta R Haryo Seto I. SH. M.Krim divisi siber ditreskrimsus Polda Jateng, karena bidang inilah yang mempunyai peran dalam pengetahuan ataupun keilmuan tentang manajemen penyidikan *cybercrime*.

²⁶ Ibid, hal.214.

²⁷ Abdulkadir Muhammad, *Hukum dan Penelitian Hukum*, (Bandung: Citra Aditya Bakti, 2004),hal 87-88.

b. Dokumentasi

Metode dokumentasi ialah mencari data atau hal-hal variable berupa transkrip, catatan, buku, majalah, surat, prasasti, notulen rapat, agenda, dan sebagainya.²⁸ Atau dapat juga diartikan sebagai proses pengumpulan data sekunder yang dicari dan diperlukan. Selanjutnya melakukan *content identification* dengan mempelajari substansi dari data sekunder tersebut. Dokumentasi untuk mendokumentasikan data-data sekunder yang diperoleh dari Ditreskrimsus Polda Jateng dan bahan-bahan hukum yang ada.

6. Teknik Pengujian Validitas Data

Dalam suatu penelitian, kevaliditasan data memiliki pengaruh yang amat besar didalam memastikan hasil akhir suatu penelitian. Sehingga buat memperoleh data yang valid diperlukan suatu teknik mengecek keabsahan suatu data. Keabsahan data dalam penelitian ini menggunakan teknik Triangulasi. Triangulasi ialah suatu teknik pemeriksaan data yang menggunakan sesuatu hal yang lain diluar itu demi keperluan pemeriksaan dan perbandingan terhadap data itu.²⁹

Teknik triangulasi dalam skripsi ini menggunakan triangulasi sumber dengan langkah-langkah sebagai berikut :³⁰

1. Membandingkan data hasil interviu dengan data hasil pengamatan.
2. Membandingkan apa yang dikatakan orang di depan umum dengan apa yang dikatakan secara pribadi.
3. Membandingkan apa yang diungkapkan orang-orang terhadap situasi penelitian beserta apa yang diungkapkan sepanjang waktu.

²⁸ Arikunto Suharsimi, *Prosedur Penelitian : Suatu Pendekatan Praktek*, (Jakarta : Rineka Cipta, 1992), hal.236.

²⁹ Moloeng, Lexy J, *Metode Penelitian Kualitatif*, (Bandung: PT Rosdakarya, 2002), hal.178.

³⁰ Moloeng, Lexy J, *Metode Penelitian...*, hal.180.

4. Membandingkan perspektif dan keadaan seseorang melalui berbagai pandangan dan pendapat orang semacam rakyat biasa, orang yang berpendidikan menengah atau tinggi, orang pemerintahan, maupun orang berada.
5. Membandingkan hasil *interview* menggunakan isi suatu dokumen yang berkaitan. Dengan menggunakan teknik ini penelitian dilakukan dengan membandingkan data-data yang diperoleh dari Ditreskrimsus Polda Jateng melalui wawancara dengan isi suatu data dokumen yang berkaitan seperti literatur, buku-buku, peraturan perundang-undangan yang berlaku dan pendapat para ahli yang berhubungan dengan masalah yang diteliti, seperti dokumen yang didapat dari Ditreskrimsus Polda Jateng. Bertujuan supaya mendapatkan hasil penelitian yang diharapkan sebanding dengan fokus yang diteliti. Diharapkan beserta data yang valid bisa memperkuat hasil dari penelitian.

7. Metode Analisis Data

Teknik analisis data dalam penelitian penting agar data yang sudah terkumpul dapat dianalisis, sehingga dapat menghasilkan jawaban untuk memecahkan masalah-masalah yang telah dikemukakan. Teknik analisis data dalam penelitian ini menggunakan analisis kualitatif dengan interaktif model yaitu komponen penyajian data dan reduksi data dilaksanakan bersama dengan pengumpulan data, lalu setelah data terkumpul lantas tiga komponen tersebut berinteraksi dan bila kesimpulan dirasa kurang maka perlu adanya penelitian dan verifikasi kembali mengumpulkan data lapangan.³¹ Tahapan-tahapannya adalah:³²

³¹ H.B.Sutopo, "*Metode Penelitian Kualitatif*", (Surakarta: UNS Press,1999), hal 8.

³² Ibid, hal 9.

- a. Reduksi data, merupakan metode seleksi, abstraksi dan penyederhanaan dari data *fieldnote*.
- b. Penyajian data, merupakan suatu realita organisasi informasi yang memungkinkan kesimpulan penelitian dapat dilakukan, sajian data dapat meliputi berbagai jenis matrik, gambar atau skema, jaringan kerja, kaitan kegiatan dan table.
- c. Kesimpulan dan verifikasi. Dalam pengumpulan data peneliti harus sudah memahami berbagai hal yang di temui, dengan melakukan pencatatan peraturan-peraturan, pola pernyataan, konfigurasi-konfigurasi yang mungkin, arahan sebab akibat dan berbagai potensi kesimpulan yang diverifikasi.

F. Sistematika Penulisan

Untuk memberikan pemahaman menyeluruh mengenai pembahasan dalam penulisan hukum ini. Dalam bagian ini, penulis mensistematisasikan dalam bagian-bagian yang akan dibahas menjadi lima bab dan tiap-tiap bab dibagi dalam sub-sub bab yang saling terkait, tersistematis, terarah dan mudah dimengerti, sehingga saling mendukung dan menjadi satu kesatuan yang bulat dan utuh. Adapun sistematika penulisan hukum tersebut adalah sebagai berikut :

BAB I : PENDAHULUAN

Dalam bab ini penulis menguraikan mengenai latar belakang masalah, rumusan masalah, tujuan dan manfaat penelitian, tinjauan pustaka, kerangka pemikiran, metode penelitian, dan sistematika penulisan.

BAB II : KONSEP DAN TEORI

Dalam bab ini penulis menguraikan mengenai tinjauan tentang sistem peraturan kepolisian, tinjauan tentang cyber crime, tinjauan tentang

Ditreskrimsus Polda Jateng, tinjauan tentang Problematika Prosedur dan Penanganan Terhadap Penumpukan Perkara Tindak Pidana Cyber Crime, Teori Sistem Hukum, Teori Bekerjanya Hukum.

BAB III : PROSEDUR PENANGANAN TINDAK PIDANA *CYBERCRIME*

Dalam bab ini penulis menguraikan mengenai gambaran umum tentang Polda Jateng, kedudukan Ditreskrimsus Polda Jateng dalam sistem peradilan pidana pada tindak pidana cyber crime, serta prosedur penanganan dan langkah-langkah polda jateng dalam menangani Tindak Pidana *cyber crime*.

BAB IV: PROBLEMATIKA DAN PENYELESAIAN PENUMPUKAN PERKARA *CYBERCRIME* DI POLDA JATENG

Dalam bab ini memuat hasil penelitian dan pembahasan tentang Problematika dan penyelesaian terhadap penumpukan perkara *Cybercrime* di Polda Jateng, serta upaya yang dilakukan Ditreskrimsus Polda Jateng untuk memaksimalkan perannya dalam mengatasi Tindak Pidana *cyber crime* di Polda Jateng.

BAB V : PENUTUP

Dalam bab ini penulis menguraikan mengenai simpulan serta saran dari hasil penelitian yang telah dilakukan penulis yang dapat penulis kemukakan pada para pihak yang terkait.

BAB II

TINJAUAN UMUM *CYBERCRIME*

A. Tindak Pidana *Cybercrime*

1. Pengertian *Cybercrime*

Cyber Crime apabila kita terjemahkan kedalam bahasa Indonesia hingga maksudnya kejahatan siber. Kata kejahatan dalam Kamus Besar Bahasa Indonesia (KBBI) ialah perbuatan yang jahat, watak yang jahat ataupun sikap yang berlawanan dengan nilai serta norma yang berlaku yang sudah disahkan oleh hukum. Ada pula kata siber dalam Kamus Besar Bahasa Indonesia merupakan sistem PC serta data ataupun berhubungan dengan internet.

Kejahatan merupakan kelakuan yang diancam pidana yang bertabat melawan hukum yang berhubungan dengan kesalahan serta dicoba oleh orang yang sanggup bertanggung jawab. Penafsiran yang lain mengenai *cyber crime* merupakan kejahatan berbasis *teknologi* telematika yang berikutnya disebut sebagai kejahatan telematika dalam bermacam sumber kerap diucap dengan sebutan: Penyalahgunaan PC ataupun Kejahatan PC (*computer crime; computer- related crime; computer assisted crime*). Kejahatan Mayantara (*cyber crime*), Kejahatan PC (*computer cyber*).³³

Gregory mengemukakan *cybercrime* adalah bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung melalui internet, dan dapat mengeksploitasi komputer lain yang terhubung dengan internet. Keamanan sistem yang memiliki banyak celah dapat menyebabkan seorang hacker memanfaatkan celah

³³ Aloysius Wisnubroto, *Strategi Penanggulangan Kejahatan Telematika*, Penerbit Universitas Atma Jaya Yogyakarta, (Yogyakarta, 2010), hal 1.

keamanan untuk masuk ke dalam sistem, merusak serta mengambil data-data yang tidak seharusnya diketahui oleh pihak luar³⁴.

Cybercrime merupakan kejahatan yang berbeda dengan kejahatan konvensional (*street crime*). *Cyber crime* muncul bersamaan dengan lahirnya revolusi teknologi informasi. Sebagaimana dikemukakan oleh Ronni R. Nitibaskara bahwa: “Interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi. Penyimpangan social menyesuaikan bentuk dan karakter baru dalam kejahatan³⁵.

Menurut Undang-Undang ITE No 11 Tahun 2008 tentang Informasi Transaksi Elektronik sendiri mendefinisikan *cybercrimes* atau kejahatan elektronik sebagai: Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, elektronik data interchange (EDI), surat elektronik (*electronic mail*), *telegram*, *teleks*, *telecop*y atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya³⁶.

“*Computer abuse is broadly defined to be any incident associated with computer technology in which a victim suffered or could suffered loss and a perpetrator by intention made or could have gain*”, yang kemudian diterjemahkan oleh Andi Hamzah sebagai penyalahgunaan komputer didefinisikan secara luas sebagai suatu kejadian yang berhubungan dengan teknologi komputer yang seorang

³⁴ Robert. J Gregory, Op. Ciit, hal 139.

³⁵ Ronni R Nitibaskara dalam Didik M. Arief Mansur dan Elisatris Gultom, Cyber Law Aspek Hukum Teknologi Informasi, (Bandung, PT Refika Aditama, 2005) hlm. 25.

³⁶ Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik

korban menderita atau akan telah menderita kerugian dan seorang pelaku dengan sengaja memperoleh keuntungan atau akan telah memperoleh keuntungan”.³⁷

Berdasarkan berbagai pengertian *computer crime* di atas, maka dapat dirumuskan bahwa *computer crime* merupakan perbuatan melawan yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Adapun ruang lingkup kejahatan siber antara lain, yaitu: (a) pembajakan; (b) penipuan; (c) pencurian; (d) pornografi; (e) pelecehan; (f) pemfitnahan; dan (g) pemalsuan.³⁸ Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi dalam beberapa literatur dan praktiknya dikelompokkan dalam beberapa bentuk, antara lain:

- a. *Unauthorized Access to Computer System and Service* (Akses tidak sah ke sistem komputer dan jasa); Adalah suatu bentuk kejahatan yang dilakukan dengan cara merentas atau memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah. Biasanya pelaku kejahatan (*hacker*) melakukan dengan tujuan sabotase atau mencuri data/informasi penting dan rahasia. Namun begitu, tidak sedikit juga yang melakukan hal tersebut karena merasa tertantang dan ingin menguji keahliannya untuk menembus suatu sistem dengan tingkat keamanan yang tinggi. Ada juga yang melakukan hal tersebut untuk iseng atau menyampaikan aspirasi dengan cara yang berbeda. Seperti kasus situs Telkomsel yang dihack oleh *hacker*;
- b. *Illegal Contents*, Merupakan suatu modus *cyber crime* dengan cara memasukkan data atau informasi ke Internet tentang sesuatu hal yang tidak benar, tidak etis,

³⁷ Andi Hamzah, Hukum Pidana yang berkaitan dengan komputer, (Jakarta : Sinar Grafika Offset, 1993) hal. 18

³⁸ Maskun, *Kejahatan Siber Cyber Crime*, (Jakarta:Kharisma Putra Utama,2013) hal. 50-51.

dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contoh dapat penulis kemukakan pemuatan pemberitaan yang bohong/ tidak benar atau memfitnah yang dampaknya dapat meruntuhkan harkat martabat atau harga diri pihak lain, atau hal-hal yang berhubungan dengan pornografi dan penghinaan bahkan pemuatan informasi yang merupakan rahasia negara.

- c. *Data Forgery*, Adalah modus kejahatan dalam dunia maya yang dilakukan dengan cara memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scripless dokument melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah olah terjadi salah ketik yang pada akhirnya menguntungkan pelaku;
- d. *Cyber Espionage*, Suatu modus operandi kejahatan dunia maya yang memanfaatkan jaringan internet, untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan cara memasuki sistem jaringan komputer (*computer network system*) pihak yang menjadi sasarannya.
- e. *Cyber sabotage and extortion*, kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, yang mengakibatkan data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut,

tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai *cyber-terrorism*.

- f. *Offense against Intellectual property*, Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.
- g. *Infringements of privacy*, kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. 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.³⁹

2. Kebijakan Kriminal Penanggulangan *Cybercrime*

Kebijakan penanggulangan *cybercrime* dengan hukum pidana termasuk bidang *penal policy* yang merupakan bagian dari *criminal policy* (kebijakan penanggulangan kejahatan). Ditinjau dari sudut *criminal policy*, usaha penanggulangan kejahatan (termasuk penanggulangan *cybercrime*) tidak bisa dilaksanakan semata-mata secara parsial dengan hukum pidana (sarana penal), namun harus pula ditempuh dengan pendekatan sistemik/integral.⁴⁰ Sebagai salah satu bentuk *high tech crime* yang dapat melampaui batas-batas negara (bersifat

³⁹ Antoni, "Kejahatan Dunia Maya (Cyber Crime) dalam Simak Online", dikutip dari <http://jurnal.radenfatah.ac.id/index.php/Nurani/article/view/1192>, diakses pada 22 Juli 2021.

⁴⁰ Barda Nawawi Arif, *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan* (Bandung : Citra Aditya Bakti, 2005), hal,125.

transnational/ transborder), merupakan hal yang wajar jika upaya penanggulangan *cybercrime* juga harus ditempuh dengan pendekatan teknologi (*techno prevention*). Dibalik itu, diperlukan juga pendekatan kultural/budaya, pendekatan edukatif/moral, dan bahkan menggunakan pendekatan global melalui kerjasama internasional.

Operasionalisasi kebijakan penal meliputi kriminalisasi, dekriminalisasi, penalisasi dan depenalisasi. Penegakan hukum pidana tersebut sangat tergantung pada perkembangan politik hukum, politik kriminal, dan politik sosial. Oleh karena itu, penegakan hukum tidak hanya memperhatikan hukum yang otonom, melainkan memperhatikan juga masalah kemasyarakatan dan ilmu perilaku sosial⁴¹. Kebijakan criminal merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana).⁴² Jadi pada hakikatnya, kebijakan kriminalisasi adalah bagian atas kebijakan kriminal (*criminal policy*) dengan memanfaatkan sarana hukum pidana (penal) sehingga itu tergolong bagian dari kebijakan hukum pidana (*penal policy*), khususnya kebijakan formulasi.

Menurut Bassiouni, keputusan untuk melakukan dekriminalisasi dan kriminalisasi mesti didasarkan pada faktor-faktor kebijakan tertentu dengan menimbang bermacam-macam faktor, termasuk ⁴³:

- a. Keseimbangan sarana-sarana yang memerlukan didalam hubungannya dengan hasil-hasil yang ingin dicapai;
- b. Analisis biaya terhadap hasil-hasil yang diperoleh dalam hubungannya dengan tujuan-tujuan yang dicari;

⁴¹ Bambang Poernomo, *Kapita Selekta Hukum Pidana* (Yogyakarta: Liberty, 1988), 52.

⁴² Barda Nawawi Arif, *Op.Ciit.*, hal,130.

⁴³ *Ibid.*, hal, 132.

- c. Penafsiran atau penelitian tujuan-tujuan yang dicari itu dalam kaitannya bersama prioritas-prioritas lainnya didalam pengalokasian sumber-sumber tenaga manusia;
- d. Pengaruh sosial dari dekrimalisasi dan kriminalisasi yang berkenaan dengan pengaruh-pengaruhnya yang sekunder.

Sudarto menyatakan bahwa di dalam menjalankan kriminalisasi sebuah perbuatan harus diperhatikan empat hal berikut:⁴⁴

- a. Penerapan hukum pidana harus memperhatikan tercapainya pembangunan nasional, yaitu mewujudkan masyarakat yang adil dan makmur yang merata baik spiritual maupun material berdasarkan Pancasila;
- b. Aktivitas yang diusahakan untuk ditanggulangi dan dicegah dengan hukum pidana seharusnya merupakan perbuatan yang tidak dikehendaki, yaitu perbuatan yang menghadirkan kerugian (material dan spiritual) pada kalangan warga masyarakat;
- c. Penggunaan hukum pidana perlu mempertimbangkan prinsip “biaya dan hasil” (*cost and benefit principle*);
- d. Penggunaan hukum pidana perlu pula memperhatikan kapasitas atau kemampuan daya kerja dari badan-badan penegak hukum pidana, jangan sampai ada kelebihan beban tugas (*overbelasting*).

Ada lima hal yang perlu diperhatikan oleh pembentuk undang-undang (legislator) dalam melakukan kriminalisasi *cybercrime*, yaitu:⁴⁵

- a. Kriminalisasi harus merupakan usaha yang mendukung terciptanya tujuan akhir kebijakan kriminal, yakni mensejahterakan dan melindungi masyarakat;

⁴⁴ Sudarto, *Hukum dan Hukum Pidana*, (Bandung: Alumni, 1981), hal.44-48.

⁴⁵ Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, (Yogyakarta: Aswaja Pressindo, 2008), hal.60-61.

- b. Perbuatan yang akan dikriminalisasi tersebut benar-benar dicela oleh masyarakat;
- c. Perlu diperkirakan tentang keuntungan dan kerugian kriminalisasi;
- d. Perlu diusahakan supaya tidak terjadi over-kriminalisasi yang bisa berpengaruh secara sekunder berkenaan kepentingan masyarakat;
- e. Perlu disesuaikan antara kemampuan penegak hukum dengan penegakan hukum;

3. Formulasi Tindak Pidana *Cybercrime*

Formulasi hukum pidana di Indonesia yang berkaitan dengan masalah *cybercrime*, selama ini dapat diidentifikasi sebagai berikut:

- a. Dalam KUHP

Perumusan tindak pidana di dalam KUHP kebanyakan masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan *cybercrime*, selain itu juga terdapat berbagai kelemahan dan keterbatasan dalam menghadapi perkembangan teknologi dan *high tech crime* yang sangat bervariasi. Dalam kasus *Unauthorized Transfer Payment* di Bank Negara Indonesia (BNI) Cabang New York Agency (Tahun 1986), Pengadilan Negeri Jakarta Pusat selain menjatuhkan pidana penjara terhadap terdakwa karena terbukti secara sah dan meyakinkan melanggar Pasal 363 KUHP, yaitu pencurian yang dilakukan oleh lebih dari 2 orang atau lebih secara bersama-sama, juga membuktikan bahwa terdakwa terbukti secara sah dan meyakinkan melanggar Pasal 233 KUHP yaitu merusak barang yang digunakan untuk membuktikan sesuatu dihadapan pihak yang berwajib. Putusan itu dikuatkan Putusan Pengadilan Tinggi Jakarta, dan

Putusan Mahkamah Agung.⁴⁶ Pasal 233 KUHP Barang siapa dengan sengaja menghancurkan, merusak, membikin tidak dapat dipakai, menghilangkan barang-barang yang digunakan untuk meyakinkan atau membuktikan sesuatu di muka penguasa yang berwenang, akta-akta, surat-surat atau daftar-daftar yang atas perintah penguasa umum, terus-menerus atau untuk sementara waktu disimpan, atau diserahkan kepada seorang pejabat, ataupun kepada orang lain untuk kepentingan umum, diancam dengan pidana penjara paling lama empat tahun.

b. Undang-undang di luar KUHP

- 1) UU No.36 Tahun 1999 tentang Telekomunikasi, diancam pidana terhadap perbuatan: (1) menyalahgunakan akses ke jaringan telekomunikasi (Pasal 50 jo.22); (2) mengakibatkan gangguan fisik dan elektromagnetik kepada penyelenggaraan telekomunikasi (Pasal 55 jo.38); (3) menyadap informasi melewati jaringan telekomunikasi (Pasal 56 jo.40).
- 2) Pasal 26A UU No. 20 Tahun 2001 tentang Perubahan Atas UU No.31 Tahun 1999 terhadap Pemberantasan Tindak Pidana Korupsi; Pasal 38 UU No.15 Tahun 2002 terhadap Tindak Pidana Pencucian Uang; dan pasal 44 Ayat (2) UU No.30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi; mengakui electronic record menjadi alat bukti yang sah.
- 3) UU No.32 Tahun 2002 tentang Penyiaran, diantara lain mengatur tindak pidana:
- 4) Pasal 57 jo. 36 Ayat (5) mengancam pidana kepada siaran yang: a) bersifat menghasut, fitnah, menyesatkan dan/atau bohong; b) menonjolkan faktor

⁴⁶ Aloysius Wisnubroto, Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer, Universitas Atmajaya, Yogyakarta, 1999, hlm.131.

kekerasan, perjudian, cabul, penyalahgunaan narkotika dan obat terlarang; atau c) mempertentangkan, agama, ras, suku dan antar golongan.

- 5) Pasal 57 jo. 36 Ayat (6) mengancam pidana kepada siaran yang merendahkan, melecehkan, memperolokkan mengabaikan nilai-nilai agama, harkat manusia Indonesia, dan merusak hubungan internasional.
- 6) Pasal 58 jo. 46 Ayat (3) mengancam pidana terhadap siaran iklan niaga yang memuat didalamnya: a) promosi yang menghubungkan dengan ajaran suatu ideologi, agama, pribadi dan/atau kelompok, yang menyinggung perasaan dan merendahkan martabat orang lain, ideologi orang lain, pribadi orang lain, dan atau kelompok orang lain; b) promosi minuman keras atau sejenisnya dan bahan zat adiktif; c) promosi rokok yang memperagakan wujud rokok; d) hal-hal yang bertentangan terhadap kesusilaan masyarakat dan nilai-nilai agama; dan/atau e) eksploitasi anak di bawah umur 18 tahun.
- 7) Undang-Undang No. 28 Tahun 2014 tentang Hak Cipta

Ketentuan Undang-Undang No. 28 Tahun 2014 tentang Hak Cipta diterapkan pada kasus pembajakan Program Komputer *Word Star* versi 5.0, pada tahun 1990. pengadilan negeri bandung menjatuhkan pidana penjara dan pidana denda kepada terdakwa, karena terbukti secara sah dan meyakinkan melanggar Pasal 11 ayat (1) huruf k, juncto Pasal 14 huruf g, juncto pasal 44 ayat (1) Undang-undang No. 7 Tahun 1987 tentang hak cipta, juncto Keputusan Presiden (Kepres) RI Nomor 25 Tahun 1989, Juncto Pasal 55 ayat (1), juncto pasal 64 KUHP. Putusan ini dikuatkan oleh Putusan Pengadilan Tinggi Bandung.⁴⁷ Dalam pasal 11 ayat (1) huruf k, diatur tentang program komputer sebagai hak cipta khusus. Pasal 44 ayat (1)

⁴⁷ Aloysius Wisnubroto. Ibid, hlm, 162.

Barangsiapa dengan sengaja dan tanpa hak mengumumkan atau memperbanyak suatu ciptaan atau memberikan izin untuk itu, dipidana dengan pidana penjara paling lama 7 (Tujuh) tahun dan/ atau denda paling banyak Rp 100.000.000 (seratus juta rupiah).

8) UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU-ITE), Bab VII Perbuatan yang dilarang, bermuat ketentuan pidana bagi setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mentransmisikan dan/atau mendistribusikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan:

- a) Melanggar kesusilaan; mempunyai muatan perjudian; mempunyai muatan penghinaan dan/atau pencemaran nama baik; mempunyai muatan pemerasan dan/atau pengancaman (Pasal 27).
- b) Menebarkan informasi bohong dan menyesatkan yang menimbulkan kerugian konsumen dalam transaksi elektronik; menyebarkan informasi yang bertujuan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok dalam masyarakat tertentu berdasarkan pada suku, agama, ras, dan antar golongan (SARA) (Pasal 28)
- c) Mengirimkan informasi yang bermuat ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29).
- d) Mengakses komputer dan/atau sistem elektronik milik orang lain; mengakses komputer dan/atau sistem elektronik dengan tujuan memperoleh informasi elektronik dan/atau dokumen elektronik; mengakses komputer dan/atau sistem elektronik dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan (Pasal 30).

- e) Melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik; melakukan intersepsi elektronik pada transmisi dokumen elektronik dan/atau informasi elektronik yang tidak bersifat publik (Pasal 31)
- f) Menambah, merubah, mengurangi, melakukan transmisi, merusak, memindahkan, menghilangkan, menyembunyikan, suatu informasi elektronik dan/atau dokumen elektronik milik publik atau orang lain; mentransfer atau memindahkan informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak mempunyai hak; menimbulkan terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia menjadikan dapat diakses oleh publik dengan keutuhan data yang bukan sebagaimana mestinya (Pasal 32).
- g) Terhambatnya sistem elektronik dan/atau mengakibatkan sistem elektronik jadi tidak bekerja sebagaimana mestinya (Pasal 33).
- h) Memproduksi, mengadakan, menjual untuk digunakan, mengimpor, mendistribusikan, memiliki, atau menyediakan (a) perangkat lunak atau perangkat keras yang dikembangkan atau secara khusus dirancang untuk memudahkan perbuatan sebagaimana dimaksud Pasal 27-33; (b) sandi lewat komputer, kode akses, atau hal lain yang serupa dengan itu yang ditujukan agar sistem elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan dalam Pasal 27-33 (Pasal 34).
- i) 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 35).

- j) Melakukan perbuatan sebagaimana dimaksud dalam Pasal 27-34 yang mengakibatkan kerugian bagi orang lain (Pasal 36).
- k) Melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27-36 diluar wilayah Indonesia terhadap sistem elektronik yang berada di wilayah yurisdiksi Indonesia (Pasal 37). Kriminalisasi cybercrime di Indonesia khususnya dalam UU-ITE dapat dibagi dalam dua kategori, yaitu perbuatan yang menggunakan komputer sebagai sarana kejahatan, dan perbuatan-perbuatan 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 menciptakan komputer sebagai sasaran ialah setiap aktivitas dengan menggunakan komputer yang ditujukan pada sistem komputer, data komputer, atau jaringan komputer, atau ketiganya secara bersama-sama. Perilaku tersebut dilakukan bukan di ruang nyata, melainkan di ruang maya, sehingga semua aktivitas yang dilarang sebab peraturan perundang-undangan terjadi di ruang maya.⁴⁸

B. Pertanggungjawaban Pidana atau Pidanaan

Pertanggungjawaban pidana pada dasarnya mengandung pencelaan pembuat (subjek hukum) berdasarkan tindak pidana yang sudah dilakukannya. Oleh sebab itu,

⁴⁸ Widodo, *Aspek Hukum Pidana*, Op.Cit, hal 64-66.

pertanggungjawaban pidana mengandung di dalamnya pencelaan/ pertanggungjawaban subjektif dan objektif. artinya, secara objektif si pencipta telah melakukan tindak pidana menurut hukum yang berjalan (asas legalitas), dan secara subjektif si pencipta patut dipertanggungjawabkan berdasarkan tindakan pidana yang dilakukan itu (*asas culpabilitas/kesalahan*) sehingga layak dipidana. Persyaratan dan asas-asas pertanggungjawaban pidana tersebut adalah hal-hal yang telah diterima secara konvensional dan umum dalam doktrin/teori, maupun didalam peraturan perundang-undangan (hukum positif). Bagi adanya pertanggungjawaban pidana mula-mula harus memenuhi persyaratan objektif, yaitu perbuatannya mesti sudah merupakan tindak pidana menurut hukum yang berjalan (asas legalitas).⁴⁹

Berdasar persyaratan objektif yang konvensional, pertanggungjawaban *cybercrime* mestinya harus didasarkan atas dasar sumber hukum perundang-undangan yang berjalan saat ini, baik didalam KUHP ataupun didalam undang-undang khusus di luar KUHP. Namun dalam nyatannya didalam peraturan perundang-undangan yang ada dan berjalan sekarang di Indonesia, tidak semua kasus *cybercrime* bisa dijangkau. Selain itu didalam peraturan perundang-undangan yang berlaku sekarang (baik KUHP maupun UU khusus di luar KUHP) mempunyai berbagai kelemahan dan kemampuan sangat terbatas didalam menghadapi berbagai masalah *cybercrime*. Berbagai kelemahan atau masalah tersebut antara lain:⁵⁰

- a. Di dalam UU No.32 Tahun 2002 tentang penyiaran, belum ada penentuan kualifikasi delik (sebagai pelanggaran atau kejahatan) sehingga mampu menimbulkan masalah yuridis;

⁴⁹ Admaja Priyatno, Kebijakan Legislasi Tentang Sistem Pertanggungjawaban Pidana Korporasi di Indonesia,(CV. Utomo, Bandung, 2004), Hal. 15.

⁵⁰ Barda Nawawi Arif, Op.Cit, hal.142.

- b. Dalam berbagai undang-undang, terdapat subjek hukum berupa korporasi namun tidak membuat aturan tentang pertanggungjawaban pidana untuk korporasi, misalnya dalam UU No.36 Tahun 1999 tentang Telekomunikasi;
- c. Didalam undang-undang yang mengatur pertanggungjawaban pidana korporasi (seperti dalam undang-undang pencucian uang dan korupsi), belum diatur ketentuan mengenai aturan pidana pengganti denda bagi korporasi apabila denda tidak dibayar;
- d. Didalam undang-undang yang berisi ancaman pidana minimal khusus, belum ada ketentuan mengenai pedoman atau aturan penerapan pidana minimal khusus;
- e. Pengakuan yuridis terhadap *electronic record* sebagai alat bukti hanya ada pada Undangundang Korupsi (UU No. 31 Tahun 1999 jo. UU No. 20 Tahun 2001, UU No. 30 Tahun 2002 tentang Pemberantasan Tindak Pidana Korupsi); dan Undang-Undang Tindak Pidana Pencucian Uang (UU No. 15 Tahun 2002), sehingga menjadi masalah apabila akan diterapkan untuk tindak pidana lainnya khususnya yang berkaitan dengan *cybercrime*.

Masih terbatasnya undang-undang yang ada khususnya yang mengatur *cybercrime*, berarti asas legalitas konvensional saat ini menghadapi tantangan serius dari perkembangan *cybercrime*. Hal ini dapat dimaklumi karena:

- a. Perangkat hukum yang belum memadai

Para penyidik (khususnya Polri) melakukan analogi atau perumpamaan dan persamaan terhadap pasal-pasal yang ada dalam KUHP sependapat bahwa perlu dibuat undang-undang yang khusus mengatur *cybercrime*.
- b. Kemampuan penyidik

Secara umum penyidik Polri masih sangat minim dalam penguasaan operasional komputer dan pemahaman terhadap hacking komputer serta kemampuan

melakukan penyidikan terhadap kasus-kasus itu. Beberapa faktor yang sangat berpengaruh (determinan) adalah:

- 1) Kurangnya pengetahuan tentang komputer.
- 2) Pengetahuan teknis dan pengalaman para penyidik dalam menangani kasus-kasus *Cybercrime* masih terbatas.
- 3) Faktor sistem pembuktian yang menyulitkan para penyidik.

c. Alat Bukti

Persoalan alat bukti yang dihadapi di dalam penyidikan terhadap *cybercrime* antara lain berkaitan dengan karakteristik kejahatan *cybercrime* itu sendiri, yaitu ; sasaran atau media *cybercrime* adalah data dan atau sistem komputer atau sistem internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelakunya, *cybercrime* seringkali dilakukan hampir-hampir tanpa saksi, di sisi lain, saksi korban seringkali berada jauh di luar negeri sehingga menyulitkan penyidik melakukan pemeriksaan saksi dan pemberkasan hasil penyidikan.

d. Fasilitas komputer forensic

Untuk membuktikan jejak-jejak para *hacker*, dan *cracker* dalam melakukan aksinya terutama yang berhubungan dengan program-program dan data-data komputer, sarana Polri belum memadai karena belum ada komputer forensic. Fasilitas ini diperlukan untuk mengungkap data-data digital serta merekam dan menyimpan bukti-bukti berupa *soft copy* (image, program, dsb). Dalam hal ini Polri masih belum mempunyai fasilitas forensic computing yang memadai. Fasilitas *forensic computing* yang akan didirikan Polri diharapkan akan dapat

melayani tiga hal penting yaitu *evidence collection, forensic analysis, expert witness*.⁵¹

Pertanggungjawaban pidana pelaku *cybercrime* juga perlu mengandung makna pencelaan subjektif. Masudnya secara subjektif si pelaku patut dicela atau dipersalahkan atau dipertanggungjawabkan bagi tindak pidana yang dilakukannya sehingga ia layak dipidana. Secara singkat sering dinyatakan, tiada pidana (pertanggungjawaban pidana) tanpa kesalahan (asas culpabilitas). Asas culpabilitas ini juga tentunya harus diperhatikan dalam masalah pertanggungjawaban pidana *cybercrime*. Walaupun mungkin menghadapi tantangan sendiri dalam kasus-kasus *cybercrime* karena tidak mudah membuktikan adanya unsur kesalahan (dolus/culpa) dalam masalah *cybercrime*.

C. Yurisdiksi dalam Tindak Pidana *Cybercrime*

Yurisdiksi adalah refleksi dari kedaulatan suatu negara, yang dilaksanakan dalam batas-batas wilayahnya.⁵² Secara etimologis yurisdiksi berasal dari bahasa latin yaitu *yurisdictio* yang terdiri dari 2 (dua) suku kata, *yuris* yang berarti kepunyaan menurut hukum, dan *dictio* yang berarti, ucapan, sabda, perkataan. Sisi lain dari persyaratan objektif untuk pertanggungjawaban *cybercrime* adalah masalah yurisdiksi, khususnya yang berkaitan dengan masalah ruang berlakunya hukum pidana menurut tempat. Didalam format hukum pidana yang sekarang berlaku, hukum pidana pada dasarnya hanya berlaku di wilayah negaranya sendiri (asas teritorial), dan bagi warga negaranya sendiri (asas personal/nasional aktif). Hanya

⁵¹ Dista Amalia Arifah, KASUS *CYBERCRIME* DI INDONESIA Indonesia's *Cybercrime Case*, Jurnal Bisnis dan Ekonomi, Vol.18 No.2, hlm.193

⁵² Sigid Suseno, *Yurisdiksi Tindak Pidana Siber*, Refika Aditama, Bandung, 2012, hlm.54.

saja untuk tindak pidana tertentu bisa digunakan asas universalitas dan asas nasional pasif.

1. Prinsip Universal (*The Universality Principle*)

Prinsip universal adalah prinsip yang digunakan dalam melaksanakan yurisdiksi negara dengan berdasar pada tindak pidana yang membahayakan nilai-nilai universal dan kepentingan umat manusia atau menyerang masyarakat internasional secara keseluruhan. Prinsip ini pelaksanaan yurisdiksi negara tidak didasarkan pada adanya hubungan antara negara dengan tindak pidana tersebut, sebagaimana prinsip teritorial (berdasarkan tempat tindak pidana dilakukan), prinsip nasional aktif (berdasarkan kewarganegaraan pelaku tindak pidana), prinsip nasional pasif (berdasarkan kewarganegaraan korban), dan prinsip perlindungan (berdasarkan kepentingan negara yang bersifat vital). Berdasarkan *the princeton principle on universal jurisdiction*, yurisdiksi universal adalah yurisdiksi kriminal yang hanya didasarkan pada sifat kejahatan tanpa tempat kejahatan dilakukan, kebangsaan dari pelaku kejahatan, kebangsaan korban kejahatan dan keterkaitan lain dengan negara yang melaksanakan yurisdiksi. Kejahatan yang termasuk ke dalam yurisdiksi universal adalah kejahatan berat berdasarkan hukum internasional.

2. Prinsip Nasional Aktif (*The Active Nationality Principle*)

Prinsip nasional aktif adalah prinsip yang digunakan dalam pelaksanaan yurisdiksi negara dengan berdasarkan pada nasionalitas atau kewarganegaraan. Prinsip nasional aktif terdapat dalam Pasal 5 KUHP, berdasarkan prinsip ini negara mempunyai yurisdiksi terhadap warga negaranya yang melakukan tindak pidana di dalam yurisdiksi negara lain. Prinsip ini menunjukkan adanya ikatan nasionalitas atau warga negara dengan negaranya, Untuk prinsip ini Malcom

N.Shaw menggunakan istilah *the nationality principle*, sementara Starke memasukan prinsip nasional aktif ini kedalam yurisdiksi terhadap individu.

3. Prinsip Nasional Pasif (*The Passive Nationality Principle*)

Prinsip nasional pasif adalah prinsip yang didasarkan pada nasionalitas atau kewarganegaraan, dalam hal ini kewarganegaraan korban tindak pidana. Istilah *the passive personality principle* yang digunakan oleh Malcolm N.Shaw.⁵³ Berdasarkan prinsip ini suatu negara memiliki yurisdiksi untuk mengadili pelaku tindak pidana di luar negeri yang menimbulkan kerugian kepada warga negaranya, dasar pembenaran prinsip nasional pasif ini adalah bahwa setiap negara berhak untuk melindungi warga negaranya di luar negeri apabila negara teritorial dimana tindak pidana dilakukan tidak mengadili pelaku tindak pidana tersebut. Negara asal korban memiliki kewenangan untuk mengadili pelaku tindak pidana tersebut bila orang tersebut berada di wilayahnya.

Terkait masalah yurisdiksi di ruang maya (*cyber space*), Masaki Hamano mengungkapkan terlebih dahulu adanya yurisdiksi yang dilandaskan pada prinsip-prinsip tradisional. Menurutnya ada tiga kategori yurisdiksi tradisional, yaitu yurisdiksi legislatif (*legislative jurisdiction* atau *jurisdiction to prescribe*); yurisdiksi yudisial (*judicial jurisdiction* atau *jurisdiction to adjudicate*); dan yurisdiksi eksekutif (*executive jurisdiction* atau *jurisdiction to enforce*).⁵⁴ Berdasar pada pengertian ketiga yurisdiksi di atas, maka bisa disimpulkan bahwa yurisdiksi tradisional berkaitan dengan batas-batas kewenangan negara dalam tiga bidang penegakan hukum. Pertama, wewenangan dalam membuat hukum substantif; kedua, wewenangan

⁵³ Sigid Suseno. Ibid. hlm.62-63

⁵⁴ Yuliana Surya Galih, Yurisdiksi Hukum Pidana dalam Dunia Maya, Jurnal Ilmiah Galuh Justisi, No.1 Maret 2019,hal 67-68.

mengadili atau menerapkan hukum; ketiga, wewenang melaksanakan atau memaksakan kepatuhan terhadap hukum yang dibuatnya.

Masaki Hamano membedakan pengertian *cyber jurisdiction* dari kacamata dunia virtual atau *cyber* dan dari kacamata hukum. Dari kacamata dunia virtual, *cyber jurisdiction* kerap diartikan selaku kekuasaan sistem operator dan para pengguna (users) dalam melaksanakan aturan dan menerapkannya pada suatu masyarakat di ruang *cyber/virtual*. Dari kacamata hukum, *jurisdiction on cyber space* atau *cyber jurisdiction* ialah kekuasaan fisik pemerintah dan kewenangan pengadilan kepada pengguna internet atau terhadap aktivitas mereka di ruang *cyber*⁵⁵. Berhubungan dengan *cyber jurisdiction* ini, Undang-Undang Nomor 11 Tahun 2008 Tentang Transaksi dan Informasi Elektronik, Pasal 2 menerangkan bahwa undang-undang ini berlaku bagi setiap orang yang melakukan perbuatan hukum sebagaimana diatur didalam undang-undang ini, baik yang berada diluar wilayah hukum Indonesia maupun didalam wilayah hukum Indonesia, yang mempunyai akibat hukum diluar wilayah hukum Indonesia dan/atau didalam wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

Penjelasan Pasal 2 UU-ITE memaparkan bahwa undang-undang ini mempunyai jangkauan yurisdiksi bukan semata-mata untuk perbuatan hukum yang berjalan di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik bagi warga negara Indonesia ataupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang mempunyai akibat hukum di Indonesia, mengingat dalam pemanfaatan teknologi informasi bagi informasi

⁵⁵ Ibid, hal 68.

elektronik dan transaksi elektronik bisa bersifat universal atau lintas territorial. Sedangkan yang dimaksud atas “merugikan kepentingan Indonesia” ialah meliputi akan tapi tidak terbatas pada merugikan perlindungan data strategis, martabat dan harkat bangsa, keamanan dan pertahanan negara, kepentingan ekonomi nasional, kedaulatan negara dan warga negara, serta badan hukum Indonesia.

D. Penyidikan dalam Tindak Pidana *Cybercrime*

Peran utama Penyidik adalah melakukan penyidikan, yaitu “ serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya”⁷ (Pasal 1 angka 2 KUHAP). Jadi, peran utama Penyidik yaitu mencari serta mengumpulkan bukti yang dengan bukti itu: 1) membuat terang tentang tindak pidana yang terjadi, dan 2) guna menemukan tersangkanya. Pasal 42 UU ITE menyatakan penyidikan terhadap tindak pidana sebagaimana dimaksud dalam undang-undang ini, dilakukan berdasarkan ketentuan dalam hukum acara pidana dan ketentuan dalam undang-undang ini. Dalam hal ini berarti segenap ketentuan dalam undang-undang dan KUHAP yang berhubungan bersama hukum acara pidana, berlaku didalam rencana penyidikan didalam usaha mengungkap tindak pidana yang berlangsung dalam dunia *cyber*.⁵⁶

Selain penyidik pejabat Polisi Negara Republik Indonesia (Polri), Pejabat Pegawai Negeri Sipil tertentu di lingkungan pemerintah yang lingkup tugas dan tanggung jawabnya di bidang teknologi informasi dan transaksi elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam undang-undang

⁵⁶ Hedriyanto kusno yacob, Peranan penyidik dalam Tindak Pidana Cybercrime, Jurnal Ilmiah, No.6 Agustus 2017,hal 128.

hukum acara pidana untuk melakukan penyidikan tindak pidana di bidang teknologi informasi dan transaksi elektronik. Penyidik Pegawai Negeri Sipil, berwenang⁵⁷:

1. Menerima laporan atau pengaduan;
2. Mengundang setiap orang atau pihak yang lain untuk didengar dan/atau diperiksa selaku tersangka atau saksi berhubungan dengan adanya dugaan tindak pidana;
3. Melakukan pemeriksaan atas benarnya keterangan atau laporan;
4. Melakukan pemeriksaan terhadap orang dan/atau badan usaha yang patut diduga melakukan tindak pidana;
5. Melakukan pemeriksaan berdasarkan alat dan/atau sarana yang bersangkutan dengan aktivitas teknologi informasi yang diduga digunakan untuk melakukan tindak pidana;
6. Melakukan penggeledahan terhadap tempat tertentu;
7. Melakukan penyegelan dan penyitaan;
8. Meminta bantuan ahli guna kepentingan penyidikan;
9. Mengadakan penghentian penyidikan.

Undang-Undang Informatika dan Transaksi Elektronik mengatur bahwa tindakan penyidikan tindak pidana di bidang teknologi informasi dan transaksi elektronik, harus dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran pelayanan publik (masyarakat), keutuhan data, atau integritas data selaras dengan ketentuan peraturan perundang-undangan.

Penggeledahan dan/atau penyitaan kepada sistem elektronik yang terjerat dengan dugaan tindak pidana harus dilakukan berdasar izin Ketua Pengadilan Negeri setempat. Di dalam melaksanakan penggeledahan dan/atau penyitaan, penyidik harus menjaga terpeliharanya kepentingan pelayanan umum. Di dalam melakukan

⁵⁷ Aziz Syamsuddin, Tindak Pidana Khusus, Sinar Grafika, Jakarta, 2011, hal. 12

penangkapan dan penahanan, penyidik melewati penuntut umum mempunyai kewajiban meminta penetapan Ketua Pengadilan Negeri setempat dalam waktu satu kali dua puluh empat jam. Demi mengungkap tindak pidana transaksi elektronik dan informasi elektronik, penyidik bisa bekerja sama dengan penyidik negara lain dalam hal berbagi informasi dan alat bukti.

Alat bukti penyidikan, penuntutan, dan pemeriksaan di sidang pengadilan ialah:

1. Alat bukti sebagaimana dimaksud dalam ketentuan perundang-undangan,
2. Alat bukti berupa informasi elektronik dan/atau dokumen elektronik.

Alat bukti berupa informasi elektronik dan/atau dokumen elektronik dalam rangka penyidikan, penuntutan, dan pemeriksaan persidangan tindak pidana *cybercrime* dalam UU-ITE, adalah sekumpulan data elektronik, termasuk tetapi tidak terbatas pada suara, gambar, tulisan, rancangan, peta, foto, electronic data interchange (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy atau yang sejenisnya, huruf, angka, tanda, simbol, kode simbol atau perforasi yang sudah diolah yang mempunyai arti atau dapat dipahami bagi orang yang mampu memahaminya.

Dokumen Elektronik ialah setiap informasi elektronik yang dibuat, dikirimkan, diteruskan, diterima, atau disimpan dalam wujud digital, analog, elektromagnetik, optikal, atau yang sejenisnya, yang dapat ditampilkan, dilihat, dan/atau didengar menggunakan komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada suara, tulisan, gambar, rancangan, peta, foto atau yang sejenisnya, huruf, angka, tanda, kode akses, simbol atau perforasi yang mempunyai makna atau arti atau bisa dipahami oleh orang yang mampu memahaminya. Dokumen Elektronik dan/atau Informasi Elektronik dan/atau

hasil cetaknya ialah alat bukti hukum yang sah. Merupakan perluasan dari alat bukti yang sah dan sesuai dengan hukum acara yang berlaku di Indonesia, yang dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang ada dalam undang-undang ini.

Sebagaimana termaksud di dalam Pasal 5 ayat 4 UU ITE, yang menentukan bahwa ada beberapa jenis dokumen elektronik yang tidak dapat dijadikan alat bukti yang sah apabila terkait dengan pembuatan: Surat yang menurut undang-undang harus dibuat dalam bentuk tertulis; dan Surat beserta dokumennya yang menurut undang-undang harus dibuat dalam suatu bentuk akta notariil atau akta yang dibuat oleh pejabat pembuat akta.⁵⁸

⁵⁸ Johan Wahyudi, Dokumen elektronik sebagai alat bukti pada pembuktian di pengadilan, Jurnal Fakultas Hukum Universitas Airlangga Surabaya, No.2 Maret 2012, hal 123.

BAB III

PROSEDUR PENANGANAN TINDAK PIDANA CYBER CRIME DI DITRESKRIMSUS POLDA JATENG

A. Gambaran Umum Ditreskrimsus Polda Jawa Tengah Unit *Cybercrime*⁵⁹

1. Wilayah Hukum Ditreskrimsus Polda Jateng.

Direktorat Reserse Kriminal Khusus Polisi daerah Jawa tengah tercatat masuk dalam wilayah hukum Kepolisian Daerah Jawa Tengah, yang beralamat di Jalan Sukun Raya Nomor 46, Kelurahan Srandol Wetan, Kecamatan Banyumanik, Kota Semarang, Provinsi Jawa Tengah 50263.

2. Visi dan Misi Ditreskrimsus Khusus Polda Jateng.

Kepolisian Negara Republik Indonesia khususnya Ditreskrimsus Polda Jateng mempunyai visi dan misi untuk menjalankan fungsi dan tugasnya. Visi Ditreskrimsus Polisi daerah Jawa tengah ialah: “Mewujudnya Direktorat Kriminal Khusus Kepolisian Polda Jawa Tengah yang modern, profesional dan terpercaya”.⁶⁰

Misi Ditreskrimsus Polda Jawa tengah yaitu :

- a. Menghasilkan postur Polri Ditreskrimsus Polda Jawa tengah yang efektif, ideal dan efisien;
- b. Meningkatkan kualitas sumber daya manusia (SDM) Ditreskrimsus Polda Jawa tengah dalam penanganan tindak pidana khusus;
- c. Mewujudkan penegakan hukum yang adil dan menjamin kepastian hukum serta menjunjung tinggi hak asasi manusia;

⁵⁹ R. Haryo Seto I, *Wawancara*, Semarang, 16 November 2020

⁶⁰ R. Haryo Seto I, *Wawancara*, Semarang, 16 November 2020

- d. Meningkatkan pengawasan penyidikan tindak pidana khusus dalam rangka mewujudkan Polri yang akuntabel dan profesional;
- e. Menjalankan teknologi Kepolisian dan sistem informasi sebagai berkelanjutan yang berintegritas dalam mendukung kinerja Penyidik Ditreskrimsus yang optimal;
- f. Menciptakan sistem sinergi polisional bersama instansi terkait maupun komponen masyarakat dalam rangka membangun kemitraan dalam penanganan tindak pidana khusus.⁶¹

3. Fungsi Ditreskrimsus Polda Jateng.

Sesuai yang sudah tertuang dalam Pasal 139 ayat (2) Peraturan Kepala Kepolisian (Perkap) Nomor 22 Tahun 2010 tentang Susunan Organisasi dan Tata Kerja di Tingkat Kepolisian Daerah, antara lain:

- a. Penyidikan dan penyelidikan tindak pidana khusus, antara lain tindak pidana korupsi, ekonomi, dan tindak pidana tertentu di wilayah hukum Polda;
- b. Penanganan kasus beserta analisisnya, serta mempelajari dan mengkaji efektifitas pelaksanaan tugas Ditreskrimsus Polda.
- c. Pembinaan teknis, koordinasi, dan dalam mengawasi operasional, serta administratif penyidikan oleh PPNS;
- d. melaksanakan pengawasan penyidikan tindak pidana khusus di wilayah Polda; dan
- e. Pengolahan dan pengumpulan data beserta menyajikan informasi dan dokumentasi program kegiatan Ditreskrimsus.⁶²

⁶¹ Sumber: <http://reskrimsus.jateng.polri.go.id/?halaman=7>

⁶² Sumber: <http://reskrimsus.jateng.polri.go.id/?halaman=6>

4. Tugas Ditreskrimsus Polda Jawa Tengah

Ditreskrimsus Polda Jateng mempunyai tugas untuk menyelenggarakan penyidikan dan penyelidikan pada tindak pidana khusus, koordinasi, pengawasan operasional, dan administrasi penyidikan PPNS sesuai dengan ketentuan yang ada pada peraturan perundang-undangan.

B. Prosedur Penanganan Tindak Pidana *Cyber Crime* Di Ditreskrimsus Polda Jateng

Prosedur penanganan tindak pidana *cyber crime* ini tidak sesederhana semacam yang kita tahu spesialnya dalam proses penegakan hukumnya, mulai dari undang-undang yang mengendalikan menimpa kejahatan *cybercrime*, sampai Majelis hukum Negara mana yang berwenang buat mengadili masalah tersebut. Tindak pidana *cyber crime* tidak hanya diatur dalam KUHP, serta undang- undang no 19 tahun 2016 tentang pergantian undang- undang no 11 tahun 2008 Tentang Data Serta Transaksi Elektronik, sebagian pasal di KUH Perdata pula mengendalikan spesialnya menimpa perbuatan melawan hukum semacam“ penghinaan”/ pencemaran nama baik, meski dalam perihal ini penulis tidak hendak membahas proses hukum secara perdata tetapi penulis cuma mau menarangkan menimpa seberapa luas ruang lingkup tindak pidana *cyber crime* ini serta gimana mekanisme yang dicoba oleh penegak hukum (penyidik) dalam penindakan kejahatan *cyber crime* tersebut serta apa saja hambatan yang dialami oleh Penyidik dalam penanggulangan kejahatan *cyber crime*⁶³.

⁶³ R. Haryo Seto L, Wawancara, Semarang, 11 November 2020

Ditinjau dari perspektif hukum pidana, upaya penanggulangan *cyber crime* bisa dilihat dari bermacam aspek, ialah antara lain dari aspek kebijakan kriminalisasi (perumusan tindak pidana), aspek pertanggungjawaban pidana ataupun pemidanaan (tercantum aspek perlengkapan fakta/ pembuktian), serta aspek yurisdiksi yang mana perihal tersebut bisa menolong dalam perihal penanggulangan *cybercrime*. Kegiatan siber tidak lagi simpel, sebab kegiatannya ini tidak lagi dibatasi oleh teritorial sesuatu negeri, yang gampang diakses kapanpun, serta dimanapun. Kerugian bisa terjalin, baik pada pelaku transaksi, ataupun pada orang lain yang tidak melaksanakan transaksi di internet. Pembuktian ialah perihal yang sangat berarti, mengingat data elektronik belum terakomodasi dalam sistem hukum kegiatan di Indonesia secara komprehensif, serta nyatanya pula sangat rentan buat diganti, disadap, dipalsukan, serta dikirim ke bermacam penjuru dunia dalam waktu yang sangat pendek, dengan demikian dampak yang diakibatkannya dapat sangat kompleks serta rumit⁶⁴.

Pada metode penyidikan, tim penyidik *cyber crime* Ditreskrimsus Polda Jateng melakukan tugasnya untuk bisa mengungkapkan perkara pidana melalui proses dan langkah sebagai berikut:⁶⁵

1. Penyelidikan

Penyelidikan adalah serangkaian aktivitas penyidik dalam mencari dan menemukan suatu peristiwa yang diduga menjadi tindak pidana guna menentukan bisa atau tidaknya dilakukan penyidikan berdasarkan cara yang diatur dalam undang-undang ini⁶⁶

⁶⁴ R. Haryo Seto L, Wawancara, Semarang, 11 November 2020

⁶⁵ Pasal 24 Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 14 Tahun 2012 tentang Manajemen Penyidikan Tindak Pidana

⁶⁶ Pasal 1 Ayat 5 KUHAP

Berdasarkan Pasal 24 Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 14 Tahun 2012 tentang Manajemen Penyidikan Tindak Pidana, terdapat beberapa tahap penyelidikan agar dapat menentukan suatu peristiwa dapat dikatakan sebagai suatu tindak pidana, yaitu sebagai berikut:

a) Pengolahan TKP :

- 1) Mencari dan mengumpulkan keterangan, barang bukti, petunjuk, identitas para tersangka, dan korban/saksi untuk kepentingan penyelidikan selanjutnya;
- 2) Mencari hubungannya diantara korban/saksi, tersangka atau barang bukti; dan
- 3) Mendapatkan gambaran modus operandi tindak pidana yang berjalan;

b) Pemantauan (*Observasi*) :

- 1) Memperoleh kejelasan maupun melengkapi informasi yang telah ada berdasarkan pengetahuan dan gagasan yang diketahui;
- 2) Melakukan pengawasan terhadap tempat, objek, dan lingkungan tertentu buat memperoleh informasi-informasi yang dibutuhkan; dan sebelumnya;

c) Wawancara (*interview*) :

- 1) Memperoleh informasi dari pihak-pihak tertentu dengan teknik
- 2) wawancara secara terbuka maupun tertutup; dan Memperoleh kejelasan tindak pidana yang terjadi lewat cara mencari jawaban atas pertanyaan apa, siapa, dimana, mengapa, dengan apa, bilamana, bagaimana;

d) Pembuntutan (*Surveillance*) :

- 1) Membuntuti seseorang yang diduga menjadi pelaku tindak pidana ataupun orang lain yang sanggup mengarahkan kepada pelaku tindak pidana;
 - 2) Mencari tahu kebiasaan, lingkungan, aktivitas atau jaringan pelaku tindak pidana; dan
 - 3) Memburu distribusi barang ataupun tempat penyimpanan barang hasil kejahatan;
- e) Penulusuran (*Tracking*) :
- 1) Mengikuti dan mencari keberadaan pelaku tindak pidana dengan menggunakan teknologi informasi;
 - 2) Menjalankan pelacakan lewat kerja sama dengan Interpol, kementerian/badan/komisi/lembaga/instansi terkait; dan
 - 3) Melakukan penyelidikan aliran dana yang diduga dari hasil kejahatan;
- f) Penyamaran (*Uundercover*) :
- 1) Bergabung bersama kelompok tertentu untuk mendapatkan peran dari kelompok tersebut, untuk mengetahui kegiatan para pelaku tindak pidana;
 - 2) Menyusup ke dalam daerah tertentu tanpa diketahui identitasnya untuk mendapatkan bahan informasi atau keterangan; dan
 - 3) Khusus kasus peredaran narkoba, bias menggunakan teknik penyamaran sebagai calon pembeli (*undercover buy*), penyamaran untuk bisa melibatkan diri dalam distribusi narkoba sampai tempat tertentu (*controlled delivery*), penyamaran disertai penindakan/pemberantasan (*raid planning execution*);

g) Analisis dan Observasi Dokumen, yang Dilakukan terhadap Kasus-Kasus Tertentu dengan Cara:

- 1) Mengkompulir dokumen adanya kaitan yang diduga dengan tindak pidana; dan
- 2) Menganalisis dan meneliti dokumen yang didapat guna menyusun anatomi perkara tindak pidana serta modus operandinya

h) Penjabaran Bidang Tugas Subdit pada Ditreskrimsus Polda Jawa Tengah (Dasar Surat Telegram Kabareskrim Polri Nomor ST: 143/VII/2011 tanggal 4 Juli 2011): SUBDIT V/ SIBER:

- 1) Penyidikan kasus-kasus yang berhubungan pada transaksi elektronik;
- 2) Penyidikan kasus-kasus yang berhubungan pada tindak pidana pornografi online/kejahatan dunia maya (*cybercrime*).

Prosedur penanganan problematika penumpukan *cybercrime* di polda jateng, telah dilakukan oleh tim penyidik, akan tetapi masih terjadi penumpukan perkara.

Berikut ini data kasus yang belum terselesaikan di sepanjang tahun 2020:

Tabel 4.1
Penumpukan Perkara Tahun 2019

No.	Tanggal Laporan	Perkara	Tahapan Laporan	Penyidik
1	Februari 2019	Pasal 45 ayat (1) jo Pasal 27 ayat (1) UU RI No. 19 Tahun 2016 tentang Perubahan Atas UU RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik	SP2HP Henti Lidik (11-02-2019)	Unit 1 Dading
2	Februari 2019	Pasal 45A ayat (1) jo Pasal 28 ayat (1) UU RI No. 19 Tahun 2016 tentang Perubahan Atas UU RI No. 11 Tahun 2008 tentang Informasi dan Transaksi	Tahap Limpah (13-02-2019)	Unit 3 Fradinta

		Elektronik		
3	Februari 2019	Pasal 45 ayat (3) jo Pasal 27 ayat (3) UU RI No. 19 Tahun 2016 tentang Perubahan Atas UU RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik	Tahap SP2HP Henti Lidik (18-02-2019)	Unit 2
4	Februari 2019	Pasal 45 ayat (1) jo Pasal 27 ayat (1) UU RI No. 19 Tahun 2016 tentang Perubahan Atas UU RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik	Tahap II (25-02-2019)	Unit 2
5	Maret 2019	Pasal 45 ayat (3) jo Pasal 27 ayat (3) UU RI No. 19 Tahun 2016 tentang Perubahan Atas UU RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik	Tahap SP2HP Henti Lidik (08-03-2019)	Unit 2
6	April 2019	Pasal 45 ayat (3) jo Pasal 27 ayat (3) UU RI No. 19 Tahun 2016 ttg Perubahan Atas UU RI No. 11 Tahun 2008 ttg Informasi dan Transaksi Elektronik	Tahap SP3	Unit 2
7	Mei 2019	Pasal 45A ayat (3) jo Pasal 27 ayat (3) UU RI No. 19 Tahun 2016 tentang Perubahan Atas UU RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik	Tahap II	Unit 1
8	Mei 2019	Pasal 45A ayat (2) jo Pasal 28 ayat (2) UU RI No. 19 Tahun 2016 ttg Perubahan Atas UU RI No. 11 Tahun 2008 ttg Informasi dan Transaksi Elektronik	Tahap SP3 (24-5-2019)	Unit 2
9	Juli 2019	Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan dan atau setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat	Tahap II (1-07-2019)	Unit 2 VICO

		<p>diaksesnya Informasi dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan atau pengancaman.</p> <p>Pasal 45 ayat (1) dan (4) Jo Pasal 27 ayat (1) dan (4) dengan ketentuan pidana diatur dalam UU RI No. 11 Tahun 2008 berikut perubahannya pada UU RI No. 19 Tahun 2016 ttg Informasi dan Transaksi Elektronik.</p>		
10	Juli 2019	<p>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).</p> <p>Pasal 45 A ayat 2 juncto pasal 28 ayat 2 UU RI Nomor 19 tahun 2016 tentang perubahan atas UURI Nomor 11 tahun 2008 tentang informasi dan Transaksi Elektronik</p>	Tahap II (05-07-2019)	Uni 2 Dwi S
11	Juli 2019	<p>Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik</p> <p>Pasal 45 ayat (3) jo Pasal 27 ayat (3) UU RI No. 19 Tahun 2016 ttg Perubahan Atas UU RI No. 11 Tahun 2008 ttg Informasi dan Transaksi Elektronik</p>	Tahap SP3 (09-07-2019)	Unit 1
12	Juli 2019	<p>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</p> <p>Pasal 45 ayat (2) jo Pasal 27</p>	Tahap II (18-07-2019)	Unit I

		ayat (2) UU RI No. 19 Tahun 2016 ttg Perubahan Atas UU RI No. 11 Tahun 2008 ttg Informasi dan Transaksi Elektronik		
13	Juli 2019	Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan dan atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan pemerasan dan/atau pengancaman Pasal 45 ayat (1) jo Pasal 27 ayat (1) UU RI No. 19 Tahun 2016 ttg Perubahan Atas UU RI No. 11 Tahun 2008 ttg Informasi dan Transaksi Elektronik	Tahap II (30-07-2019)	Unit 1
14	Agustus 2019	Pasal 45 ayat (1) UU RI No. 19 Tahun 2016 tentang Perubahan Atas UU RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan atau pasal 30 UU RI No. 44 tahun 2008 ttg Pornografi	Tahap II (14-08-2019)	Unit 2
15	September 2019	Pasal 45 ayat (1) Jo pasal 27 ayat (1) UU RI No. 19 Tahun 2016 tentang Perubahan Atas UU RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan atau pasal 29 Jo pasal 4 ayat (1) UU RI No. 44 Tahun 2008 ttg Pornografi	Tahap II (18-09-2019)	Unit 1
16	September 2019	Pasal 45 ayat (1) UU RI No. 19 Tahun 2016 tentang Perubahan Atas UU RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan atau pasal 327 atau pasal 378 KUHPidana	Tahap II (26-09-2019)	Unit 2
17	September 2019	Setiap orang dengan sengaja dan tanpa hak mendistribusikan	Tahap II P-21 (28-06-2019)	Unit 1 Dading

		dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik. Pasal 27 ayat (3) dengan ketentuan pidana diatur dalam pasal 45 ayat 3 UU RI No. 11 Tahun 2008 berikut perubahannya pada UU RI No. 19 Tahun 2016 ttg Informasi dan Transaksi Elektronik	SP3 (30-09-2019)	
18	September 2019	Pasal 45 ayat (3) UU RI No. 19 Tahun 2016 tentang Perubahan Atas UU RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik	SP3 (30-09-2019)	Unit 1 Febri
19	November 2019	Pasal 45 ayat (1) jo Pasal 45B UU RI No. 19 Tahun 2016 ttg Perubahan Atas UU RI No. 11 Tahun 2008 ttg Informasi dan Transaksi Elektronik	Tahap II (11-11-2019)	Unit 2
20	Desember	Pasal 45 ayat (1) jo Pasal 27 ayat (1) UU RI No. 19 Tahun 2016 ttg Perubahan Atas UU RI No. 11 Tahun 2008 ttg Informasi dan Transaksi Elektronik	Tahap II (13-12-2019)	Unit 2 Bagus
21	Desember	Pasal 45 ayat (3) UU RI No. 19 Tahun 2016 tentang Perubahan Atas UU RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik	SP3 (09-12-2019)	Unit I Satria

Sumber: Data Saikara Ditreskrimsus Polda Jateng 2019

Berdasarkan tabel 4.1 menunjukkan bahwa jumlah penumpukan kasus sebanyak 21 kasus *Cybercrime*. Dari 21 kasus, jumlah kasus tertinggi pada penyidikan Tahap II yaitu sebanyak 11 kasus atau 52,38%.

Tabel 4.2.**Deskriptif Data Penumpukan Perkara Tahun 2019**

No	Jenis penyidikan	Jumlah Laporan	Persentase
1	Tahap II	11	52,38%
2	SP3	6	28,57%
3	Limpah	1	4,76%
4	Henti Lidik	3	14,28%
Jumlah		21	100%

Sumber: Data Saikara Ditreskrimsus Polda Jateng 2019

Berdasarkan tabel 4.2 menunjukkan bahwa jumlah penumpukan kasus sebanyak 21 kasus *Cybercrime*. Dari 21 kasus, jumlah kasus tertinggi pada penyidikan Tahap II yaitu sebanyak 11 kasus atau 52,38%.

Tabel 4.3**Penumpukan Perkara Tahun 2020**

NO	UNIT	LAPORAN POLISI TANGGAL	KASUS	PASAL	KET
1	UNIT 1		Barang Siapa memperdagangkan, membuat, merakit, memasukan atau menggunakan pekarangkat telekomunikasi di wilayah Republik Indonesia yang tidak sesuai dengan persyaratan teknis	Pasal 52 UU RI No 36 tahun 1999 tentang Telekomunikasi	P21, tanggal 10 Des 2019 Nomor : B-4583/ M.3.4/Eku.1/12/2019 TAHAP II, tanggal 6 Januari 2020 Nomor : B/180/I/RES. 2.5./2020/Reskrimsus
2	UNIT 1		Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Infoemasi	Pasal 27 sampai dengan pasal 33 sebagaimana dimaksud dalam pasal 45 ayat 1 pasal 45	P21, tanggal 16 Des 2019 Nomor : B-4656/ M.3.4/Eku.1/12/2019

NO	UNIT	LAPORAN POLISI TANGGAL	KASUS	PASAL	KET
			Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan atau 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 atau setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki perangkat keras atau perangkat lunak Komputer yang diranvang atau secara khusus dikembangkan untuk memfasilitasi perbuatan	ayat 2 pasal 50 Undang-undang Republik Indonesia Nomor 19 Tahun 2016 tentang perubahan Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik	TAHAP II, tanggal 6 Januari 2020 Nomor : B/181/I/RES. 2.5./2020/Reskrimsus
3	UNIT 2		Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras dan antar	Pasal 45A ayat (2) jo Pasal 28 ayat (2) UU RI No. 19 Tahun 2016 tentang perubahan atas UU RI No. 11 Tahun 2008 tentang ITE	P-21, tanggal 11 Feb 2020 Nomor: B-725/M.3.4/Eku.1/02/2020 TAHAP II, tanggal 17 Februari 2020 Nomor :

NO	UNIT	LAPORAN POLISI TANGGAL	KASUS	PASAL	KET
			golongan (SARA)		B/1856/II/RE S.2.5./2020/R eskrimsus
4	UNIT 1		Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik	Pasal 45 ayat (3) jo Pasal 27 ayat (3) UU RI No. 19 Tahun 2016 tentang perubahan atas UU RI No. 11 Tahun 2008 tentang ITE	P-21, tanggal 18 Feb 2020 Nomor: B-844/M.3.4/Eku.1/02/2020 TAHAP II, tanggal 25 Februari 2020 Nomor : B/2170/II/RE S.2.5./2020/R eskrimsus
5	UNIT 2		Setiap orang dengan sengaja dan tanpa hak melakukan manipulasi penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik dianggap seolah olah data otentik.	Pasal 35 UU RI 19 Tahun 2016 tentang perubahan atas UU RI No. 11 Tahun 2008 ttg Informasi dan Transaksi Elektronik.	-21, tgl. 27 Februari 2020 Nomor: B-926/M.3.4/Eku.1/02/2020 TAHAP II, tanggal 27 Februari 2020 Nomor : B/2260/II/RE S.2.5./2020/R eskrimsus
6	UNIT 1 Dading Cabut		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	Pasal 45 ayat (1) jo pasal 27 (1) UU RI No 11 th 2008 jo UU No 19 th 2016 tentang ITE	SP2.lid, tanggal 28 Feb 2020 Nomor: SP2.Lid/120.a/II/2020/Reskrimsus S.Ketetapan, tanggal 28 Feb 2020

NO	UNIT	LAPORAN POLISI TANGGAL	KASUS	PASAL	KET
			kesusilaan		Nomor: S.Tap/120.b/I I/2020/Reskri msus
7	UNIT 1		Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi elektronik dan/atau dokumentasi elektronik yang memiliki muatan yang melanggar kesusilaan dan atau Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi elektronik dan/atau dokumentasi elektronik yang memiliki muatan pemerasan dan atau pengancaman	Pasal 45 ayat (1) dan/atau Pasal 45 ayat (4) UU RI No. 19 Tahun 2016 ttg Perubahan Atas UU RI No. 11 Tahun 2008 ttg Informasi dan Transaksi Elektronik	P-21, tanggal 18 Maret 2020 Nomor: B-1235/M.3.4/Eku.1/03/2020 TAHAP II, tanggal 18 Maret 2020 Nomor : B/2879/III/R ES.2.5./2020/Reskrimsus
8	UNIT 1		Setiap orang dengan sengaja dan tanpa hak menyebarkan Informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).	Pasal 28 ayat (2) UU RI No. 11 Tahun 2008 berikut perubahan UU RI No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik	P-21, tanggal 16 April 2020 Nomor: B-1542/M.3.4/Eku.1/04/2020 TAHAP II, tanggal 20 April 2020 Nomor : B/4012/IV/R ES.2.5/2020/Reskrimsus

NO	UNIT	LAPORAN POLISI TANGGAL	KASUS	PASAL	KET
9	UNIT 1		Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.	Pasal 45 ayat (3) UU RI No. 19 Tahun 2016 ttg Perubahan Atas UU RI No. 11 Tahun 2008 ttg Informasi dan Transaksi Elektronik	P-21, tanggal 20 April 2020 Nomor: B-1527/M.3.4/Eku.1/04/2020 TAHAP II, tanggal 15 Juni 2020 Nomor : B/5491/VI/RES.2.5/2020/Reskrimsus
10	UNIT 1 (Brig Dading)		Setiap orang dengan sengaja dan tanpa hak menyebarkan Informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).	Pasal 28 ayat (2) UU RI No. 11 Tahun 2008 berikut perubahan UU RI No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik	P-21, tanggal 21 April 2020 Nomor: B-1536/M.3.4/Eku.1/04/2020 TAHAP II Proses (alamat tidak jelas)
11	UNIT 2		Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan Informasi dan Transaksi Elektronik	Pasal 45 ayat 1 jo pasal 27 ayat 1 UU RI No. 11 Tahun 2008 berikut perubahan UU RI No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik	P-21, tgl. 4 Mei 2020 Nomor: B-1649/M.3.4/Eku.1/05/2020 TAHAP II, tanggal 4 Mei 2020 Nomor : B/4439/V/RES.2.5./2020/Reskrimsus

NO	UNIT	LAPORAN POLISI TANGGAL	KASUS	PASAL	KET
12	UNIT 1 Sulis		Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik	Pasal 45 ayat 3 jo pasal 27 ayat 3 UU RI No. 11 Tahun 2008 berikut perubahan UU RI No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik	SP3, tanggal 30 Juni 2020 Nomor: B/SP3/29.a/VI/RES.2.5./2020/Reskrimsus
13	UNIT 1 Yoyok		Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik	Pasal 45 ayat (3) Jo 27 ayat (3)UU Nomor 19 Tahun 2016 ttg perubahan atas UU Nomor 11 Th 2008 ttg ITE ttg tindak pidana pencemaran nama baik melalui media elektronik	SP2.lid, tanggal 29 Jul 2020 Nomor: SP2.Lid/224.a/VII/2020/R eskrimsus S.Ketetapan, tanggal 29 Jul 2020 Nomor: S.Tap/224.b/VII/2020/Res krimsus
14	UNIT 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 yang melanggar kesusilaan tentang Informasi dan Transaksi Elektronik	Pasal 45 ayat 1 jo pasal 27 ayat 1 UU RI No. 11 Tahun 2008 berikut perubahan UU RI No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik	P-21, tgl. 10 Agustus 2020 Nomor: B-2846/M.3.4/Eku.1/08/2020 TAHAP II, tanggal 12 Agustus 2020 Nomor : B/7628/VIII/RE S. 2.5./2020/Res krimsus

NO	UNIT	LAPORAN POLISI TANGGAL	KASUS	PASAL	KET
15	UNIT 3		Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman	Pasal 45 ayat 4 jo pasal 27 ayat 4 UU RI No. 11 Tahun 2008 berikut perubahan UU RI No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik	SP3, tgl. 28 September 2020 Nomor : B/SP3/63.a/IX/RES.2.5./2020/Ditreskrimsus Surat Ketetapan penghentian Penyidikan, tgl. 28 September 2020 Nomor: S.Tap/63.b/IX/2020/Reskrimsus
16	UNIT 2		Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian	Pasal 45 ayat 2 Jo Pasal 27 ayat 2 UU RI No. 11 Tahun 2008 berikut perubahan UU RI No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik	P-21, tgl. 29 September 2020 Nomor: B-3801/M.3.4/Eku.1/10/2020 TAHAP II, tanggal 5 Oktober 2020 Nomor : B/9559/X/RES.2.5./2020/Reskrimsus
17	UNIT 2		Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau	Pasal 45 ayat 1 jo pasal 27 ayat 1 UU RI No. 11 Tahun 2008	P-21, tgl. 23 Oktober 2020 Nomor: B-3836/M.3.4/

NO	UNIT	LAPORAN POLISI TANGGAL	KASUS	PASAL	KET
			mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan tentang Informasi dan Transaksi Elektronik	berikut perubahan UU RI No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik	Ekur.1/10/2020 TAHAP II, tanggal 26 Oktober 2020 Nomor : B/10337/X/RES . 2.5./2020/Res krimsus
18	UNIT 2		Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik	Pasal 27 ayat (3) dengan ketentuan pidana diatur dalam pasal 45 ayat 3 UU RI No. 11 Tahun 2008 berikut perubahannya pada UU RI No. 19 Tahun 2016 ttg Informasi dan Transaksi Elektronik	SP3, Tgl 06 Nov 2019 Nomor: B/SP3/65.A/X I/RES.2.5./2020/ Ditreskrimsus Surat Perintah Penghentian Penyidikan No.Pol.: SP.Sidik/534. A/XI/2020/Dit reskrimsus, tgl. 6 Nov 2020 Surat Ketetapan No.Pol.: S.Tap/65.B/XI /2020/Ditreskr imsus, tgl. 6 Nov 2020

Sumber: Data Saikara Ditreskrimsus Polda Jateng Tahun 2020

Pada tahun 2020 berdasarkan tabel 4.4 menunjukkan bahwa jumlah penumpukan kasus sebanyak 18 kasus *Cybercrime*.

Tabel 4.4.

Deskriptif Data Penumpukan Perkara Tahun 2020

No	Jenis penyidikan	Jumlah Laporan	Persentase
1	P. 21	15	72,22%
2	SP2. Lid	2	11,11%
3	SP1	1	5,56%
Jumlah		18	100%

Sumber: Data Saikara di Ditreskrimsus Polda Jateng Tahun 2020

Pada tahun 2020 Berdasarkan tabel 4.4 menunjukkan bahwa jumlah penumpukan kasus sebanyak 18 kasus *Cybercrime*. Dari 18 kasus, jumlah kasus tertinggi pada penyidikan P. 21 yaitu sebanyak 13 kasus atau 72,22%.⁶⁷ Dengan demikian, prosedur penanganan tindak pidana *cyber crime* di Polda Jateng adalah sebagai berikut:⁶⁸

- 1) Menerima pengaduan atau laporan dari seorang tentang adanya tindak pidana.
- 2) Mencari keterangan dan barang bukti.
- 3) Memerintah berhenti seorang yang dicurigai dan menanyakan serta memeriksa tanda pengenal diri.
- 4) Mengadakan tindakan lain menurut hukum yang bertanggung jawab. Atas perintah dari penyidik bisa melakukan tindakan berupa:
- 5) Penangkapan, larangan meninggalkan tempat, penggeledahan dan penyitaan.
- 6) Pemeriksaan dan penyitaan surat.
- 7) Mengambil sidik jari dan memotret seseorang.
- 8) Membawa dan menghadapkan seseorang pada penyidik.

⁶⁷ R. Haryo Seto I, Kanit 1 Subdit V Ditreskrimsus Polda Jateng, Wawancara, Semarang, 16 November 2020

⁶⁸ R. Haryo Seto I, Kanit 1 Subdit V Ditreskrimsus Polda Jateng, Wawancara, Semarang, 16 November 2020

C. Hambatan dan Kendala yang Dihadapi oleh Pihak Kepolisian Republik Indonesia dalam Penegakan Hukum Terhadap Tindak Pidana pada Tahap Penyidikan di Polda Jawa Tengah

Sebagaimana telah disampaikan oleh informan dalam penelitian ini, Bapak R. Haryo Seto L SH, M.Krim, divisi Siber Ditreskrimsus Polda Jateng. masalah mengenai penumpukan perkara di Ditreskrimsus Polda Jateng sulit untuk diproses maupun untuk ditegakkan, karena memerlukan waktu yang cukup lama dan sulitnya melakukan penyelidikan terhadap tindak pidana tersebut. Pihak kepolisian menyadari betapa sulitnya menjangkau pelaku yang ada.⁶⁹

Beberapa kasus yang ada atau menumpuk di Ditreskrimsus Polda Jateng, sulit di tangani disebabkan karena membutuhkan kepakaran *cyber* dan dana yang sangat besar. Banyak hambatan maupun kendala yang muncul pada saat kepolisian melakukan penegakan hukum terhadap tindak pidana secara online hukum. Hambatan dan kendala sebagai berikut yang membuat sulitnya pihak kepolisian melakukan penegakan:

1. *Ip adres public website/media sosial* pelaku tindak pidana berada di luar provinsi ataupun di luar negeri.

Kasus yang berhadapan dengan wilayah luar indonesia akan mempersulit penyelidikan apabila ada perbedaan pandangan hukum antara negara Indonesia dengan negara lain, karena kemungkinan negara di mana tempat pembuatan website/media sosial pelaku berada di wilayah yang tidak ada perjanjian diplomasi / perjanjian extradisi dengan Indonesia.

2. Rekening bank ataupun akun media sosial selalu berganti-ganti.

Rekening bank yang digunakan oleh para pelaku tindak untuk menerima transaksi tersebut selalu berganti-ganti, para pelaku ini mempunyai banyak

⁶⁹ R. Haryo Seto L, Wawancara, Semarang, 16 November 2020

rekening bank dana akun media social dengan identitas yang berbeda-beda dan bank yang berbeda-beda.

- a) Data aplikasi pembukaan rekening bank dana akun media sosialnya yang digunakan untuk melakukan tindak pidana tersebut fiktif.

Data dan identitas yang digunakan oleh pelaku untuk membuat rekening bank ataupun media social menggunakan identitas palsu, sehingga pihak kepolisian menjadi kesulitan untuk menemukan pelaku tersebut.

- b) Barang bukti mudah dirubah dan hilang.

Barang bukti ini merupakan barang bukti media Informasi dan Transaksi Elektronik dapat dengan mudah dihilangkan atau dirubah oleh pelaku tersebut, sehingga perlu kecepatan dan kehati-hatian untuk mengamankan barang bukti.

- c) Kurangnya jumlah personil di dalam menangani penanganan tindak pidana.

Melihat kasus yang belum dapat diungkap oleh pihak penyidik Unit 4 (*cybercrime*) Subdit II Ditreskrimsus Polda Jateng pada tahun 2019 dan 2020 adalah 39 kasus (perkara), padahal banyak pelaku yang tidak tertangkap bukan hanya di tahun 2019-2020 saja, akan tetapi ditahun-tahun sebelumnya. Pihak penyidik harus menangani masalah-masalah *cyber crime* ini pada seluruh wilayah hukum Polda Jawa Tengah, padahal untuk Provinsi Jawa Tengah sendiri sangatlah luas, dan berdasarkan observasi dari peneliti jumlah personil unit *cybercrime* ini masih sangat sedikit dan sangatlah kurang yaitu hanya sebanyak 14 personil sedangkan Ditreskrimsus Polda Jateng menanungi seluruh wilayah jawa tengah yaitu sebanyak 29 kabupaten dan 6 kota. Sedangkan efisiennya personil di Ditreskrimsus itu minimal

berjumlah 35 personil sesuai jumlah kabupaten/kota yang ada di Jawa Tengah. Jadi 1 personil bisa menaungi 1 kabupaten/kota.

- d) Unit yang mengatasi masalah *cybercrime* hanya ada ditingkat Polda saja.

Berdasarkan Peraturan Kapolri Nomor 22 Tahun 2010 tentang Susunan Organisasi dan Tata Kerja Pada Tingkat Kepolisian Daerah, unit yang menangani masalah *cyber* merupakan salah satu bagian dari tugas-tugas Ditreskrimsus, dan Ditreskrimsus ada di tingkat Polda saja dan merupakan salah satu unsur pelaksana tugas pokok yang berada dibawah Kapolda. Kedepannya unit yang menangani permasalahan *cyber crime* ini akan dikembangkan sampai Polres tergantung pada kemampuan keuangan negara.

Apabila dianalisis menggunakan teori *Legal System* oleh Lawrence M Friedman, struktur hukum (*structure of law*) merupakan salah satu unsur dalam sistem hukum yang melakukan penegakan hukum. Struktur hukum disebut sebagai sistem Struktural yang menentukan bisa atau tidaknya hukum itu dilaksanakan dengan baik. Struktur hukum berdasarkan UU No. 8 Tahun 1981 meliputi; mulai dari Kepolisian, Kejaksaan, Pengadilan dan Badan Pelaksana Pidana (Lapas). Kewenangan lembaga penegak hukum dijamin oleh undang-undang. Sehingga dalam melaksanakan tugas dan tanggung jawabnya terlepas dari pengaruh kekuasaan pemerintah dan pengaruh-pengaruh lain. Terdapat adagium yang menyatakan “*fiat justitia et pœreat mundus*” meskipun dunia ini runtuh hukum harus ditegakkan.⁷⁰

Struktur hukum ini berkaitan dengan aparat penegak hukum yang melakukan penyidikan terhadap tindak pidana *cybercrime*, yaitu kepolisian,

⁷⁰ Lawrence M. Friedman, Sistem Hukum Perspektif Ilmu Sosial, (Bandung Nusa Media, 2011) hlm.8

dalam hal ini adalah Ditreskrimsus Polda Jateng. Khusus untuk hambatan penegakan hukum terhadap penumpukan perkara dialami oleh pihak kepolisian. Dalam hambatan yang dialami oleh kepolisian atau penyidik salah satunya adalah terbatasnya jumlah personil, dikarekapat mengungkapkan unit yang menangani masalah *cyber* hanya ada di Polda saja. Pihak penyidik juga mengalami kesulitan bila menangani seluruh wilayah hukum Polda.⁷¹

- e) Kurangnya anggaran ataupun kemampuan keuangan negara.⁷²

Apabila akan dikembangkan sampai Polres, unit yang menangani masalah *cyber* ini membutuhkan banyak dana, dan anggaran yang cukup banyak karena sarana dan prasarana yang digunakan menggunakan teknologi yang canggih untuk dapat mengungkap *cybercrime* baik itu untuk kepentingan menyelidiki ataupun untuk melakukan penyidikan. Sedangkan ketersediaan pc yang ada di Polda hanya berjumlah 3 pc, dan itu sudah membebankan biaya yang besar. Pc dengan spesifikasi prosesor intel core i9 generasi 11, ssd 2TB (Spesifikasi gaming) anggaran yaitu sekitar kurang lebih Rp. 100.000.000/unit.

- f) Tingginya tingkat pengetahuan para pelaku terhadap teknologi informasi.

Para pelaku biasanya sudah memahami atau menguasai ilmu teknologi informasi, sehingga hal tersebut dapat dilakukan para pelaku untuk mengelabui petugas agar sulit untuk ditemukan. Terkadang ilmu teknologi informasi yang dikuasai oleh petugas sangat jauh lebih sedikit dibandingkan para pelaku tindak *cybercrime*. Kebanyakan para pelaku merupakan orang

⁷¹ R. Haryo Seto L, Wawancara, Semarang, 16 November 2020

⁷² R. Haryo Seto I, *Wawancara*, Semarang, 16 November 2020

yang sudah sangat berpengalaman dalam bidang teknologi informasi. Penegakan hukum terhadap hambatan-hambatan di atas harus dilaksanakan tanpa pandang bulu, sebagai bentuk keyakinan atas doktrin hukum, bahwa setiap orang mempunyai kedudukan yang sama di depan hukum (*equality before the law*).

Di dalam majunya zaman teknologi informasi dewasa ini sangat bermanfaat bagi kehidupan. Dengan sentuhan teknologi informasi mampu menciptakan suatu proses kegiatan masyarakat yang efektif dan efisien. Namun dengan teknologi informasi tersebut terdapat celah bagi pengguna untuk menyalahgunakan teknologi informasi seperti tindak penipuan online, ujaran kebencian, pornografi dan transaksi-transaksi dagang illegal lainnya yang bertentangan dengan hukum.

Dalam penyalahgunaan teknologi informasi tersebut harus ditindaklanjuti, guna menciptakan keamanan bagi masyarakat yang merupakan tugas dari Polda. Tindaklanjut yang dilakukan oleh Polda Jateng yaitu menerima laporan dari masyarakat tentang tindak kriminal cybercrime. Selanjutnya dari pengaduan masyarakat, Kapolda memerintahkan penyidik untuk melakukan penyidikan.

Proses penyidikan yang dilakukan oleh penyidik dilakukan melalui prosedur. Prosedur penyidikan diantaranya : a. Pengolahan TKP. Pengolahan TKP yaitu kegiatan pencarian dan pengumpulan keterangan, barang bukti, petunjuk identitas para tersangka. b. Pemantauan. Proses ini bertujuan untuk memperoleh kejelasan maupun melengkapi informasi yang telah ada berdasarkan pengetahuan dan gagasan yang diketahui serta melakukan pengawasan terhadap tempat, objek dan lingkungan tersangka. c.

Wawancara. Proses ini bertujuan memperoleh informasi dari pihak tertentu seperti saksi, korban. d. Pembuntutan. Proses ini bertujuan membuntuti terduga pelaku ataupun orang lain yang sanggup mengarahkan kepada pelaku tindak pidana. e. Penelusuran. Proses ini berupa kegiatan penyidikan dengan mengikuti dan mencari keberadaan pelaku tindak pidana dengan menggunakan teknologi informasi. f. Penyamaran. Proses ini merupakan kegiatan penyidikan yang dilakukan dengan menelusup di lingkungan pelaku seperti bergabung bersama kelompok dengan penyamaran.

Proses penyidikan di Polda Jateng telah berlangsung sesuai prosedur, beberapa kejahatan telah dilakukan penyidikan, seperti kasus perdagangan, membuat, merakit, memasukan atau menggunakan pekarangkat telekomunikasi di wilayah Republik Indonesia yang tidak sesuai dengan persyaratan teknis, ujaran kebencian, pencemaran nama baik, manipulasi penciptaan, pengrusakan informasi elektronik, isu SARA, berita bohong, dan tindak asusila seperti prostitusi online dan pornografi.

Proses penyidikan tersebut belum sepenuhnya tuntas, dimana masih terjadi kendala sehingga penyidikan beberapa masih terhenti. Penumpukan disebabkan oleh terbatasnya jumlah personel dan tenaga ahli sehingga penyelesaian kasus tersebut tidak bisa diselesaikan dengan cepat. Kendala selanjutnya adalah terbatasnya dana anggaran operasional, masalah yang cukup krusial selain perangkat hukum, yaitu SDM yang belum mencukupi, anggaran serta sarana dan prasarana untuk menunjang pengungkapan kasus-kasus *cybercrime*.

BAB IV

PROBLEMATIKA DAN PENYELESAIAN TERHADAP PENUMPUKAN PERKARA *CYBERCRIME* DI POLDA JATENG

A. Problematika Penumpukan Perkara *Cybercrime* di Polda Jateng

Dalam proses penyidikan tersebut belum sepenuhnya tuntas, menurut Bapak R. Haryo Seto dimana masih terjadi kendala sehingga penyidikan beberapa masih terhenti. Penumpukan disebabkan oleh terbatasnya jumlah personel dan tenaga ahli sehingga penyelesaian kasus tersebut tidak bisa diselesaikan dengan cepat. Kendala selanjutnya adalah terbatasnya dana anggaran operasional, masalah yang cukup krusial selain perangkat hukum, yaitu SDM yang belum mencukupi, anggaran serta sarana dan prasarana untuk menunjang pengungkapan kasus-kasus *cybercrime*. Penumpukan perkara seperti yang ada dalam data saikara Polda Jateng 2019-2020 yang berjumlah 39 perkara⁷³, sehingga hal tersebut membuktikan masih banyak penumpukan perkara di Polda Jateng.

Hambatan dalam upaya penanggulangan *cybercrime* oleh aparat kepolisian khususnya di Unit *CyberCrime* DITRESKRIMSUS POLDA Jateng yang mana selaku objek riset penulis dalam melaksanakan riset, bagi hasil riset yang sudah dicoba penulis ada sebagian hambatan yang membatasi upaya penanggulangan *cybercrime*, penulis setelah itu membaginya ke dalam tiga (3) aspek bersumber pada

⁷³ R. Haryo Seto I, Kanit 1 Subdit V Ditreskrimsus Polda Jateng, Wawancara, Semarang, 16 November 2020

hasil wawancara dengan kanit 1 subdit V Cyber, Bapak R. Haryo Seto serta penelusuran rujukan lainya, ialah⁷⁴:

1. Aspek Penyidik (Sumber Daya Manusia)

Penyidik kepolisian mempunyai kedudukan berarti dalam upaya penanggulangan *cybercrime*, dimana keahlian/ mutu penyidik serta jumlah personil penyidik di tiap unit *cybercrime* wajib mencukupi serta dicermati sebab sangat mempengaruhi buat menguak kasus-kasus *cybercrime* yang dilaporkan oleh warga, terdapatnya unit *cybercrime* di area kepolisian meyakinkan kalau dibutuhkannya penyidik spesial yang mempunyai keahlian di bidang data serta transaksi elektronik guna menanggulangi kejahatan-kejahatan di dunia maya secara optimal, dalam perihal ini penulis hendak menarangkan menimpa hambatan aspek penyidik cocok dengan informasi serta hasil wawancara penulis dengan penyidik di Unit *Cyber Crime* DITRESKRIMSUS POLDA Jateng, yang mana menimpa aspek penyidik dalam penanggulangan kejahatan *cybercrime* penyidik sendiri mempunyai hambatan yang mana mulai dari mutu penyidik serta kuantitas penyidik/ jumlah personil penyidik ialah sebahai berikut:

a) Kualitas Penyidik

Pada lembaga kepolisian khususnya di Unit *Cyber Crime* di tiap POLDA di Indonesia khususnya di POLDA Jateng dalam perihal mutu penyidik masih banyak permasalahan, hal ini disebabkan belum terdapatnya pembelajaran khusus buat para calon-calon penyidik *cybercrime* yang membagikan pengetahuan terpaut *cyber* kepada para calon- calon penyidik *cybercrime* yang khususnya menanggulangi permasalahan serta metode kerja

⁷⁴ R. Haryo Seto I, Kanit 1 Subdit V Ditreskrimsus Polda Jateng, Wawancara, Semarang, 16 November 2020

yang handal dalam melaksanakan penanggulangan terhadap tindak pidana *cybercrime*, hingga dari itu dalam prakteknya di tiap POLDA tercantum di Unit *CyberCrime* DITRESKRIMSUS POLDA Jateng sendiri seluruh penyidik *cybercrime* merupakan PPNS yang mana bukan dari perguruan kepolisian ataupun berdasarkan pembelajaran khusus penyidik- penyidik tindak pidana *cybercrime* dari POLRI namun diambil dari sipil ataupun Departemen KOMINFO yang bersumber pada rekrutmen serta ketentuan yang ada, memiliki kemampuan terpaut teknologi data serta transaksi elektronik yang mana penyidiknya disebut PPNS, namun status PPNS tersebut pula tercantum dalam anggota kepolisian bila dinyatakan lulus dalam seleksi selaku penyidik *cybercrime* POLRI.

Hambatan dalam perihal mutu penyidik sendiri bisa dilihat dari aspek kekuatan serta keahlian satuan Unit *CyberCrime* di suatu POLDA yang mana dalam perihal ini di Unit *CyberCrime* DITRESKRIMSUS POLDA Jateng mempunyai personil yang terbatas yang bertugas di unit *CyberCrime*, personil tersebut belum terdapat yang mempunyai sertifikasi program *Certified Ethical Hacker* (CEH) serta sertifikasi program *Computer Hacking Forensic Investigator Certification* (CHF) untuk dapat melaksanakan pemeriksaan barang bukti digital di laboratorium digital forensik, tidak hanya itu keahlian penyidik dalam menanggulangi kasus-kasus *cybercrime* belum mencukupi sebab masih terkendala dalam hal-hal semacam, keahlian bahasa inggris, keahlian pc forensik, keahlian *mobile* forensik, keahlian analisis jaringan transaksi keuangan dan komunikasi, serta keahlian *cyber law*.

b) Jumlah Personil Penyidik

Pada lembaga kepolisian khususnya di Unit-Unit *Cyber Crime* di tiap POLDA di Indonesia khususnya di Unit *Cyber Crime* DITRESKRIMSUS POLDA Jateng dalam perihal kuantitas/ jumlah penyidik masih hadapi kekurangan pada tiap Unit *Cyber Crime*, dengan sangat terbatasnya jumlah personil penyidik memunculkan permasalahan dimana tidak sebanding dengan banyaknya laporan ataupun aduan yang masuk dari warga, pasti dalam perihal ini berefek pada lambatnya penanganan laporan tindak pidana *cybercrime* oleh pihak kepolisian/penyidik. Pada prakteknya di Unit *Cyber Crime* DITRESKRIMSUS POLDA Jateng sendiri dari segi jumlah penyidik tindak pidana *cyber crime* personil sangat terbatas sementara itu laporan yang masuk sangat banyak pasti ini menyebabkan lambatnya penindakan permasalahan yang dilaporkan, hingga dalam prakteknya sesuai wawancara penulis dengan penyidik di Unit *Cyber Crime* DITRESKRIMSUS POLDA Jateng dalam penindakan permasalahan tindak pidana *cybercrime* bukan bersumber pada laporan yang lebih cepat dilaporkan yang ditangani terlebih dulu namun bersumber pada jumlah kerugian yang lebih diprioritaskan, hingga dalam perihal ini pasti tidak adil secara penegakan hukum, namun inilah yang berjalan dilapangan sebab keterbatasan jumlah penyidik.

1. Aspek Alat Bukti

Pada tindak pidana *cybercrime* dalam perihal alat bukti berbeda dengan alat bukti pada tindak pidana umum dimana target ataupun media *cybercrime* ialah data-data ataupun sistem elektronik dengan dihubungkan ke internet, serta tidak hanya itu masih banyak serta bebasnya warung internet (warnet) serta sarana umum yang lain yang mana ini jadi permasalahan/hambatan terhadap penyidik *cybercrime*, dalam perihal ini penulis hendak menerangkan secara rinci

mengenai hambatan aspek alat bukti sesuai dengan hasil wawancara penulis dengan penyidik di Unit *Cyber Crime* DITRESKRIMSUS POLDA Jateng, yang mana menimpa aspek alat bukti dalam penanggulangan kejahatan *cybercrime* sendiri mempunyai hambatan yang mana mulai dari alat bukti digital gampang dihilangkan serta ataupun dihapus bila tidak ditangani dengan cepat serta tepat dalam sesuatu tindak pidana *cybercrime*, serta pelaku memakai sarana umum dalam melaksanakan tindak pidana *cybercrime*, ialah penjelasannya sebagai berikut:

a) Barang Bukti Digital Mudah Dihilangkan

Jika Tidak Ditangani Dengan Tepat Waktu Barang bukti dalam tindak pidana *cybercrime* sesuai prakteknya merupakan dalam bentuk digital dikarenakan yang dijadikan sasaran dalam tindak pidana *cybercrime* merupakan data-data atau sistem elektronik yang mana misalnya dalam kasus hacking dan lain sebagainya dan atau melakukan pencemaran nama baik atau penipuan secara online yang mana semua instrument yang digunakan ialah serba elektronik dengan dihubungkan ke internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelaku kejahatan *cybercrime*, maka dari itu pada prakteknya dalam hal alat bukti dalam tindak pidana *cybercrime* lebih sulit jika dibandingkan dengan alat bukti pada tindak pidana umum yang mana pada tindak pidana umum alat buktinya dalam bentuk fisik dan tidak mudah untuk dihilangkan jejaknya yang mana hal ini sangat bertolak belakang dengan tindak pidana *cybercrime* dalam hal alat bukti khususnya.

b) Pelaku Menggunakan Fasilitas Umum Dalam Melakukan Tindak Pidana *Cyber Crime*

Pada kasus- kasus tindak pidana *cybercrime* tidak sedikit pelaku tindak pidana *cybercrime* dalam melakukan aksinya menggunakan fasilitas umum dalam mengakses dan berbuat sesuatu dengan media elektronik dengan sambungan internet menggunakan fasilitas warung internet (warnet) dan atau fasilitas umum lainnya, dan kita ketahui warung internet (warnet) di Indonesia masih dengan bebasnya beroperasi tanpa ada regulasi dan pengawasan dari pemerintah ataupun penegak hukum yang ada sedangkan penyidik dalam melakukan penyelidikan dalam tindak pidana *cybercrime* untuk melakukan pelacakan pelaku berdasarkan alamat server atau informasi *IP Address* dari alat elektronik pelaku maka dalam hal ini tentu menjadi kendala dalam menangkap pelaku dan mengenai alat bukti akan semakin rumit. Pelaku-pelaku tindak pidana *cybercrime* juga memanfaatkan hal tersebut agar jejak digitalnya tidak dapat dijadikan alat bukti atau sulit mengenai pembuktian dalam kejahatan *cybercrime*.

c) Keberadaan Para Saksi Tidak di Tempat Yang Sama Dengan Korban dan Pelaku

Pada tindak pidana *cybercrime* sangat berbeda dengan tindak pidana umum, khususnya dalam hal alat bukti yang berkaitan dengan saksi-saksi, yang mana pada tindak pidana *cybercrime* saksi- saksi belum tentu keberadaannya di lokasi/ tempat yang sama dengan korban dan atau pelaku, padahal keterangan saksi merupakan hal yang penting dalam proses penegakan hukum khususnya dalam kasus tindak pidana *cybercrime* dan termasuk alat bukti sesuai Pasal 184 Ayat (1) Huruf a KUHAP yang mana keterangan saksi merupakan termasuk dari alat bukti yang sah. Saksi korban dalam kasus *cybercrime* berperan sangat penting dan tapi pada prakteknya

jarang sekali terdapat saksi dalam kasus *cybercrime* dikarenakan saksi korban yang berada di luar daerah atau bahkan berada di luar negeri, hal tersebut tentu 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, dan hal serupa dialami oleh penyidik Unit *Cyber Crime* DITRESKRIMSUS POLDA Jateng dimana sangat kesulitan menangani kasus *cybercrime* terkait aspek alat bukti yang berkaitan dengan saksi- saksi, namun beda halnya ketika pelaku *cybercrime* tertangkap tangan dalam melakukan aksi kejahatannya dimana alat bukti dapat langsung diamankan oleh petugas kepolisian yang tentunya tidak terlalu membutuhkan saksi-saksi dalam hal tersebut.

2. Aspek Sarana dan Prasarana

Pada tindak pidana *cybercrime* dalam menguak kasus-kasus *cybercrime* diperlukan sarana yang sanggup mendukung kinerja aparat kepolisian/penyidik, sarana tersebut berbentuk laboratorium forensik pc yang digunakan buat menguak data-data yang bertabiat digital dan merekam serta menaruh bukti-bukti yang berbentuk *soft copy* (foto, program, html, suara, serta lain sebagainya). Pc forensik diketahui selaku digital forensik, ada pula tujuannya yakni buat mengamankan serta menganalisis fakta digital, dan mendapatkan bermacam

kenyataan yang objektif dari suatu peristiwa ataupun pelanggaran keamanan dari sistem data, bermacam kenyataan tersebut hendak jadi fakta yang hendak digunakan dalam proses hukum⁷⁵. Lewat internet forensik, penyidik bisa mengenali siapa saja orang yang mengirim email, kapan serta dimana keberadaan alamat pengirim bersumber pada server pengirim, serta dalam contoh lain kita dapat melihat siapa pengunjung *web* secara lengkap dengan data *IP Address*, perlengkapan elektronik yang dipakainya serta keberadaannya dan aktivitas apa yang dicoba pada *web* tersebut⁷⁶.

Bersumber pada hasil wawancara serta riset penulis dengan salah satu penyidik di Unit *Cyber Crime* DITRESKRIMSUS POLDA Jateng, ialah dengan bapak R. Haryo Seto L SH, M. Krim, yang mana dia menarangkan dalam perihal kondisi sarana yang digunakan dalam penindakan permasalahan *cybercrime* serta dari puluhan POLDA dari tiap provinsi di Indonesia cuma sebagian POLDA yang telah mempunyai laboratorium digital forensik, tercantum POLDA Jateng telah memiliki laboratorium digital forensik. Dalam perihal ini tim forensik Ditreskrimsus Polda Jateng ikut membantu POLDA di daerah hukum pulau Jawa bagian tengah ialah termasuk POLDA Wilayah Istimewa Yogyakarta.

B. Penanganan Problem Penumpukan Perkara *Cybercrime* di Polda Jateng

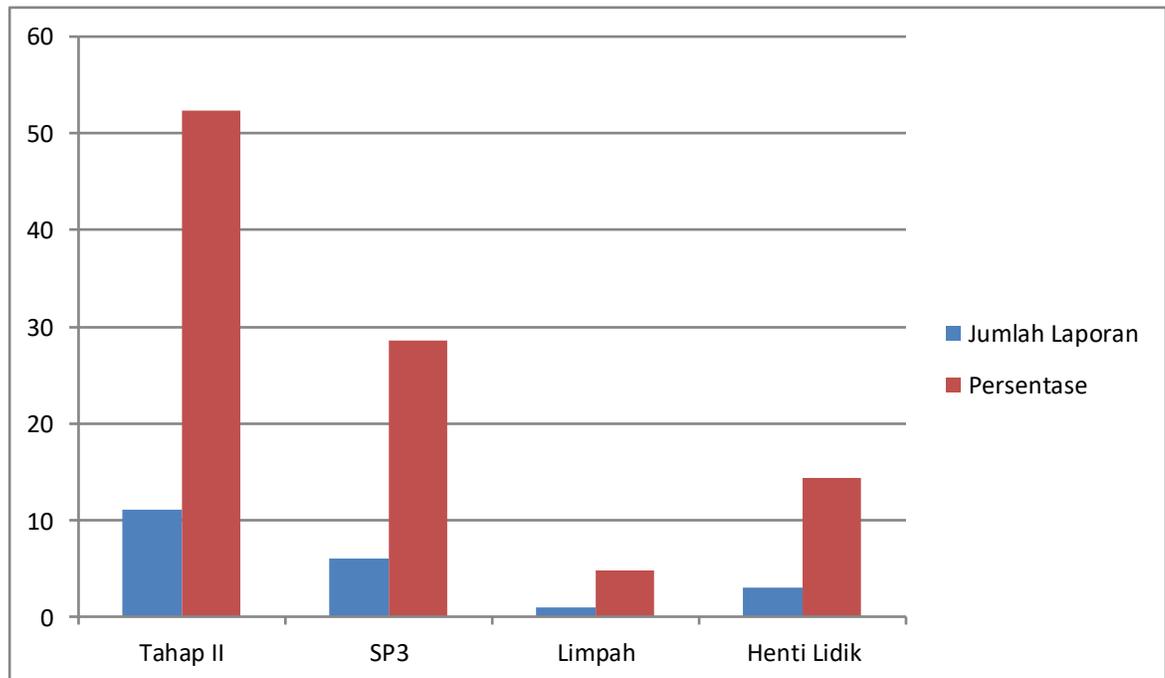
Berdasarkan laporan dari Polda Jateng Tahun 2019 menunjukkan bahwa jumlah penumpukan kasus sebanyak 21 kasus *cybercrime*. Dari 21 kasus, jumlah kasus tertinggi pada penyidikan Tahap II yaitu sebanyak 11 kasus atau 52,38%.

⁷⁵ Hendy Sumadi, "Kendala Dalam Menanggulangi Tindak Pidana Penipuan Transaksi Elektronik Di Indonesia", dikutip dari <http://ejournal.sthb.ac.id/index.php/jwy/article/view/102>, (diakses pada 1 Agustus 2021)

⁷⁶ Sucipto, komputer forensik, <http://www.seputarpengetahuan.com/2014/11/komputer-forensik-pengertian-dan-tujuan> (diakses pada 2 Agustus 2021)

Berdasarkan laporan dari Polda Jateng Tahun 2020 menunjukkan bahwa jumlah penumpukan kasus sebanyak 18 kasus *cybercrime*. Dari 18 kasus, jumlah kasus tertinggi pada penyidikan P. 21 yaitu sebanyak 13 kasus atau 72,22%. Berikut dapat dilihat pada diagram 4.1 dan 4.2⁷⁷:

Gambar 4.1
Diagram Penumpukan Perkara *Cybercrime* Tahun 2019



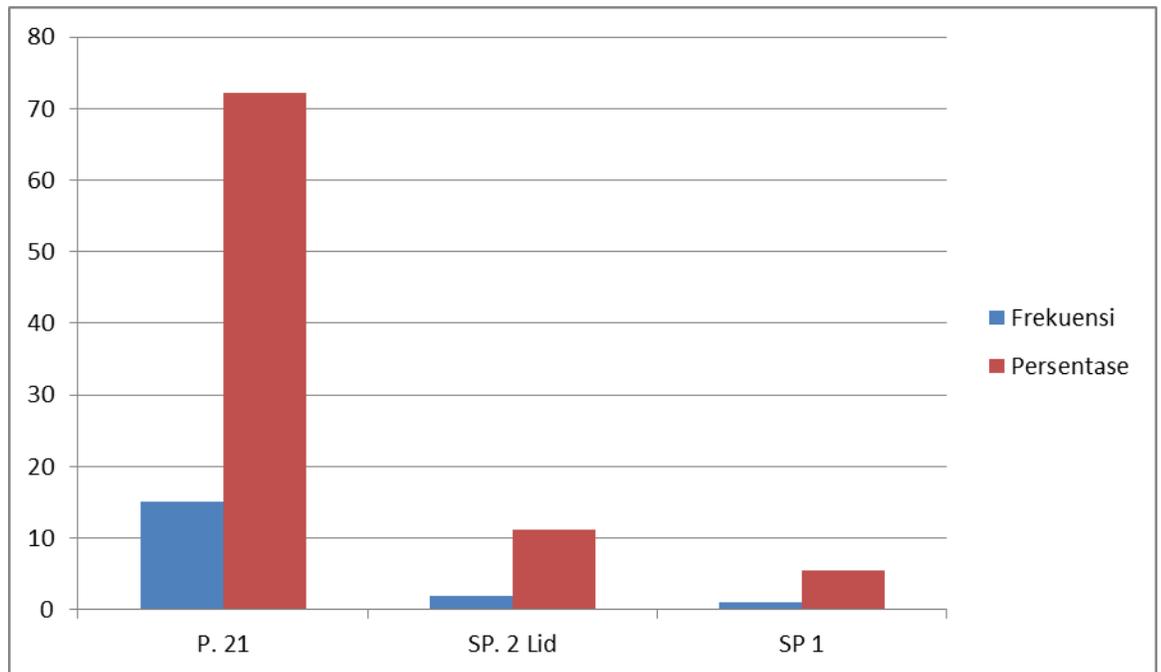
Sumber: Data Saikara Ditreskrimsus Polda Jateng Tahun 2019

Kondisi penumpukan perkara *Cybercrime* di Polda Jateng tahun 2019 menunjukkan bahwa kinerja penyidik Ditreskrimsus Polda Jateng masih belum maksimal. Belum maksimalnya penyidik disebabkan karena keterbatasan personil. Kendala keterbatasan personil seperti tenaga ahli IT dan *cyber forensic*. Terbatasnya jumlah personil tenaga ahli.

⁷⁷ R. Haryo Seto I, Kanit 1 Subdit V Ditreskrimsus Polda Jateng, Wawancara, Semarang, 16 November 2020

Gambar 4.2.

Diagram Penumpukan Perkara *Cybercrime* Tahun 2020



Sumber: Data Saikara Dittreskrimsus Polda Jateng Tahun 2020

Berdasarkan diagram di atas, kondisi penumpukan perkara *cybercrime* di Polda Jateng tahun 2019-2020 menunjukkan bahwa kinerja penyidik masih belum maksimal. Ketidakmaksimalan itu disebabkan karena keterbatasan personil. Kendala keterbatasan personil seperti tenaga ahli IT dan *cyber forensic*. Terbatasnya jumlah personil tenaga ahli. Lebih ironis lagi laporan tingkat kejahatan siber di Jawa Tengah semakin meningkat, dengan keterbatasan personil dan tenaga ahli di pihak kepolisian maka penyelesaian kasus tersebut tidak bisa diselesaikan dengan cepat. Dampaknya bisa dirasakan langsung oleh pihak korban atau kejahatan siber. Kualitas fasilitas teknologi informasi di Jawa Tengah memang sudah cukup baik, namun tidak sebanding dengan jaminan keamanan oleh para pengguna⁷⁸.

⁷⁸ Aswan, Tindak Pidana Penipuan Berbasis Transaksi Online. Makassar: Guepedia, 2019.

Kendala lain yang krusial adalah terbatasnya dana anggaran operasional, masalah yang cukup krusial selain perangkat hukum, yaitu SDM yang belum mencukupi, anggaran serta sarana dan prasarana untuk menunjang pengungkapan kasus-kasus *cybercrime*. Sekarang ini anggaran yang ada hanya cukup untuk satu perkara per satu bulan. Padahal kenyataannya satu bulan bisa sampai 15 kasus⁷⁹.

Langkah-langkah yang ditempuh oleh Polda Jateng untuk menangani penumpukan adalah:⁸⁰

1. Menambah tim penyidik, mengingat faktor jumlah penyidik menjadi kendala terhambatnya penyidikan.
2. Menyediakan serta menambah tenaga penyidik yang kompeten di bidang IT beserta sarana-sarana teknologi yang diperlukan.
3. Meningkatkan anggaran operasional. Peningkatan ini mengingat jumlah dana yang tersedia tidak sebanding dengan jumlah kasus yang ditangani.
4. Melakukan peningkatan kompetensi penyidik dan penyidik pembantu melalui penerbitan sertifikasi profesi penyidik POLRI POLDA Jawa Tengah. Dalam melaksanakan peningkatan kompetensi penyidik dan penyidik pembantu ini dilakukan secara efektif dikarenakan dilaksanakan tiap tahun dengan kuota yang terus bertambah.
5. Dalam mengurangi terjadinya penumpukan, maka biasanya menyerahkan kasus-kasus ke unit lain yang sedang menangani kasus lebih sedikit.

⁷⁹Avi, Detiknews, *Penanganan Kasus Cyber Crime Terganjil Regulasi dan Anggaran*, <http://repository.ums.ac.id/bitstream/handle/123456789/7445/BAB%20IV.pdf?sequence=4&isAllowed=y> ,(diakses tanggal 2 Juni 2021)

⁸⁰R. Haryo Seto I, Kanit 1 Subdit V Ditreskrimsus Polda Jateng, Wawancara, Semarang, 16 November 2020

6. Kedepannya Ditreskrimsus Polda Jateng menginginkan unit yang menangani permasalahan *cybercrime* ini akan dikembangkan sampai polres, tentu dengan fasilitas yang memadai.

Berdasarkan hasil penelitian di Polda Jateng, bahwa masih terdapat penumpukan perkara. Penumpukan ini disebabkan oleh Aspek penyidik yang belum memiliki keahlian yang mumpuni seperti keahlian bahasa inggris, keahlian pc forensik, keahlian *mobile forensik*, keahlian analisis jaringan transaksi keuangan dan komunikasi, serta keahlian *cyber law*. Selain itu permasalahan yang ada adalah masih kurangnya jumlah penyidik. Problematika selanjutnya adalah barang bukti yang mudah dihilangkan sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelaku kejahatan *cybercrime*, maka dari itu pada prakteknya dalam hal alat bukti dalam tindak pidana *cybercrime* lebih sulit jika dibandingkan dengan alat bukti pada tindak pidana umum yang mana pada tindak pidana umum. Sulitnya mengungkap kasus karena pelaku menggunakan fasilitas umum dalam melakukan aksinya. Keberadaan saksi tidak di tempat yang sama dengan korban dan pelaku. Serta aspek sarana prasarana yang kurang mendukung.

Kendala tersebut disebabkan masih terbatasnya undang-undang yang ada khususnya yang mengatur *cybercrime*. Hasil penelitian sesuai dengan kenyataan di lapangan bahwa kendala pengungkapan kasus *cybercrime* disebabkan:

1. Perangkat hukum yang belum memadai

Para penyidik (khususnya Polri) melakukan analogi atau perumpamaan dan persamaan terhadap pasal-pasal yang ada dalam KUHP sependapat bahwa perlu dibuat undang-undang yang khusus mengatur *cybercrime*.

2. Kemampuan penyidik

Secara umum penyidik Polri masih sangat minim dalam penguasaan operasional komputer dan pemahaman terhadap hacking komputer serta kemampuan melakukan penyidikan terhadap kasus-kasus itu. Beberapa faktor yang sangat berpengaruh (determinan) adalah:

- a. Kurangnya pengetahuan tentang komputer.
- b. Pengetahuan teknis dan pengalaman para penyidik dalam menangani kasus-kasus *Cybercrime* masih terbatas.
- c. Faktor sistem pembuktian yang menyulitkan para penyidik.

3. Alat Bukti

Persoalan alat bukti yang dihadapi di dalam penyidikan terhadap *cybercrime* antara lain berkaitan dengan karakteristik kejahatan *cybercrime* itu sendiri, yaitu ; sasaran atau media *cybercrime* adalah data dan atau sistem komputer atau sistem internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelakunya, *cybercrime* seringkali dilakukan hampir-hampir tanpa saksi, di sisi lain, saksi korban seringkali berada jauh di luar negeri sehingga menyulitkan penyidik melakukan pemeriksaan saksi dan pemberkasan hasil penyidikan.

4. Fasilitas komputer forensic

Untuk membuktikan jejak-jejak para *hacker*, dan *cracker* dalam melakukan aksinya terutama yang berhubungan dengan program-program dan data-data komputer, sarana Polri belum memadai karena belum ada komputer forensic. Fasilitas ini diperlukan untuk mengungkap data-data digital serta merekam dan menyimpan bukti-bukti berupa *soft copy* (image, program, dsb). Dalam hal ini Polri masih belum mempunyai fasilitas forensic computing yang memadai. Fasilitas *forensic computing* yang akan didirikan Polri diharapkan akan dapat melayani tiga hal penting yaitu *evidence collection, forensic analysis, expert witness*.

Berdasarkan uraian di atas, dapat diketahui bahwa terjadinya penumpukan perkara *cybercrime* disebabkan oleh oleh aspek penyidik yang belum memiliki keahlian yang mumpuni, kurangnya jumlah penyidik, barang bukti yang mudah dihilangkan, pelaku menggunakan fasilitas umum dalam melakukan aksinya, keberadaan saksi tidak di tempat yang sama dengan korban dan pelaku dan aspek sarana prasarana yang kurang mendukung.

Dari hasil penelitian yang telah dilakukan mengenai problematika dan penyelesaian perkara *cybercrime* di Polda Jateng menunjukkan bahwa masih terjadi penumpukan perkara *cybercrime* di Polda Jateng. Penanganan ini dilakukan dengan menambah tim penyidik, mengingat faktor jumlah penyidik menjadi kendala terhambatnya penyidikan. Menyediakan serta menambah tenaga penyidik yang kompeten di bidang IT beserta sarana-sarana teknologi yang diperlukan. Meningkatkan anggaran operasioanal. Peningkatan ini mengingat jumlah dana yang tersedia tidak sebanding dengan jumlah kasus yang ditangani. Melakukan peningkatan kompetensi penyidik dan penyidik pembantu melalui penerbitan sertifikasi profesi penyidik POLRI POLDA Jawa Tengah. Dalam melaksanakan peningkatan kompetensi penyidik dan penyidik pembantu ini dilakukan secara efektif dikarenakan dilaksanakan tiap tahun dengan kuota yang terus bertambah. Dalam mengurangi terjadinya penumpukan, maka biasanya menyerahkan kasus-kasus ke unit lain yang sedang menangani kasus lebih sedikit. Kedepannya Ditreskrimsus Polda Jateng menginginkan unit yang menangani permasalahan *cybercrime* ini akan dikembangkan sampai polres, tentu dengan fasilitas yang memadai.

Menimbang berdasarkan hasil diatas, keputusan untuk melakukan dekrimalisasi dan kriminalisasi didasarkan pada faktor-faktor kebijakan tertentu dengan menimbang bermacam-macam faktor, termasuk:

1. Keseimbangan sarana-sarana yang memerlukan didalam hubungannya dengan hasil-hasil yang ingin dicapai;

2. Analisis biaya terhadap hasil-hasil yang diperoleh dalam hubungannya dengan tujuan-tujuan yang dicari;
3. Penafsiran atau penelitian tujuan-tujuan yang dicari itu dalam kaitannya bersama prioritas-prioritas lainnya didalam pengalokasian sumber-sumber tenaga manusia;
4. Pengaruh sosial dari dekriminialisasi dan kriminalisasi yang berkenaan dengan pengaruh-pengaruhnya yang sekunder.

Berdasarkan uraian di atas bahwa langkah-langkah penanganan problematika penumpukan perkara *cybercrime* di Polda Jateng dengan menambah tim penyidik, meningkatkan anggaran operasioanal, peningkatan kompetensi penyidik dan penyidik pembantu.

BAB V

PENUTUP

A. Kesimpulan

1. Berdasarkan data kasus pada tahun 2020 menunjukkan bahwa jumlah penumpukan kasus sebanyak 18 kasus *Cybercrime*. Dari 18 kasus, jumlah kasus tertinggi pada penyidikan P. 21 yaitu sebanyak 13 kasus atau 72,22%. Dengan demikian, unit *cybercrime* Polda Jateng mengambil langkah prosedur penanganan sebagai berikut:
 - a. Menerima pengaduan atau laporan dari seorang tentang adanya tindak pidana.
 - b. Mencari keterangan dan barang bukti.
 - c. Memerintah berhenti seorang yang dicurigai dan menanyakan serta memeriksa tanda pengenal diri.
 - d. Mengadakan tindakan lain menurut hukum yang bertanggung jawab. Atas perintah dari penyidik bisa melakukan tindakan berupa:
 - e. Penangkapan, larangan meninggalkan tempat, penggeledahan dan penyitaan.
 - f. Pemeriksaan dan penyitaan surat.
 - g. Mengambil sidik jari dan memotret seseorang.
 - h. Membawa dan menghadapkan seseorang pada penyidik.
2. Kondisi penumpukan perkara *Cybercrime* di Polda Jateng tahun menunjukkan bahwa kinerja penyidik Ditreskrimsus Polda Jateng masih belum maksimal. Belum maksimalnya penyidik disebabkan karena keterbatasan personil. Kendala keterbatasan personil seperti tenaga ahli IT dan *cyber forensic*. Terbatasnya jumlah personil tenaga ahli. Kendala lain yang krusial adalah terbatasnya dana

anggaran operasional, masalah yang cukup krusial selain perangkat hukum, yaitu SDM yang belum mencukupi, anggaran serta sarana dan prasarana untuk menunjang pengungkapan kasus-kasus *cybercrime*. Sekarang ini anggaran yang ada hanya cukup untuk satu perkara per satu bulan. Padahal kenyataannya satu bulan bisa sampai 15 kasus. Adapun langkah penyelesaian ditempuh oleh *Cybercrime* Polda Jateng untuk menangani penumpukan adalah:

- a. Menambah tenaga penyidik yang kompeten di bidang IT.
- b. Meningkatkan anggaran operasioanal.
- c. Peningkatan kompetensi penyidik dan penyidik
- d. Meminimalisir penumpukan dengan menyerahkan kasus-kasus ke unit
- e. Ditreskrimsus Unit *Cybercrime* Polda Jateng dalam menangani kasus *cybercrime* perlu dikembangkan sampai polres, dikarenakan fasilitas kurang memadai.

B. Saran

Berdasarkan hasil penelitian dan pembahasan diketahui bahwa masih terjadi penumpukan kasus penanganan penyidikan *Cybercrime*. Oleh karena itu disarankan kepada Polda Jateng agar :

1. Untuk menambah tim penyidik, mengingat faktor jumlah penyidik menjadi kendala terhambatnya penyidikan.
2. Menyediakan tenaga penyidik yang kompeten di bidang IT
3. Meningkatkan anggaran operasioanal. Peningkatan ini mengingat jumlah dana yang tersedia tidak sebanding dengan jumlah kasus yang ditangani

DAFTAR PUSTAKA

Buku dan Jurnal :

- Wahid, Abdul dan Labib, Muhammad, 2005, *Kejahatan Mayantara*, Bandung, Rafikia Aditama.
- Muhammad, Abdulkadir, 2004, *Hukum dan Penelitian Hukum*, Bandung, Citra Aditya Bakti.
- Aryyaguna, Adhi Dharma, 2017, “Tinjauan Kriminologis Terhadap kejahatan Penipuan Berbasis Online”, *Skripsi* Fakultas Hukum Universitas Hasanudin Makassar.
- Antoni, A, 2018, *Dunia Maya (Cyber Crime)*”, *Simak Online*, Fakultas Syariah dan Hukum UIN Raden Fatah Palembang.
- Sanda, Antonius, 2016, “*Tinjauan Yuridis Terhadap Fenomena Cyber Bullying Sebagai Kejahatan di Dunia Cyber Dikaitkan Dengan Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008*” skripsi Fakultas Hukum Universitas Hassanudin Makassar.
- Arikunto, Suharsimi, 1992, *Prosedur Penelitian : Suatu Pendekatan Praktek*. Jakarta, Rineka Cipta.
- Admaja, Priyatno, 2004, *Kebijakan Legislasi Tentang Sistem Pertanggungjawaban Pidana Koorporasi di Indonesia*, Bandung, CV Utomo.
- Poernomo, Bambang, 1988, *Kapita Selekta Hukum Pidana*. Yogyakarta, Liberty.
- Arif, Barda Nawawi, 2005, *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan*. Bandung, Citra Aditya Bakti.
- Ashshofa, Burhan, 2013, *Metode Penelitian Hukum*. Jakarta, PT Rineka Cipta.
- Syamsuddin, Aziz, 2011, *Tindak Pidana Khusus*, Jakarta, Sinar Grafika.
- Didik, M. Arief Mansur dan Gultom, Alisatris, 2005, *Cyber Law-Aspek Hukum Teknologi Informasi*. Bandung, Refika Aditama.
- Edmon, Makarim. 2003, *Kompilasi Hukum Telematika*. Jakarta, Raja Grafindo Persada.
- Jacob, Hedriyanto kusno, 2017, “*Peranan penyidik dalam Tindak Pidana Cybercrime*”, *Jurnal Ilmiah*.
- Gregory, J Robert, 2015, *Psychological Testing: Hisory, Principles, and Applications*. United States of Amerika, Pearson Education Limited.
- Sukanto, Soerjono, 1986, *Pengantar Penelitian Hukum*. Jakarta, UI Presa.
- Sudarto, 1998, *Hukum dan Hukum Pidana*. Bandung, Alumnii.
- Suseno, Sigid, 2012, *Yurisdiksi Tindak Pidana Siber*, Refika Aditama, Bandung.

- Wahyudi, Johan, 2012, “*Dokumen elektronik sebagai alat bukti pada pembuktian di pengadilan*”, Jurnal Fakultas Hukum Universitas Airlangga Surabaya.
- Suparni, Niniek, 2009, “*Cyberspace Problematika dan Aplikasi Pengaturannya*”, Jakarta, Sinar Grafika.
- Bakara, Surya Putra Dharma, 2016, “*Upaya Direktorat Kriminal Khusus Subdit Cyber Crime Dalam Menanggulangi Tindak Pidana Cyber Crime Yang Berkaitan Dengan Pornografi dan Pornoaksi (STUDI POLDA LAMPUNG)*” skripsi Fakultas Hukum Universitas Lampung.
- Suteki, dan Taufani, Galang, 2018, *Metodologi Penelitian Hukum (Filsafat, Teori dan Praktik)*. Depok, PT Raja Grafindo Persada.
- Widodo, 2008, *Aspek Hukum Pidana Kejahatan Mayantara*, Yogyakarta, Aswaja Pressindo.
- Widodo, 2015, *Memerangi Cybercrime Karakteristik Motivasi dan Srategi Penangananya dalam Perspektif Kriminologi*, Jakarta, Aswaja Pressindo.
- Arifah, Dista Amalia, 2017, “*Kasus Cybercrime di Indonesia*”, Jurnal Bisnis dan Ekonomi.
- Galih, Yuliana Surya, 2019, “*Yurisdiksi Hukum Pidana dalam Dunia Maya*”, Jurnal Ilmiah Galuh Justisi.
- Sutopo, HB, 1999, *Metode Penelitian Kualitatif*, Surakarta, UNS Press.
- Moloeng, Lexy J, 2002, *Metode Penelitian Kualitatif*, Bandung, PT Rosdakarya.

Peraturan Perundang-Undangan :

- Undang-Undang Dasar Negara Republik Indonesia 1945
- Kitab Undang-Undang Hukum Acara Pidana.
- Undang-undang Nomor 1 tahun 1946 Jo Undang-undang Nomor 73 Tahun 1958 tentang Pembentukan Kitab undang-undang hukum Pidana.
- Undang-Undang No.8 tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP).
- Undang-undang Nomor. 2 tahun 2002 Tentang Kepolisian Negara Republik Indonesia.
- PP No. 27 Tahun 1983 jo PP No.58 Tahun 2010 tentang Pelaksanaan KUHAP.
- Undang-Undang Nomor 11 Tahun 2008 Tentang Internet & Transaksi Elektronik (ITE).
- Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 14 Tahun 2012 tentang Manajemen Penyidikan Tindak Pidana.

Website :

<http://humas.polri.go.id/News/Pages/Sosialisasi-Perkap-nomor-14-tahun-2012.aspx> (diakses pada 11 desember 2020)

<http://repository.umy.ac.id/bitstream/handle/123456789/7445/BAB%20IV.pdf?sequence=4&isAllowed=y> (diakses pada 2 Mei 2021)

<http://repository.umy.ac.id/bitstream/handle/123456789/7445/BAB%20IV.pdf?sequence=4&isAllowed=y> (diakses pada 2 Juni 2021)

<http://ejournal.sthb.ac.id/index.php/jwy/article/view/102>, (diakses pada 1 Agustus 2021)

<http://www.seputarpengetahuan.com/2014/11/komputer-forensik-pengertian-dan-tujuan> (diakses pada 2 Agustus 2021)

Lampiran-lampiran



Foto di Ditreskrimsus Polda Jateng Subdit V Siber 17 november 2020



Foto bersama Ibu Ainun sekretaris Subdit V Ditreskrimsus Polda Jateng 16 november 2020

TRANSKRIP WAWANCARA SKRIPSI

Narasumber : R. Haryo Seto L SH, M.Krim.,
Durasi wawancara : 35 menit
Tanggal wawancara : 16 November 2020
Tempat : JL. Sukun raya no 46 Spondol Wetan, Banyumanik, Semarang

Hasil wawancara :

Pertanyaan: bagaimana kendala proses penumpukan perkara di Ditreskrimsus Polda Jateng bisa terjadi?

Jawaban:

masalah mengenai penumpukan perkara di Ditreskrimsus Polda Jateng sulit untuk diproses maupun untuk ditegakkan, karena memerlukan waktu yang cukup lama dan sulitnya melakukan penyelidikan terhadap tindak pidana tersebut. Pihak kepolisian menyadari betapa sulitnya menjangkau pelaku yang ada. Beberapa kasus yang ada atau menumpuk di Ditreskrimsus Polda Jateng, sulit di tangani disebabkan karena membutuhkan kepakaran cyber dan dana yang sangat besar.

Pertanyaan : Problematika apa saja yang terjadi dalam penumpukan perkara cyber crime di Polda Jateng?

Jawaban:

Ya, banyak. Seperti kurangnya personel dan tenaga ahli sehingga proses penyelesaiannya tidak bisa dilakukan dengan cepat. Selain itu terbatasnya anggaran dana operasional, SDM yang belum mencukupi serta kurangnya sarana dan prasarana yang memadai.

Pertanyaan: Bagaimana kondisi sarana dan prasarana yang ada di Polda Jateng?

Jawaban:

Terkait kondisi sarana yang digunakan dalam penindakan permasalahan cybercrime serta dari puluhan POLDA dari tiap provinsi di Indonesia cuma sebagian POLDA yang telah mempunyai laboratorium digital forensik, tercantum POLDA Jateng telah memiliki laboratorium digital forensik. Dalam perihal ini tim forensik Ditreskrimsus Polda Jateng ikut membantu POLDA di daerah hukum pulau Jawa bagian tengah ialah termasuk POLDA Wilayah Istimewa Yogyakarta.

Pertanyaan: Apakah tugas dari menangani masalah cybercrime hanya ditangani oleh personil Ditreskrimsus saja?

Jawaban :

Iya mas. Berdasarkan Peraturan Kapolri Nomor 22 Tahun 2010 tentang Susunan Organisasi dan Tata Kerja Pada Tingkat Kepolisian Daerah, unit yang menangani masalah cyber merupakan salah satu bagian dari tugas-tugas Ditreskrimsus, dan Ditreskrimsus ada di tingkat Polda saja dan merupakan salah satu unsur pelaksana tugas pokok yang berada dibawah Kapolda. Kedepannya unit yang menangani permasalahan cyber crime ini akan dikembangkan sampai polres tergantung pada kemampuan keuangan negara.

Pertanyaan : Selanjutnya apa yang bapak harapkan dalam menangani penumpukan perkara Cybercrime di Ditterskrimsus Polda Jateng ini?

Jawaban :

Keinginan saya yaitu, 1. Menambah jumlah penyidik, karena jelas ini sangat kekurangan. 2. Menambah penyidik yang kompeten dalam bidang IT, serta melengkapi sarana teknologi yang diperlukan. 3. Meningkatkan anggaran dana operasional yang tersedia, karena dana yang ada sekarang tidak cukup untuk menyelesaikan kasus-kasus yang ada. 4. Melaksanakan pendidikan dalam rangka melakukan peningkatan penyidik melalui penerbitan sertifikasi profesi penyidik. 5. Kedepannya saya menginginkan unit yang menangani kasus ini tidak hanya ada di Polda saja, tapi isa dikembangkan sampai ke Polres.

Surat keterangan telah melaksanakan penelitian dari Ditreskrimsus Polda Jateng,

18 November 2020

KEPOLISIAN NEGARA REPUBLIK INDONESIA
DAERAH JAWA TENGAH
DIREKTORAT RESERSE KRIMINAL KHUSUS
Jalan Sukun Raya 46, Banyumanik, Semarang



SURAT KETERANGAN

Nomor: SKET/ 19 /XI/HUM.5.4./2020/Reskrimsus

Yang bertanda tangan di bawah ini Direktur Reserse Kriminal Khusus Polda Jateng menerangkan bahwa:

Nama : SIGIT PAMUNGKAS

NIM : 1502056057

Jurusan : Sarjana Program Studi Ilmu Hukum

Perguruan Tinggi: Universitas Islam Negeri (UIN) Walisongo Semarang

benar-benar telah melakukan penelitian/riset dari tanggal 16 November s.d. 17 November 2020 di Subdit V / tipidsiber Ditreskrimsus Polda Jateng untuk mengumpulkan data guna penulisan Skripsi pada Program Studi S-1 Ilmu Hukum Universitas Islam Negeri (UIN) Walisongo Semarang dengan judul "PROBLEMATIKA PROSEDUR DAN PENANGANAN TERHADAP PENUMPUKAN PERKARA TINDAK PIDANA CYBER CRIME DI POLDA JATENG".

Demikian surat keterangan ini dibuat untuk dapat dipergunakan sebagaimana mestinya.

Dikeluarkan di : Semarang
Pada tanggal : 18. November 2020

a.n. DIREKTUR RESERSE KRIMINAL KHUSUS
WADIR


DJOKO JULIANTO, S.I.K., M.H.
AJUN KOMISARIS BESAR POLISI NRP 77071232