TINJAUAN HUKUM PENENTUAN LOCUS DELICTI DALAM PENYIDIKAN KEJAHATAN SIBER

TESIS

Oleh:

AKSARUDIN ADAM

NIM : 20302400387

Konsentrasi : Hukum Pidana

PROGRAM MAGISTER (S2) ILMU HUKUM
UNIVERSITAS ISLAM SULTAN AGUNG
SEMARANG
2025

TINJAUAN HUKUM PENENTUAN LOCUS DELICTI DALAM PENYIDIKAN KEJAHATAN SIBER

TESIS

Diajukan untuk penyusunan Tesis
Program Studi Ilmu Hukum

Oleh:

AKSARUDIN ADAM
NIM : 20302400387
Konsentrasi : Hukum Pidana

PROGRAM MAGISTER (S2) ILMU HUKUM
UNIVERSITAS ISLAM SULTAN AGUNG
SEMARANG
2025

TINJAUAN HUKUM PENENTUAN LOCUS DELICTI DALAM PENYIDIKAN KEJAHATAN SIBER

Diajukan Untuk Penyusunan Tesis

Program Magister Hukum

Oleh:

Nama : AKSARUDIN ADAM

NIM : 20302400387

Program Studi : Magister (S2) Ilmu Hukum (M.H.)

Disetujui oleh:

Pembimbing I

Tanggal,

Prof. Dr. H. Gunarto, S.H., S.E., Akt., M.Hum.

NIDN. 06-0503-6205

Dekan

Fakultas Hukum

UNISSULA

Prof. Dr. H. Jawade Hafidz, S.H., M.H.

NIDN. 06-2004-6701

TINJAUAN HUKUM PENENTUAN LOCUS DELICTI DALAM PENYIDIKAN KEJAHATAN SIBER

Telah Dipertahankan di Depan Dewan Penguji
Pada Tanggal 13 November 2025
Dan dinyatakan **LULUS**

Tim Penguji
Ketua,
Tanggal,

Dr. Arpangi, S.H., M.H.
NIDN. 06-1106-6805

Anggota

Prof. Dr. H. Gunarto, S.H., S.E., Akt., M.Hum.
NIDN. 06-0503-6205

Anggota,

Dr. Ratih Mega Puspasari, SH, MKn.
NIDN. 06-2410-8504

Mengetahui
Dekan
Fakultas Hukum
UNISSULA

Prof. Dr. H. Jawade Hafidz, S.H., M.H.
NIDN: 06-2004-6701

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama : AKSARUDIN ADAM
NIM : 20302400387

Dengan ini saya nyatakan bahwa Karya Tulis Ilmiah yang berjudul:

TINJAUAN HUKUM PENENTUAN LOCUS DELICTI DALAM PENYIDIKAN KEJAHATAN SIBER

Adalah benar hasil karya saya dan penuh kesadaran bahwa saya tidak melakukan tindakan plagiasi atau mengambil alih seluruh atau sebagian besar karya tulis orang lain tanpa menyebutkan sumbernya. Jika saya terbukti melakukan tindakan plagiasi, saya bersedia menerima sanksi sesuai dengan aturan yang berlaku.

Semarang, 30 Oktober 2025
Yang Membuat Pernyataan.

(AKSARUDIN ADAM)

PERNYATAAN PERSETUJUAN UNGGAH KARYA ILMIAH

Saya yang bertanda tangan di bawah ini:

Nama	:	AKSARUDIN ADAM
NIM	:	20302400387
Program Studi	:	Magister Ilmu Hukum
Fakultas	:	Hukum

Dengan ini menyerahkan karya ilmiah berupa ~~Tugas Akhir/Skripsi/~~Tesis~~/Disertasi~~* dengan judul:

TINJAUAN HUKUM PENENTUAN LOCUS DELICTI DALAM PENYIDIKAN KEJAHATAN SIBER

dan menyetujuinya menjadi hak milik Universitas Islam Sultan Agung serta memberikan Hak Bebas Royalti Non-ekslusif untuk disimpan, dialihmediakan, dikelola dalam pangkalan data, dan dipublikasikannya di internet atau media lain untuk kepentingan akademis selama tetap mencantumkan nama penulis sebagai pemilik Hak Cipta.

Pernyataan ini saya buat dengan sungguh-sungguh. Apabila dikemudian hari terbukti ada pelanggaran Hak Cipta/Plagiarisme dalam karya ilmiah ini, maka segala bentuk tuntutan hukum yang timbul akan saya tanggung secara pribadi tanpa melibatkan pihak Universitas Islam Sultan Agung.

Semarang, 30 Oktober 2025

Yang Membuat Pernyataan.

(AKSARUDIN ADAM)

*Coret yang tidak perlu

KATA PENGANTAR

Puji Syukur tercurahkan kepada Tuhan Yang Maha Esa yang telah melimpahkan segala kemudahan dan kelancaran kepada Penulis, sehingga Penulis dapat menyelesaikan Tesis yang berjudul: **Tinjauan Hukum Penentuan *Locus Delicti* dalam Penyidikan Kejahatan Siber** yang dapat diselesaikan penulis secara tepat waktu.

Kejahatan siber dilakukan dalam *cyberspace*, dengan media internet sebagai perantara untuk melakukan kejahatan siber. Pelaku kejahatan siber dapat melakukan kegiatan kejahatan siber baik dari jarak dekat dari target kejahatan maupun dari jarak yang sangat jauh pun dapat dilakukannya kejahatan siber terhadap target korban kejahatan siber. Dari pernyataan tersebut dapat dilihat bahwa kejahatan siber dapat dilakukan dimana saja, kapan saja serta berdampak kemana saja, seakan-akan kejahatan siber dalam dunia siber tampak tanpa batas. Namun demikian kejahatan-kejahatan siber memiliki kompleksitas masing-masing ketika pemeriksaan pengadilan mengharuskan adanya *locus delicti* yang jelas. *Locus Delicti* ini penting karena selain undang-undang mengharuskan surat dakwaan menyebutkan *locus delicti* yang jelas, *locus delicti* juga penting untuk menentukan keberlakuan hukum, yurisdiksi atau kompetensi relatif. dalam penyidikan kejahatan siber, tempat kejadian perkara bisa berada di berbagai yurisdiksi, baik internasional maupun nasional, sehingga menimbulkan masalah dalam menentukan pengadilan yang berwenang.

Maksud dan tujuan dari penulisan ini adalah untuk melengkapi tugas-tugas dan memenuhi syarat guna menyelesaikan program Magister Hukum studi di Fakultas Hukum Universitas Islam Sultan Agung Semarang. Secara khusus tujuan penelitian ini adalah untuk mengetahui dan menganalisa (1) politik hukum pidana nasional dalam mengakomodir kejahatan siber, (2) skema penentuan *locus delicti* dalam penyidikan kejahatan siber, (3) problematika hukum dalam penentuan *locus delicti* pada penyidikan kejahatan siber.

Penulis menyadari bahwa penyusunan tesis ini tidak dapat selesai tanpa bantuan dan dukungan dari berbagai pihak, oleh karenanya dalam kesempatan yang baik ini penulis mengucapkan terima kasih yang tak terhingga kepada yang terhormat:

1. Prof. Dr. H. Gunarto, S.H., S.E. Akt., M.Hum., selaku Rektor Universitas Islam Sultan Agung Semarang;
2. Dr. H. Jawade Hafidz, SH., MH, selaku Dekan Fakultas Hukum Universitas Islam Sultan Agung Semarang sekaligus Pembimbing yang dengan penuh kepakaran, kebijaksanannya dan telah berkenan meluangkan waktu memberikan bimbingan kepada penulis untuk segera menyelesaikan penulisan tesis ini;
3. Dr. Andri Winjaya Laksana, S.H, M.H, selaku Ketua Program Studi Magister Illmu Hukum Fakultas Hukum Universitas Islam Sultan Agung Semarang;

4. Para Penguji Ujian Tesis, yang telah memberikan bimbingan dan petunjuk serta arahan demi sempurnanya tesis ini sebagai karya ilmiah yang dapat bermanfaat;
5. Dosen, yang telah memberikan ilmu yang tiada terhingga bagi diri penulis selama kuliah pada Program Magister Hukum Universitas Islam Sultan Agung Semarang;

Penulis berharap semoga tesis ini dapat bermanfaat bagi mahasiswa dan masyarakat pada umumnya dan civitas akademika Universitas Islam Sultan Agung Semarang pada khususnya.

Semarang, September 2025
Penulis

Aksarudin Adam

ABSTRAK

Dalam penyidikan kejahatan siber, tempat kejadian perkara bisa berada di berbagai yurisdiksi, baik internasional maupun nasional, sehingga menimbulkan masalah dalam menentukan pengadilan yang berwenang. Hal ini semakin diperumit dengan adanya Undang-Undang Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur tentang yurisdiksi tindak pidana siber dengan prinsip-prinsip yang berbeda, seperti prinsip teritorial, prinsip nasional, dan prinsip universal. Karena selalu terdapat perbedaan antara lokasi (*locus*) pelaku dengan lokasi akibat yang ditimbulkan.

Tujuan Penelitian ini adalah untuk mengetahui dan menganalisa (1) politik hukum pidana nasional dalam mengakomodir kejahatan siber, (2) skema penentuan *locus delicti* dalam penyidikan kejahatan siber, (3) problematika hukum dalam penentuan *locus delicti* pada penyidikan kejahatan siber.

Metode pendekatan yang digunakan dalam penelitian ini adalah yuridis normatif. Spesifikasi penelitian ini bersifat deskriptif analitis. Sumber data yang digunakan adalah data sekunder. Data sekunder adalah data yang diperoleh dari penelitian kepustakaan yang terdiri dari bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier.

Berdasarkan hasil penelitian dapat disimpulkan: (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diperbarui melalui Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024, menjadi produk politik hukum nasional dalam mengakomodir norma hukum pidana terhadap beberapa jenis kejahatan siber yang terjadi di Indonesia. (2) Locus delicti ini tidak ada ketentuannya di dalam produk hukum nasional yang berkaitan dengan penanganan kejahatan siber yaitu UU ITE dan KUHAP. Dalam menentukan locus delicti dalam tindak pidana cyber crime yaitu sama atau relevan dengan teori penentuan tempat kejadian pada tindak pidana konvensional yaitu berdasarkan pendapat para ahli hukum pidana (doktrin). (3) Dalam penentuan locus delicti pada proses penyidikan kejahatan siber memiliki problematika dalam aspek yurisdiksi, yang mana tindak pidana cyber crime ini merupakan tindak pidana yang pelaku dan korban tidak hanya di negara yang sama dan juga tidak selalu berkewarganegaraan yang sama yakni tindak pidana cyber crime ini juga merupakan tindak pidana transnasional, pada sistem hukum pidana yang berlaku saat ini, hukum pidana pada umumnya hanya berlaku di wilayah negaranya sendiri (asas teritorial) dan untuk warga negaranya sendiri (asas personal/nasional aktif), hanya delik-delik tertentu yang dapat digunakan asas nasional pasif dan asas universal yang mana delik-delik tersebut termasuk kejahatan cyber crime.

Kata Kunci: Locus Delicti, Penyidikan, Kejahatan Siber.

ABSTRACT

In cybercrime investigations, the crime scene can be located in various jurisdictions, both international and national, creating challenges in determining the competent court. This is further complicated by the Electronic Information and Transactions Law (UU ITE), which regulates the jurisdiction of cybercrimes with different principles, such as territorial, national, and universal principles. This is because there is always a difference between the location (locus) of the perpetrator and the location of the resulting consequences.

The aim of this research is to determine and analyze (1) national criminal law policy in accommodating cybercrime, (2) the scheme for determining the locus delicti in cybercrime investigations, (3) legal problems in determining the locus delicti in cybercrime investigations.

The approach method used in this research is normative juridical. The specifications of this research are analytical descriptive. The data source used is secondary data. Secondary data is data obtained from library research consisting of primary legal materials, secondary legal materials and tertiary legal materials.

Based on the research results, it can be concluded: (1) Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which was later updated through Law Number 19 of 2016 and Law Number 1 of 2024, became a national legal policy product in accommodating criminal law norms regarding several types of cyber crimes that occur in Indonesia. (2) There are no provisions for this locus delicti in national legal products related to handling cyber crimes, namely the ITE Law and the Criminal Procedure Code. In determining the locus delicti in cyber crime, it is the same or relevant to the theory of determining the place of occurrence in conventional crimes, namely based on the opinions of criminal law experts (doctrine). (3) In determining the locus delicti in the process of investigating cybercrime, there are problems in the jurisdictional aspect, where this cyber crime is a crime where the perpetrator and victim are not only in the same country and are not always the same citizen, namely this cyber crime is also a transnational crime, in the current criminal law system, criminal law generally only applies in the territory of the country itself (territorial principle) and for its own citizens (active personal/national principle), only certain crimes can be used, namely the passive national principle and the universal principle, where these crimes include cyber crimes.

Keywords: Locus Delicti, Investigation, Cybercrime.

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Indonesia adalah negara yang berdasarkan hukum, yang bermakna bahwa Negara Indonesia adalah Negara hukum sebagaimana tercantum di dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.[1] Hukum memiliki arti penting dalam setiap aspek kehidupan, pedoman tingkah laku manusia dalam hubungannya dengan manusia yang lain, dan hukum yang mengatur segala kehidupan masyarakat Indonesia.

Setiap tindakan warga negara diatur dengan hukum, setiap aspek memiliki aturan, ketentuan dan peraturannya masing-masing. Hukum menetapkan apa yang harus dilakukan, apa yang boleh dilakukan serta apa yang dilarang. Salah satu bidang dalam hukum adalah hukum pidana yaitu mengatur tentang aturan perbuatan-perbuatan tertentu yang dilarang. Sedangkan tindak pidana, merupakan perbuatan yang dilarang oleh suatu aturan hukum yang mana disertai ancaman (sanksi).[2]

Hukum pidana di Indonesia menurut catatan sejarah mengalami perubahan yang sangat signifikan, karena sejalan dengan perkembangan sosial budaya masyarakat

[1] Anirut Chuasanga and Ong Argo Victoria, Legal Principles Under Criminal Law in Indonesia Dan Thailand, *Jurnal Daulat Hukum*, 2 (1), March 2019, h 131

[2] Sulistiyawan Doni Ardiyanto, Eko Soponyono, and Achmad Sulchan, Judgment Considerations Policy in Decree of the Court Criminal Statement Based On Criminal Destination, *Jurnal Daulat Hukum*: 3 (1), March 2020, h 180

di mana hukum tersebut diberlakukan. Dalam kaitan itu, hukum selalu berubah-ubah karena kejahatan yang terjadi juga berubah-ubah dan cenderung mengalami perkembangan.

Untuk menjawab problematika tersebut dibutuhkan perangkat hukum yang memadai guna mengakomodasi kekosongan hukum yang disebabkan adanya kejahatan-kejahatan baru yang belum terakomodir dalam undang-undang. Sejalan dengan hal tersebut, kejahatan yang bersifat tradisional terus berkembang seiring dengan perubahan zaman yang terus maju, sehingga penegakan hukum (*law an forcement*) tidak mengalami kesulitan dalam melakukan proses penegakannya.

Peradaban manusia mengalami perubahan drastis dalam dekade pada penghujung Abad ke-19. Perubahan tersebut terutama menyangkut interaksi dan pergaulan yang tidak terbatas dengan menggunakan media telekomunikasi. Dalam tata pergaulan dunia yang baru itu, tidak terlihat lagi sekat-sekat atau batas suatu negara. Tidak lagi dipersoalkan warna kulit, ras dan golongan. Karena tidak lagi mengindahkan jarak dan waktu, hubungan dapat dilakukan kapan saja, di mana saja dan dari mana saja. Hal inilah yang dikenal sebagai hubungan global.[3]

Indonesia merupakan bagian dari tata pergaulan hubungan global tersebut. Sebagai masyarakat global, manusia harus melaksanakan pemahaman dunia dalam tatanan yang baru, sehingga dalam mewujudkan negara yang maju harus mampu

[3] Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya*, Cet. I; Yogyakarta: Laksbang Pressindo, 2007, h. 1.

menempatkan dan memosisikan diri sebagai negara yang siap dan mampu dalam menghadapi persaingan global.

Perkembangan teknologi membawa perubahan dengan munculnya teknologi informasi elektronik berupa sistem komputer. Salah satu karya dibidang teknologi informasi dalam sistem komputer yang membawa perubahan besar pada abad ke20 ini diantaranya adalah internet (*International Network*). Dengan internet masyarakat dapat mengakses beragam informasi, berkomunikasi, berbelanja, hingga melakukan transaksi keuangan secara tidak langsung melalui media elektronik. Dengan berbagai kemudahan serta manfaat positif yang diberikan oleh perkembangan teknologi informasi tersebut, tak luput juga terdapat dampak negatif dari kemajuan teknologi informasi, yakni munculnya kejahatan dalam dunia maya atau kejahatan siber (*cybercrime*). Cybercrime merupakan suatu aktivitas kejahatan yang berhubungan dengan dunia maya (*cyberspace*) dan komputer yang berbasis pada kecanggihan perkembangan teknologi internet sebagai media utama untuk melangsungkan kejahatan.[4]

Supremasi hukum di Indonesia tidak terlepas dari perkembangan teknologi saat ini. Kemajuan teknologi dapat dianggap sebagai pedang bermata dua yang dapat memberikan manfaat atau menimbulkan masalah dalam kehidupan sehari-hari. Hal ini menyebabkan aktivitas kriminal di dunia maya semakin bervariasi dan meluas.[5] Secara

[4] Sahat Maruli, *Cyber Law,* Cet.1, Cakra, Bandung, 2020, h 23

[5] K. Permata, dkk. Analisis Yuridis dalam Fenomena Revenge Porn di Indonesia dan Upaya Perlindungan Hukum terhadap Korban. *Jurnal Pendidikan Tambusai*, 8 (1) 2024, h 5512

umum kejahatan siber adalah kejahatan yang dilakukan oleh seseorang, sekelompok orang dan korporasi (badan hukum) dengan cara menggunakan atau dengan sasaran komputer atau sistem komputer atau jaringan komputer. Kejahatan ini terjadi di dunia maya (*virtual*) sehingga mempunyai karakteristik yang berbeda dengan kejahatan tradisional. Kejahatan siber (*cybercrime*) merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif yang sangat luas bagi seluruh bidang kehidupan modern saat ini.[6]

Kejahatan siber merupakan kejahatan dengan cara memanipulasi komputer dan/atau sistem komputer dengan cara apapun yang dilakukan dengan itikad buruk untuk memperoleh uang, barang atau keuntungan lainnya atau dimaksudkan untuk menimbulkan kerugian kepada pihak lain.[7] Kejahatan siber dapat muncul karena adanya kelemahan dan celah pada sistem komputer. Kelemahan dan celah tersebut yang dimanfaatkan oleh para pelaku kejahatan siber. Pelaku kejahatan siber ada beberapa jenis serta tujuan tertentu, seperti *cracker* yang bertujuan untuk merugikan pihak korban demi keuntungan diri sendiri atau kelompok *cracker* dengan cara mencari celah atau mencari kelemahan pada sistem komputer dari target lalu mengambil keuntungan dari kelemahan sistem tersebut. Namun ada seorang atau sekelompok orang yang menggunakan cara yang sama, yaitu mencari kelemahan dan celah dari

[6] Lastary Okvania, dkk. Analisis Putusan Pengadilan Negeri Payakumbuh Nomor 4/Pid.Sus/2022/PN Pyh dengan Putusan Mahkamah Agung Republik Indonesia Tentang Tindakan Pidana Konten Asusila lewat Media WhatsApp, *Unes Law Review*, 5 (4) Juni 2023, h 3532

[7] Sarah Barber, Westminster Hall Debate on the Computer Misuse Act 1990. *House of Commons Library*, 2022, h 2

sistem komputer, tetapi untuk membantu pihak pemilik sistem komputer untuk membenahi sistem komputer agar memperkuat sistem keamanan pada komputer tersebut, yakni *hacker*.

Dari kedua pengertian diatas dapat dipahami bahwa pencari celah pada sistem komputer terdapat dua sisi yang sering diistilahkan sebagai *hacker* sebagai *white hat* dan *cracker* sebagai *black hat*. Melihat beberapa pernyataan diatas, bahwa kejahatan siber dapat menyebabkan kerugian terhadap pihak korban dari kejahatan siber. Banyak macam dari tindakan kejahatan siber yang dilakukan oleh pelaku cracker, beberapa diantaranya ialah *Phishing*, *Carding, Cyberstalking, Malware attack, Cyber Espionage*, dan sebagainya.[8]

Kejahatan siber sendiri tidak selalu pada target merugikan pihak lain atau korban, namun ada pula bentuk tindakan kejahatannya yang sebelumnya sudah ada praktik kejahatan tersebut sebelum adanya internet lalu diadopsi dan menjadi tindakan yang dilakukan secara *cyber* atau online. Tindakan yang dimaksudkan contohnya seperti judi online, penyebaran konten pornografi di internet, penyebaran berita palsu atau hoax, pencemaran nama baik, perdagangan anak dan sebagainya yang mana tindakan tersebut ter-*upgrade* praktiknya dengan perantara internet.

Kejahatan siber dilakukan dalam *cyberspace*, dengan media internet sebagai perantara untuk melakukan kejahatan siber. Pelaku kejahatan siber dapat melakukan kegiatan kejahatan siber baik dari jarak dekat dari target kejahatan maupun dari jarak

[8] Daniel F. T. Popal, Upaya Penanggulangan Tindak Pidana Mayantara (Cybercrime), *Lex Administratum*, XII (5) September 2023, h 2

yang sangat jauh pun dapat dilakukannya kejahatan siber terhadap target korban kejahatan siber. Biasanya pelaku kejahatan siber melakukannya tanpa kekerasan, meminimalisir kontak fisik dengan target dengan menggunakan peralatan dan teknologi yang mumpuni serta memanfaatkan jaringan internet untuk melakukan kejahatan siber.[9] Dari pernyataan tersebut dapat dilihat bahwa kejahatan siber dapat dilakukan dimana saja, kapan saja serta berdampak kemana saja, seakan-akan kejahatan siber dalam dunia siber tampak tanpa batas.

Secara sosiologis, kita melihat bagaimana masyarakat menghadapi dampak kejahatan siber dalam kehidupan sehari-hari, menciptakan kekhawatiran dan ketidakamanan. Dari perspektif filosofis, penting untuk menjelajahi relevansi nilai-nilai UUD NRI 1945 dalam menanggapi tantangan hukum yang berasal dari dunia digital yang terus berkembang. Secara yuridis, pergeseran paradigma kejahatan digital menuntut pemahaman mendalam tentang bagaimana undang-undang yang ada dapat beradaptasi untuk efektif menegakkan hukum dalam konteks kejahatan siber.

Kejahatan siber dimungkinkan adanya delik formal dan delik materiil. Delik formal adalah perbuatan seseorang yang memasuki komputer milik orang lain tanpa ijin, sedangkan delik materiil adalah perbuatan yang menimbukan akibat kerugian bagi orang lain. Dengan adanya kejahatan siber telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khusunya dalam jaringan internet maupun intranet. Namun demikian

[9] Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, ctk. Kedua, PT Refika Aditama, Bandung, 2009, h 27.

kejahatan-kejahatan siber memiliki kompleksitas masing-masing ketika pemeriksaan pengadilan mengharuskan adanya *locus delicti* yang jelas. *Locus Delicti* ini penting karena selain undang-undang mengharuskan surat dakwaan menyebutkan *locus delicti* yang jelas, *locus delicti* juga penting untuk menentukan keberlakuan hukum, yurisdiksi atau kompetensi relatif. Padahal dalam kasus-kasus cyber crime, penentuan *locus delicti* tidak sesederhana pada kasus-kasus kejahatan tradisional atau kejahatan yang lainnya.

Dalam hukum pidana, penentuan *locus* menjadi instrumen penting dalam menyelesaikan suatu perkara terutama untuk penegak hukum. *Locus Delicti* sendiri merupakan tempat terjadinya atau dilakukan suatu tindak pidana, Dalam kasus kejahatan siber, *locus* menjadi aspek krusial serta kompleks, mengingat kejahatan ini dilakukan melalui internet yang dapat dilakukan kapanpun serta dimanapun, hal ini menyebabkan penentuan *locus* menjadi hal yang sulit bagi aparat penegak hukum. Serta kemudahan akses internet saat ini menyebabkan mudahnya suatu dokumen atau informasi dapat dirubah yang dimana hal ini dapat memberikan pengaruh secara langsung terhadap proses penyidikan dalam penentuan *locus delicti*.[10]

Secara implikatif penyidikan kejahatan siber yang mana pada prinsipnya penentuan *locus delicti* sangat penting karena berpengaruh langsung terhadap kompetensi pengadilan yang akan berwenang mengadili kasus tersebut. Pasal 84-86

[10] Muhammad Adrian Fitra Yamazaki. Analisis Prosedural Penegakan Hukum Pidana dalam Situasi Pandemi Covid-19 Penyesuaian Terhadap Ancaman Kejahatan Yang Timbul Akibat Pandemi Covid-19. *Jurnal Hukum dan Kewarganegaraan*, 6 (7) 2024, h 1-6

Kitab Undang-Undang Hukum Acara Pidana (Selanjutnya disebut KUHAP) mengatur bahwa pengadilan negeri berwenang mengadili segala perkara berdasarkan tempat kejadian perkara.

Namun, dalam penyidikan kejahatan siber, tempat kejadian perkara bisa berada di berbagai yurisdiksi, baik internasional maupun nasional, sehingga menimbulkan masalah dalam menentukan pengadilan yang berwenang. Hal ini semakin diperumit dengan adanya Undang-Undang Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur tentang yurisdiksi tindak pidana siber dengan prinsip-prinsip yang berbeda, seperti prinsip teritorial, prinsip nasional, dan prinsip universal. Karena selalu terdapat perbedaan antara lokasi (*locus*) pelaku dengan lokasi akibat yang ditimbulkan. Bahkan tidak jarang tindakan seorang pelaku yang berada di suatu negara tertentu, menimbulkan akibat dari perbuatannya tersebut di negara lain.

Berdasarkan latar belakang masalah di atas, maka penulis tertarik untuk membahas lebih konkrit mengenai kajian secara yuridis atas pelaksanaan penyidikan kejahatan siber dengan penentuan tempat terjadinya tindak pidana tersebut yang mana penulis menuangkannya dalam penelitian berjudul: "*Tinjauan Hukum Penentuan Locus Delicti dalam Penyidikan Kejahatan Siber*".

B. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas maka permasalahan penelitian ini adalah:

1. Bagaimana politik hukum pidana nasional dalam mengakomodir kejahatan siber?
2. Bagaimana skema penentuan locus delicti dalam penyidikan kejahatan siber?
3. Apa problematika hukum dalam penentuan locus delicti pada penyidikan kejahatan siber?

C. Tujuan Penelitian

Adapun yang menjadi tujuan dalam penulisan tesis ini yang bertujuan sebagai berikut:

1. Untuk mengetahui dan menganalisis politik hukum pidana nasional dalam mengakomodir kejahatan siber;
2. Untuk mengetahui dan menganalisis skema penentuan locus delicti dalam penyidikan kejahatan siber;
3. Untuk mengetahui dan menganalisis problematika hukum dalam penentuan locus delicti pada penyidikan kejahatan siber.

D. Manfaat Penelitian

Penelitian ini dilaksanakan dalam rangka penyusunan tesis dan hasil pada penelitian ini diharapkan mempunyai manfaat dari segi teoris atau akademisi maupun segi praktis yaitu:

1. Manfaat Teoritis

   Untuk menambah khasanah keilmuaan bagi para akademisi dalam pengembangan ilmu hukum pidana terkait dengan tinjauan hukum penentuan *locus delicti* dalam penyidikan kejahatan siber;

2. Manfaat Praktis

   a) Bagi Penegak Hukum

      Untuk menambah pengetahuan terkait tinjauan hukum penentuan *locus delicti* dalam penyidikan kejahatan siber;

   b) Bagi Masyarakat Secara Umum

      Untuk menambah pengetahuan terkait tinjauan hukum penentuan *locus delicti* dalam penyidikan kejahatan siber.

E. Kerangka Konseptual

1. Tinjauan

Tinjauan berasal dari kata "tinjau" yang artinya mempelajari dengan cermat. Kata tinjau mendapat akhiran "-an" menjadi tinjauan yang artinya perbuatan meninjau. Pengertian tinjauan adalah mempelajari dengan cermat, memeriksa (untuk memahami), pandangan, pendapat (sesudah menyelidiki, mempelajari, dan sebagainya). Tinjauan adalah kegiatan merangkum sejumlah data besar yang masih mentah kemudian mengelompokan atau memisahkan komponen-komponen serta bagian-bagian yang relevan untuk kemudian mengkaitkan data yang dihimpun untuk menjawab permasalahan. Tinjauan merupakan usaha untuk menggambarkan pola-pola

secara konsisten dalam data sehingga hasil analisis dapat dipelajari dan diterjemahkan dan memiliki arti.[11] Tinjauan dapat diartikan sebagai kegiatan pengumpulan data, pengolahan, dan analisa sebagai sistematis.

2. Hukum

Pengertian hukum belum *communis opinio doktorum* (tercapai kesepakatan pendapat) dan kata-kata Immanuel Kant kurang lebih seratus lima puluh tahun yang lalu masih berlaku sampai sekarang, yaitu *Noch suchen die Juristen eine Definition zu ihrem Begriffe von Recht* (yang kalau diterjemahkan bebas kira-kira artinya adalah tidak ada satu pun definisi hukum yang memuaskan atau masih juga para sarjana hukum mencari-cari suatu definisi tentang hukum).[12] Menurut Utrecht, hukum adalah himpunan peraturan-peraturan (perintah-perintah dan larangan-larangan) yang mengurus tata tertib suatu masyarakat dan karenanya harus ditaati oleh masyarakat itu.

3. *Locus Delicti*

Locus Delicti, *Locus* (Inggris) yang berarti lokasi atau tempat, secara istilah yaitu berlakunya hukum pidana yang dilihat dari segi lokasi terjadinya perbuatan pidana. Locus delicti perlu diketahui untuk (a) menentukan apakah hukum pidana Indonesia berlaku terhadap perbuatan pidana tersebut atau tidak; (b) menentukan kejaksaan dan pengadilan mana yang harus mengurus perkaranya (kompetensi relative).[13] Menurut Van Hamel yang dianggap sebagai locus delicti adalah (1) tempat

[11] Surayin, *Analisis Kamus Umum Bahasa Indonesia*, Bandung, Yrama Widya, 2005, h 10
[12] L.J. Van Apeldoorn, *Pengantar Ilmu Hukum*, Djakarta : Noor Komala, 1962, h 13.
[13] Adami Chazawi, *Pelajaran Hukum Pidana*, Raja Grafindo Persada, Jakarta 2002, h 70

di mana seorang pelaku itu telah melakukan sendiri perbuatannya; (2) tempat di mana alat yang telah dipergunakan oleh seorang pelaku itu bekerja; (3) tempat di mana akibat langsung dari sesuatu tindakan itu telah timbul; (4) tempat di mana sesuatu akibat konstitutif itu telah diambil.

4. Penyidikan

Penyidikan merupakan tahapan penyelesaian perkara pidana setelah penyelidikan yang merupakan tahapan permulaan mencari ada atau tidaknya tindak pidana dalam suatu peristiwa. Ketika diketahui ada tindak pidana terjadi, maka saat itulah penyidikan dapat dilakukan berdasarkan hasil penyelidikan. Pada tindakan penyelidikan, penekanannya diletakkan pada tindakan "mencari dan menemukan" suatu "peristiwa" yang dianggap atau diduga sebagai tindakan pidana. Sedangkan pada penyidikan titik berat penekanannya diletakkan pada tindakan "mencari serta mengumpulkan bukti". Penyidikan bertujuan membuat terang tindak pidana yang ditemukan dan juga menentukan pelakunya.[14]

5. Kejahatan Siber

Kejahatan siber atau cybercrime menurut Menurut *The U.S. Dept.of Justice*, *computer crime* adalah indakan ilegal apapun yg memerlukan pengetahuan tentang teknologi komputer untuk perbuatan jahat. Menurut Freddy haris, cybercrime merupakan suatu tindak pidana dengan karakteristik-karakteristik sebagai berikut (1) *Unauthorized access* (dengan maksud untuk memfasilitasi kejahatan); (2)

[14] Bambang Poernomo. *Asas-Asas Hukum Pidana*. Yogyakarta. Seksi Kepidanaan Fakultas Hukum Universitas Gajah Mada, 1996. h.57

Unauthorized alteration or destruction of data; (3) Mengganggu atau merusak operasi komputer; (4) Mencegah atau menghambat akses pada komputer.[15]

F. Kerangka Teori

1. Teori Bekerjanya Hukum

Robert Seidman memakai teori tentang bekerjanya hukum untuk melakukan analisis tentang pembentukan hukum dan juga analisis terhadap implementasi hukum. Pembentukan hukum dan implementasinya tidak lepas dari pengaruh sosial dan personal terutama pengaruh sosial politik. Kualitas dan karakter hukum juga tidak lepas dari pengaruh personal tersebut terutama kekuatan politik pada saat hukum itu dibentuk. Teori bekerjanya hukum yang dirumuskan Robert Seidman yang dikutip Rahardjo adalah sebagai berikut:

1) Bagaimana seseorang pemegang peran diharapkan untuk bertindak ditunjukkan dalam setiap peraturan hukum;
2) Setiap person pemegang peran dalam bertindak dan mengambil keputusan merespon peraturan hukum tergantung dan dikendalikan oleh peraturan hukum yang berlaku. Setiap sanksi dari aktivitas lembaga pelaksananya dan semua lingkungan kekuatan sosial, politik, dan lain sebagainya yang bekerja atas dirinya;

[15] Lita Sari Marita, Cyber Crime dan Penerapan Cyber Law dalam Pemberantasan Cyber Law di Indonesia, *Cakrawala: Jurnal Humaniora Universitas Bina Sarana Informatika*, 15 (2) 2015, h 2

3) Lembaga pelaksana menanggapi peraturan hukum dalam mengambil langkah tergantung dan dikendalikan oleh peraturan hukum yang berlaku. Setiap sanksi dari aktivitas Lembaga pelaksananya dan semua lingkungan kekuatan sosial, politik, dan lain sebagainya yang bekerja atas dirinya juga dari umpan balik yang datang dari pemegang peran dan birokrasi;
4) Langkah yang akan ditempuh oleh lembaga pembuat undangundang (legislatif) untuk menanggapi regulasi hukum akan ditentukan berfungsinya peraturan hukum yang berlaku. Mulai dari setiap sanksi dari seluruh kompleks kekuatan sosial, politik, dan lain sebagainya yang bekerja atas mereka juga merupakan umpan balik yang datang dari pemegang peran dan birokrasi.[16]

Hukum harus dapat berfungsi dengan baik agar hak masyarakat mendapatkan kesejahteraan dapat terpenuhi. [17] Menurut Sorjono Soekanto untuk memahami bagaimana fungsi hukum itu, tidak dapat lepas dari aspek penegakan hukum, yakni pelaksanaan suatu kebijakan atau suatu komitmen yang bersangkutan dengan 5 faktor pokok yaitu:

a. Faktor hukumnya sendiri yang merupakan dasar kebijakan;
b. Faktor penegak hukum, yakni pihak-pihak yang membentuk maupun menerapkan hukum;
c. Faktor sarana atau fasilitas yang mendukung penegakan hukum;
d. Faktor masyarakat, yakni lingkungan dimana hukum berlaku atau diterapkan;

[16] Satjipto Rahardjo, *Ilmu Hukum,* Alumni, Bandung, 1992, h. 21
[17] C.S.T. Kansil, *Pengantar Ilmu Hukum*, Balai Pustaka, Jakarta, 2002, h 7.

e. Faktor budaya, yakni sebagai hasil kerja, cipta dan rasa yang didasarkan pada karsa manusia di dalam pergaulan hidup.[18]

Dalam perspektif sosial, hukum bekerja bukan pada ruang yang hampa.[19] Terdapat hubungan resiprositas antara hukum dengan variabelvariabel lain dalam masyarakat. "Di samping hukum berfungsi sebagai alat untuk pengendalian sosial (*as a tool of social control*) hukum juga dapat dimanfaatkan sebagai sarana untuk rekayasa sosial (*as a tool of social engineering*) sebagaimana dideskripsikan oleh Roscou Pound".[20]

Bekerjanya hukum dalam masyarakat melibatkan beberapa unsur atau aspek yang saling memiliki keterkaitan sebagai suatu sistem. Beberapa aspek tersebut yaitu:

Lembaga Pembuat Hukum (*Law Making Institutions*), Lembaga Penerap Sanksi, Pemegang Peran (*Role Occupant*) serta Kekuatan Sosietal Personal (*Societal Personal Force*), Budaya Hukum serta unsur-unsur Umpan Balik (*feed back*) dari proses bekerjanya hukum yang sedang berjalan.[21]

Lebih lanjut menurut Muladi, ada tiga faktor yang mempengaruhi efektifitas penegakan hukum yaitu: (1) Adanya strategi penegakan hukum yang tepat dan dirumuskan secara komprehensif dan integral; (2) Adanya kehendak politik untuk

[18] Soerjono Soekanto, *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum*, PT. Raja Grafindo, Jakarta 1993, h 5

[19] Fithriatus Shalihah, *Buku Ajar Sosiologi Hukum*, Fakultas Hukum Universitas Islam Riau, Pekanbaru, 2015, h 72

[20] Ronny Hanitijo Soemitro, *Perpektif Sosial dalam Pemahaman Masalah-Masalah Hukum*, CV Agung, Semarang, 1989, h 23

[21] Muladi, Demokratisai, *Hak Asasi Manusia, dan Reformasi Hukum di Indonesia*, The Habibie Centre, Jakarta, 2002, h 27

melaksanakan strategi tersebut; (3) Adanya "pressure" dalam bentuk pengawasan masyarakat.[22]

Bekerjanya hukum juga dapat diartikan sebagai kegiatan penegakan hukum.[23] Penegakan hukum pada hakikatnya merupakan suatu proses untuk mewujudkan tujuan-tujuan hukum menjadi kenyataan. Namun demikian "penegakan hukum dinilai masih lemah". Lemahnya penegakan hukum ini terlihat dari yang masyarakat tidak menghormati hukum, demikian pula kewibawaan aparat penegak hukum yang semakin merosot sehingga tidak lagi dapat memberikan rasa aman dan tenteram.[24]

Konsepsi operasional tentang bekerjanya hukum dalam masyarakat dengan didasarkan pada dua konsep yang berbeda, yaitu "konsep tentang ramalan-ramalan mengenai akibat-akibat (*prediction of consequences*) yang dikemukakan oleh Lundberg dan Lansing tahun 1973 dan konsep Hans Kelsen tentang aspek rangkap dari suatu peraturan hukum".

Berdasarkan konsep Lundberg dan Lansing, serta konsep Hans Kelsen tersebut Robert B. Seidman dan William J. Chambliss menyusun suatu Konsep Bekerjanya Hukum di dalam Masyarakat. Keberhasilan pelaksanaan suatu peraturan perundang-undangan sangat tergantung banyak faktor. Secara garis besar bekerjanya hukum dalam masyarakat akan ditentukan oleh beberapa faktor utama. Faktor tersebut meliputi

---

[22] *Ibid*, h 28

[23] Muladi dan Barda Nawawi Arief, *Pidana dan Pemidanaan*, Semarang, Banda Penyediaan Bahan Kuliah, 1984, h 91

[24] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, PT. Citra Aditya Bakti, Bandung, 2010, h 69

keseluruhan komponen sistem hukum, yaitu faktor substansial, faktor struktural dan faktor kultural.

2. Teori Positivisme Hukum

Banyak ahli pikir penganut ajaran positivisme hukum, salah satunya adalah H.L.A Hart, yang mengatakan bahwa hukum itu harus kongkrit, maka harus ada pihak yang menuliskan. Pengertian ”yang menuliskannya” itu menunjuk pengertian bahwa hukum harus dikeluarkan oleh suatu pribadi (subjek) yang memang mempunyai otoritas untuk menerbitkan dan menuliskannya. Otoritas tersebut adalah negara. Otoritas negara ditunjukan dengan adanya atribut negara, berupa kedaulatan negara. Berdasarkan kedaulatannya, secara internal negara berwenang untuk mengeluarkan dan memberlakukan apa yang disebut sebagai hukum positif. Selanjutnya H.L.A. Hart, mengatakan : (1) hukum (yang sudah dikonkritisasi dalam bentuk hukum positif) harus mengandung perintah; (2) tidak selalu harus ada kaitanya antara hukum dengan moral dan dibedakan dengan hukum yang seharusnya diciptakan (*there is no necessary connection between law and morals or law as it ought so be*).[25]

Pendapat Hart yang dipaparkan pada butir (2) mengindikasikan tolakkan dari Hart bahwa hukum harus bersumber dari sesuatu yang abstrak. Ini adalah konsekuensi logis cara berpikir dalam ajaran positivisme, yang bersumber dari hubungan sebab akibat suatu gejala dengan gejala lain secara kongkrit (kasat mata). Oleh karenanya

[25] Teguh Prasetyo dan Abdul Hakim Barkatullah, *Ilmu Hukum dan Filsafat Hukum*, Yogyakarta, Pustaka Pelajar, 2007, h 97-99.

pertimbangan-pertimbangan moral tidak harus terkait dengan terbitnya hukum positif, karena pertimbangan moral bukanlah hal yang konkrit. Begitu kuatnya logika positivisme menjadi pedoman berpikir Hart, tercermin dari ajarannya bahwa "... *the analysis or study of legal consepts in an important study to be distinguished from historical inquiries, sociological inquiries and the critical appraisal of law is terms or moral, socials aims*...".[26]

Cara pandang Hart di atas sama dengan cara pandang John Austin (1790- 1859) yang menyatakan bahwa norma hukum harus memuat; pemerintah, kewajiban dan sanksi. Terkait dengan perintah (*command*) harus memenuhi dua (2) syarat sebagaimana disampaikan John Austin[27], yakni:" *Command are laws if two conditions are satisfied: firts, they must be general: second they must be commended by what exists in very political society, whatever its contitutional form, namely, a or a group of person who are in receipt of habitual obedience from most of the society*...".

Terkait dengan realitas objektif, apakah benar kajian hukum positif bisa dipisahkan dari nilai-nilai tertentu seperti moral? Bukankah hukum positif dibuat dalam tatanan yang terikat pada ruang dan waktu, sehingga ada nilai-nilai tertentu yang akan mempengaruhinya? Bukankah nilai-nilai tertentu bahkan kepentingan-kepentingan tertentu dapat mengikat pembuat hukum maupun adressat hukum,

[26] Asep Bambang Hermanto, Ajaran Positivisme Hukum Di Indonesia: Kritik Dan Alternatif Solusinya, *Selisik*, 2 (4), Desember 2016, h 112

[27] David Dyzenhaus, Sophia Reibentanz Moreau and Arthur Ripstein (ed.), *Law and Morality; Readings in Legal Philosophy*. 3rd edition, Toronto, University of Toronto Press, 2007, h. 30-31.

sehingga harus dikatakan bahwa hukum positif pun terbit sebagai produk nilai-nilai tertentu.

HL.A Hart memecahkan hukum (dalam hal ini hukum positif) di dalam dua (2) bagian: pertama, primary rules, yaitu aturan aturan hukum yang secara langsung memberikan hak-hak dan kewajiban kepada orang per-orang. Aturan-aturan itu meliputi aturan hukum perdata dan hukum pidana. Kedua, *secondary rules*, yaitu aturan-aturan hukum yang memberikan hak-hak dan kewajiban kepada penguasa negara.[28]

Paparan di atas, seperti apa yang dikemukan oleh Hans Kelsen, mengatakan bahwa memecah hukum (dalam hal ini hukum positif) menjadi dua (2) bagian besar yaitu teori hukum murni dan *stufenbauttheory*. Kedua bahasan besar tersebut boleh dikatakan sebagai hasil reduksionis oleh Hans Kelsen, beberapa ajarannya yang terangkum dalam ajaran hukum murni (*the pure theory of law*) yang dipaparkan sebagai berikut:

1) Bahwa hukum harus dilepas dari moral, pertimbangan-pertimbangan yang abstrak, pertimbangan politik, ekonomi, dan faktor di luar hukum lainnya. Tujuan hukum adalah kepastian. Begitu kuatnya prinsip ini diajarkan oleh Hans Kelsen sehingga ia pun sampai pada pendapat bahwa ilmu hukum harus dipisahkan dari ilmu sosial. Seorang ahli hukum harus mepelajari hukum lepas dari ilmu-ilmu kemasyarakatan maupun kondisi sosial;

[28] Asep Bambang Hermanto, *Op.Cit*, 2 (4), Desember 2016, h 113

2) Bahwa hukum harus benar-benar objektif tanpa prasangka. Oleh karena itu Hans Kelsen dalam hal ini berbeda dengan HLA Hart maupun John Austin. Bagi Hans Kelsen aturan hukum bukanlah hasil dari perintah penguasa karena penguasa berpotensi memiliki kepentingan subjektif dan bisa memiliki agenda politik yang bisa menyebabkan aturan yang dibuat menjadi tidak objektif;
3) Keadilan adalah persoalah diwilayah "*ought to be*" (yang seharusnya), bukan "*is*" (yang ada). Dengan demikian bagi Hans Kelsen, keadilan bukan merupakan bagian dari kajian ilmu hukum positif. Keadilan adalah persoalan keharusan (ideal, apa yang seharusnya) tetapi bersifat metayuridis. Keadilan menurut Hans Kelsen merupakan persoalan bersifat tidak rasional (dalam terminologi positivisme, pen) yang tidak jelas batas-batasnya sehingga tidak dapat menjadi konsep yang memuaskan apabila dikaji dari apa yang oleh Hans Kelsen disebut ajaran hukum murni.[29]

Dari uraian ketiga pakar hukum tersebut, yaitu Hart, Autin maupun Kelsen, maka yang menjadi objek telaah kajian hukumnya adalah aturan hukum positif. Pertanyaannya adalah apakah ketika pecahan-pecahan itu disatukan akan menghasilkan aturan hukum sebagai satu kesatuan sistem? Apakah bagian-bagian yang dipecah-pecah (sebagaimana terlihat pada pendapat Hart, Austin, dan Kelsen) kalau disatukan kembali akan menghasilkan rangkuman yang utuh tentang hukum? Ini adalah pertanyaan pokoknya.

[29] *Ibid*

Pertanyaan-pertanyaan tersebut di atas, perlu mendapatkan jawaban karena berbeda dengan ajaran filsafat positivisme, objek pengaturan adalah manusia. Memang manusia adalah realitas tetapi manusia selalu terikat pada nilai-nilai tertentu, tatanan sosial tertentu. Hukum positif pun di dalam perkembangannya juga terikat pada nilai-nilai tertentu, bahkan kepentingan-kepentingan tertentu, karena terbitnya hukum positif sesungguhnya juga merupakan keputusan politik, yang mendasarkan pada panutan nilai-nilai tertentu. Dengan menyadari hal-hal seperti itu maka tidak serta merta reduksionisme dapat secara mudah dilakukan dalam kajian ilmu hukum.

Pertanyaannya yang mendasar adalah apakah mungkin, hukum positif itu "Bebas Nilai"?. Ciri dari positivisme berikutnya adalah objektif atau bebas nilai. Oleh karena itulah dalam paradigma positivisme ada dikotomi yang tegas antara fakta dengan nilai, dan mengharuskan subjek peneliti mengambil jarak terhadap realitas dengan sikap netral. Akan tetapi perilaku manusia dapat berubah sesuai dengan faktor yang mempengaruhinya. Fenomena sosial secara alamiah adalah subjektif dan tidak akan dapat dipahami sebagai sesuatu yang objektif. Sebenarnya sulit untuk mendeskripsikan mengenai perilaku manusia, terlebih digambarkan berdasarkan karakteristik eksternal. Karakteristik eksternal manusia bisa saja menimbulkan interpretasi yang beragam. Ilmu-ilmu sosial, dengan demikian akan selalu menjadi pengetahuan yang subjektif. Oleh karena itu yang sangat diperlukan adalah ada pemahaman sikap dan arti tindakan.

Seiring dengan perkembangan ilmu pengetahuan dan eksplorasi terus menerus dalam mencari kebenaran ilmiah, maka ajaran positivisme yang berpijak pada realitas,

objektivitas, netralitas dan menekankan pada fakta mulai dipertanyakan keabsahannya ketika cara berpikir positivisme harus diterapkan pada soal-soal kemasyarakatan. Dengan demikian, bahwa saintifikasi hukum modern sangat dipengaruhi oleh kemunculan paradigma positivisme di dalam ilmu pengetahuan modern. Modernitas bukan hanya mempengaruhi sains dan teknologi belaka, tetapi juga menjadi sumber perubahan pada kehidupan masyarakat, dan juga ilmu hukum.

Ilmu hukum yang dikembangkan dalam tradisi pemikiran positivisme dalam beberapa hal bertentangan dengan tradisi pemikiran hukum doktrinal yang tumbuh pada masa pra – positivisme, tidak serta merta indentik dengan tradisi pemikiran hukum doktrinal. Beberapa prinsip di dalam hukum positivisme bahkan bertentangan di dalam ilmu hukum doktrinal seperti ditunjukan dengan adanya ajaran fiksi hukum maupun kepastian hukum. Walaupun demikian dominasi saintifikasi hukum moderen masih didominasi hingga saat ini. Karakter utama sistem hukum modern adalah sifat rasionalitas. Rasionalitas ini ditandai oleh sifat peraturan hukum yang prosedural. Prosedural, dengan demikian menjadi dasar legalitas yang penting untuk menegakkan apa yang disebut keadilan, bahkan prosedur menjadi lebih penting dari pada bicara tentang keadilan itu sendiri. Di dalam konteks ini unpaya mencari keadilan (*searching for justice*) bisa menjadi gagal hanya karena terbentur dengan masalah prosedur. Hampir semua penangan kasus hak asasi manusia sesuai dengan prosedur hukum yang berlaku, demikian ungkapan yang merepresentasikan tanpa pentingnya prosedur demi terjamin rasionalitas hukum. Sebaliknya segala bentuk upaya lain mencari kebenaran

dalam upaya menegakkan keadilan, di luar peraturan hukum yang berlaku, tidak dapat diterima dan dianggap sebagai *out of legal thought*, bahkan bisa disebut ilegal.[30]

Pada sistem hukum modern, keadilan sudah dianggap diberikan dengan membuat hukum positif, tetapi dalam praktik, penggunaaan paradigma positivisme hukum dalam hukum modern ternyata banyak menimbulkan kekakuan-kekakuan sedemikian rupa sehingga pencarian kebenaran (searching for the truth) dan keadilan (searching for justice) tidak pernah tercapai dikarenakan terhalang oleh tembok-tembok prosedural. Kejadiankejadian tersebut lebih memprihatikan, karena akibat menggunakan kacamata positivisme kaku dalam mengintepretasikan berbagai undang undang di Indonesia, maka berbagai kebijakan penegakkan hukum maupun putusan Hakim gagal untuk menghasilkan suatu keadilan yang substansial, melainkan hanya sekedar mampu menghasilkan keadilan yang prosedural.

Pelajaran yang dapat ditarik adalah bahwa formal justice yang ditegakan melalui hukum positif (undang-undang) di Indonesia yang dikatakan menjunjung tinggi rule of law, ternyata belum mampu mewujudkan keadilan yang substansial. Upaya untuk mewujudkan substansial justice bisa gagal karena terbentur prosedur yang harus dipenuhi dalam memenuhi legalitas sistem hukum modern. Dengan melalui undang undang, pihak-pihak tertentu dapat merusak hati nurani atau akal sehat yang bersifat genuine dibalik pernyataan" semua harus sesuai dengan hukum", namun ketika prosedur hakim tersebut dijalankan, ternyata pemenuhan rasa keadilan bisa terhalang

[30] Asep Bambang Hermanto, *Op.Cit*, 2 (4), Desember 2016, h 115

oleh prosedur ataupun formalitas yang justru diciptakan oleh hukum modern itu sendiri. Istilah supremasi hukum (*supremacy of law*) selalu diidentikan dengan undang undang, maka akibatnya persoalan hukum tereduksi menjadi sekedar persoalan ketrampilan teknis yuridis.

Kemudian, demi kepentingan profesional terjadilah sakralisasi terhadap hukum positif. Maka positivisme hukum harus dipertahankan dengan alasan supremasi hukum, sekalipun hukum positif membelenggu Indonesia dalam ketidak berdayaan mengungkap kasus-kasus yang mengantarkan Indonesia pada kemerosotan etika berbangsa. Oleh karena itu, yang sangat diperlukan saat ini adalah membentuk mental dan moral yang berintegritas. Sejalan dengan ungkapan Presiden Jokowi, dalam Nawa Cita adalah perlu "Revolusi Mental" atau sejalan dengan ucapan Presiden pertama Ir. Soekarno, bangsa ini perlu "*Nation and Character Building*". Penegakkan hukum bisa berjalan dengan baik dan keadilan dapat terwujud, maka yang menjadi prioritas utama adalah para penegak hukumnya yang bermoral dan berintegritas, bukan keberadaan undang undang nya terlebih dahulu atau yang diutamakan.[31]

G. Metode Penelitian

Terdapat beberapa cara atau metode yang digunakan penulis dalam menyusun tesis ini, sebelumnya perlu diketahui arti dari "metode" itu sendiri. Metode adalah teknik-teknik yang digeneralisasikan dengan baik agar dapat diterima atau digunakan

[31] *Ibid*, h 116

secara sama dalam satu disiplin, praktek, atau bidang disiplin dan praktek.

Dalam menyusun tesis ini harus didahului oleh sebuah riset atau penelitian, sebab dengan adanya sebuah penelitian diharapkan bisa mencapai sasaran yang ingin dicapai. Dengan metode penelitian yang akan digunakan dalam penelitian, memberikan gambaran mengenai pokok-pokok yang sangat cermat dan syarat-syarat yang sangat ketat pula, sehingga metode penelitian tersebut dapat menjaga agar pengetahuan yang didapat dari hasil penelitian tersebut mempunyai nilai ilmiah yang tinggi. Dengan demikian agar tesis ini dapat dipertanggungjawabkan nilai-nilai ilmiahnya.

Metode penelitian yang dipakai oleh penulis dalam penelitian ini adalah:

1. Metode Pendekatan

Untuk mengadakan pengkajian dalam penelitian ini penulis menggunakan metode yuridis normatif atau pendekatan hukum tertulis (perundang-undangan/*statute approach*). Pendekatan yuridis normatif adalah pendekatan yang dilakukan berdasarkan bahan hukum utama dengan cara menelaah teori-teori, konsep-konsep, asas-asas hukum serta peraturan perundang - undangan yang berhubungan dengan penelitianini. Pendekatan ini dikenal pula dengan pendekatan kepustakaan, yakni dengan mempelajari buku-buku, peraturan perundang - undangan dan dokumen lain yang berhubungan dengan penelitian ini.[32]

[32]Rony Hanitijo Soemitro, *Metodologi Penelitian Hukum dan Jurimetri*, Ghalia Indonesia, Jakarta, 1990, h 34

2. Spesifikasi Penelitian

Penelitian ini menggunakan spesifikasi penelitian secara deskriptif analisis atau yang bersifat pemaparan objek penelitian. Tujuan dari spesifikasi penelitian deskriptif yaitu untuk memperoleh gambaran yang lengkap tentang keadaan hukum yang berlaku di tempat tertentu dan pada waktu tertentu. Peristiwa hukum yang berlaku pada saat tertentu tersebut sangat bergantung pada situasi dan dinamika masyarakat yang berkembang.

3. Sumber Data

Data yang digunakan untuk penelitian ini adalah data sekunder. Data sekunder adalah data yang diperoleh dari penelitian kepustakaan yang terdiri dari bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier.

1. Bahan hukum primer tersebut terdiri dari:
    a. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
    b. Kitab Undang-Undang Hukum Pidana;
    c. Kitab Undang-Undang Hukum Acara Pidana;
    d. Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Republik Indonesia;
    e. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
2. Bahan hukum sekunder yaitu terdiri dari:
    a. Buku-buku;

b. Rancangan Undang-Undang;

c. Hasil penelitian ahli hukum;

d. Tesis, Skripsi, Disertasi.

3. Bahan hukum tersier yang terdiri dari:

a. Kamus Hukum;

b. Kamus besar bahasa Indonesia;

c. Pedoman ejaan yang disempurnakan;

d. Ensiklopedia.

4. Metode Pengumpulan Data

Untuk mendapatkan data dalam penelitian ini, digunakan metode pengumpulan data sebagai berikut:

Studi Pustaka atau Studi Dokumen

Metode pengumpulan data yang utama digunakan dalam studi pustaka adalah data sekunder yang diperoleh dari buku-buku kepustakaan, peraturan perundang-undangan, maupun pendapat-pendapat para ahli hukum.

5. Metode Analisis Data

Data yang telah diperoleh tersebut kemudian dianalisa dengan analisa kualitatif, yaitu analisa data dengan tidak menggunakan angka-angka, tetapi data yang diperoleh melalui penelitian. Analisa data secara kualitatif dilakukan dengan cara menelaah seluruh data yang tersedia dari berbagai sumber, yaitu dari dokumen pribadi, dokumen resmi, menguji data dengan konsep, teori Undang-Undang yang terkait, dimana dengan

metode ini diharapkan akan diperoleh data yang jelas mengenai pokok permasalahanya.

H. Sistematika Penulisan

Sistematika penulisan ini terbagi dalam 4 (empat) bab yaitu sebagai berikut:

BAB I, Pendahuluan, meliputi: Latar Belakang Masalah, Perumusan Masalah, Tujuan Penelitian, Manfaat Penelitian, Kerangka Konseptual, Kerangka Teori, Metode Penelitian, Sistematika Penulisan.

BAB II, Tinjauan Pustaka terdiri dari: Tinjauan Umum Penyidikan, Tinjauan Umum *Locus Delicti*, Tinjauan Umum Kejahatan Siber, Kejahatan Siber dalam Perspektif Hukum Islam.

BAB III Hasil Penelitian Dan Pembahasan, terdiri dari: (1) politik hukum pidana nasional dalam mengakomodir kejahatan siber, (2) skema penentuan locus delicti dalam penyidikan kejahatan siber, (3) problematika hukum dalam penentuan locus delicti pada penyidikan kejahatan siber.

BAB IV Penutup, terdiri dari: Kesimpulan, Saran.

BAB II

TINJAUAN PUSTAKA

A. Tinjauan Umum Penyidikan

Dalam menyelesaikan kasus acara pidana ada beberapa rangkaian tindakan salah satu nya yaitu penyidikan terhadap tindak pidana. Tahapan penyidikan adalah rangkaian penting yang harus dilaksanakan dalam menyelesaikan kasus pidana untuk mengungkapkan kasus tersebut layak atau tidak atas dugaan tindak pidana yang telah terjadi. Sehingga tahap penyidikan dalam proses hukum tidak dapat dipisahkan dari adanya ketentuan perundang-undangan yang mengatur mengenai tindak pidana.[33]

Berdasarkan Pasal 1 angka 2 KUHAP (Kitab Undang-Undang Hukum Acara Pidana) 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 menentukan tersangkanya.

Berdasarkan kutipan diatas dapat diberi kesimpulan bahwa penyidikan merupakan sekumpulan tindakan kepolisian atau pegawai negeri sipil tertentu untuk mencari dan mengumpulkan bukti sesuai cara yang diatur dalam kitab undang-undang hukum acara pidana, serta bukti yang didapatkan memberi titik terang suatu tindak

[33] Muhammad Dhika Silva Pradana. Proses Penyidikan Terhadap Pelaku Tindak Pidana Kecelakaan Lalu Lintas Yang Mengakibatkan Korban Meninggal Dunia Di Kepolisian Resor Kota Pati, *Doctoral Dissertation*, Universitas Islam Sultan Agung Semarang. 2023. h 19.

pidana yang terjadi, dan juga penyidikan dilakukan untuk menemukan siapa pelaku tindak pidana.

Penyidikan merupakan tahapan penyelesaian suatu perkara pidana setelah dilakukan penyelidikan yang merupakan langkah pertama untuk mencari ada atau tidaknya tindak pidana dalam suatu peristiwa.[34] Apabila ditentukan telah terjadinya suatu tindak pidana, maka dapat dilakukan penyidikan berdasarkan hasil penyidikan.[35] Pada kegiatan penyelidikan, penekanannya diletakkan pada tindakan "mencari dan menemukan" suatu "peristiwa" yang dianggap atau diduga sebagai tindakan pidana. Sedangkan pada penyidikan titik berat penekanannya diletakkan pada tindakan "mencari serta mengumpulkan bukti" dan "menentukan tersangka".

Penyidikan adalah langkah panjang yang harus dilakukan oleh penyidik polri, langkah aplikasi pengetahuan tentang dua wilayah hukum, yaitu wilayah hukum yang normatif dan wilayah hukum yang progresif sosiologis. Wilayah hukum yang normatif diartikan bahwa polisi yang penyidik itu hanya mengikuti serangkaian peraturan perundang-undangan.

Kesimpulan dari pengertian diatas bahwa penyidikan merupakan kegiatan yang dilakukan oleh penyidik melalui serangkaian tindakan yang panjang. Dimana dalam melaksanakan penyidikan tersebut menggunakan hukum yang normatif, sehingga

[34] Joko Sriwidodo. *Pengantar Hukum Acara Pidana*. Cet.1. Yogyakarta. Penerbit Kepel Press. 2023. H 79

[35] *Ibid*

penyidikan melaksanakan sesuai dengan aturan hukum atau perundang-undangan itulah yang menjadi target atau ukuran selesainya proses hukum di tingkat penyidikan.

Menurut de Pinto, menyidik (*opsporing*) berarti "pemeriksaan permulaan oleh pejabat-pejabat yang untuk itu ditunjuk oleh undang-undang segera setelah mereka dengan jalan apapun mendengar kabar yang sekedar beralasan, bahwa ada terjadi sesuatu pelanggaran hukum". Sementara itu, Rahmadhan Kasim dan Apriyanti Nusa menyatakan bahwa filosofi tindakan penyidikan esensinya untuk mencari dan mengumpulkan bukti, yang dengan bukti tersebut ditemukan siapa tersangkanya.[36]

Dari kutipan tersebut dapat disimpulkan bahwa menyidik yaitu kegiatan yang dilakukan oleh pejabat-pejabat dengan mendengar telah terjadi suatu tindak pidana untuk dilakukan pemeriksaan permulaan sesuai dengan peraturan yang mengatur. Dan penyidikan memiliki fungsi dimana dilakukan penyidikan untuk mencari dan mengumpulkan bukti-bukti yang ada dalam tindak pidana yang terjadi sehingga dari bukti-bukti yang didapatkan ditemukan pelaku dalam tindak pidana tersebut.

Menurut Pasal 1 angka 1 KUHAP (Kitab Undang-Undang Hukum Acara Pidana) penyidik adalah Pejabat polisi Negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh undang-undang untuk melakukan penyidikan.

Penyidik pejabat polisi negara republik Indonesia karena kewajibannya dalam melaksanakan penyidikan memiliki wewenang sebagai berikut:

---

[36] Febri dan Yetisma Saini. *Hukum Acara Pidana Indonesia*. Sumbar. Penerbit LPPM Universitas Bung Hatta. 2022. h 30.

a. Menerima laporan atau pengaduan dari seorang tentang adanya tindak pidana;
b. Melakukan tindakan pertama pada saat di tempat kejadian;
c. Menyuruh berhenti seorang tersangka dan memeriksa tanda pengenal diri tersangka;
d. Melakukan penangkapan, penahanan, penggeledahan, dan penyitaan;
e. Melakukan pemeriksaan dan penyitaan surat;
f. Mengambil sidik jari dan memotret seorang;
g. Memanggil orang untuk didengar dan diperiksa sebagai tersangka atau saksi;
h. Mendatangkan orang ahli yang diperlukan dalam hubungannya dengan pemeriksaan perkara;
i. Mengadakan penghentian penyidikan;
j. Mengadakan tindakan lain menurut hukum yang bertanggung jawab.[37]

Wewenang yang disebutkan di atas merupakan kegiatan penyidik yang diatur dalam kitab undang-undang hukum acara pidana dalam melakukan penyidikan. Penyidik dalam melaksanakan tugas penyidikan harus berpegang teguh dengan wewenang yang telah diberikan oleh undang-undang sehingga tidak terjadinya penyimpangan wewenang yang dilakukan oleh penyidik dalam melaksanakan tugasnya.

Berdasarkan penjelasan Kitab Undang-Undang Hukum Acara Pidana (KUHAP), makna tindakan lain menurut hukum yang bertanggung jawab yaitu instansi

[37] Pasal 7 ayat 1 KUHAP

atau Lembaga penyidik diatas yang mempunyai fungsi yang sama dengan penyidik polri, mereka mempunyai kewenangan untuk menangkap dan menahan tersangka. Instansi atau Lembaga yang dimaksud yaitu Kejaksaan, Komisi Pemberantasan Korupsi (KPK), Imigrasi, Bea Cukai dan TNI Angkatan Laut.

Pada tahap penyelidikan, penekanan diletakkan pada "mencari dan menemukan suatu peristiwa tindak pidana". Sedangkan pada tahap penyidikan, penekanannya diletakkan pada tindakan "mencari dan mengumpukan bukti-bukti" agar tindak pidana menjadi terang serta agar dapat menemukan siapa pelakunya. Pada Pasal 184 Undang-Undang No.8 Tahun 1981 dalam hal mencari serta mengumpulkan alat-alat bukti yang sah meliputi keterangan saksi, keterangan ahli, surat, petunjuk, keterangan terdakwa.

B. Tinjauan Umum Locus Delicti

Locus Delicti, *Locus* (Inggris) yang berarti lokasi atau tempat, secara istilah yaitu berlakunya hukum pidana yang dilihat dari segi lokasi terjadinya perbuatan pidana[38] atau secara sederhana *locus delicti* adalah tempat terjadinya tindak pidana. *Locus Delicti*, atau yang sering disebut tempat kejadian perkara, adalah lokasi di mana tindak pidana terjadi dan digunakan untuk menentukan yurisdiksi pengadilan yang berwenang untuk memeriksa kasus tersebut.[39] *Locus delicti* perlu diketahui untuk:

1) Menentukan apakah hukum pidana Indonesia berlaku terhadap perbuatan pidana tersebut atau tidak.

[38] Adami Chazawi, *Pelajaran Hukum Pidana,* Raja Grafindo Persada, Jakarta 2002, h 70
[39] Teguh Prasetyo. *Hukum Pidana Edisi Revisi*. Jakarta. Raja Grafindo Persada, 2014. h 63

2) Menentukan kejaksaan dan pengadilan mana yang harus mengurus perkaranya (kompetensi relative).[40]

Pentingnya pemahaman terhadap berlakunya hukum pidana berdasarkan lokasi kejadian atau *Locus Delicti*, perlu disadari untuk:

a. Mempertimbangkan apakah perbuatan pidana tersebut tunduk pada yurisdiksi hukum pidana Indonesia, yang merujuk pada ketentuan Pasal 2-8 KUHP.
b. Memilih badan hukum yang tepat untuk menangani kasus tertentu adalah hal yang penting dan berkaitan dengan kewenangan yang sesuai.[41]

Ada banyak pendapat dari beberapa ahli mengenai *locus delicti* yaitu antara lain sebagai berikut: menurut Van Hattum, pemerintah berpendapat bahwa yang harus dipandang sebagai *locus delicti* itu adalah seorang pelaku telah melakukan kejahatannya, dan bukan tempat kejahatan itu telah menimbulkan akibat. Profesor Van Bemmelen berpendapat bahwa yang harus dipandang sebagai *locus delicti* itu pada dasarnya adalah tempat seseorang pelaku telah melakukan perbuatannya secara material.[42]

Menurut Van Hamel yang dianggap sebagai *locus delicti* adalah:

1) Tempat di mana seorang pelaku itu telah melakukan sendiri perbuatannya.
2) Tempat di mana alat yang telah dipergunakan oleh seorang pelaku itu bekerja.
3) Tempat di mana akibat langsung dari sesuatu tindakan itu telah timbul.

---

[40] Aliefka Albiandro, Analisis Hukum dalam Menentukan Locus Delicti dalam Perkara Tindak Pidana Pemalsuan Akta Otentik, *JOM Fakultas Hukum Universitas Riau*, IX (1) Januari-Juni 2022, h 2

[41] Teguh Prasetyo. *Op. Cit*, 2014. h 85

[42] P.A.F Lamintang, *Dasar-Dasar Hukum Pidana*, Sinar Baru, Bandung, 2013, h 113

4) Tempat di mana sesuatu akibat konstitutif itu telah diambil.[43]

Moeljatno menjelaskan bahwa para ahli dalam menentukan manakah yang menjadi tempat terjadinya pidana berbeda pendapat, sehingga menimbulkan dua aliran, yaitu:

1) Aliran yang menentukan "di satu tempat", yaitu tempat dimana terdakwa melakukan perbuatan tersebut.
2) Aliran yang menentukan "di beberapa tempat", yaitu mungkin tempat perbuatan dan mungkin di tempat akibat.[44]

Moeljatno dalam bukunya menjelaskan bahwa aliran pertama dipelopori oleh Pompe dan Langemeyer yang mengatakan bahwa tempat kejahatan bukan ditentukan oleh tempat akibat dari perbuatan, melainkan ditentukan berdasarkan dimana terdakwa berbuat. Mengenai pandangan ini diperluas dengan tempat dimana alat yang dipergunakan oleh terdakwa berbuat, jika terdakwa menggunakan alat. Aliran yang kedua dianut oleh Simon, Van Hammel, Joker dan Bemelen yang menyatakan bahwa tempat perbuatan itu boleh dipilih antara tempat dimana perbuatan dimulai terdakwa sampai dengan perbuatan itu selesai dengan timbulnya akibat.

Maka terhadap penentuan *locus delicti* yang dilakukan oleh aparat penegak hukum harus tetap berpegang pada teori yang ada yaitu teori tempat dimana kejahatan dilakukan, teori perbuatan alat, teori alat yang digunakan dalam melakukan kejahatan, dan teori akibat yang di timbulkan atas delik pidana yang dilakukan oleh pelaku. Maka

[43] *Ibid*, h 180
[44] Moeljatno, *Asas-Asas Hukum Pidana*, Bina Aksara, Jakarta, 1987, h 78-79

dari itu penentuan *locus delicti* dalam suatu kejahatan khusus maupun kejahatan konvensional sama tidak ada perbedaan.

Parameter menentukan locus delicti menurut teori materiil. Perbuatan dan akibat yang ditimbulkan perbuatan terjadi di dalam suatu wilayah hukurn pengadilan negeri. Jika perbuatan dan akibat yang ditimbulkannya terjadi dalam suatu lingkungan daerah hukum pengadilan negeri, pengadilan negeri tersebutlah yang, berwenang untuk memeriksa dan mengadilinya. Disini kita lihat antara perbuatan dan akibat yang ditimbulkannya tidak terpecah dalam dua tempat yang berlainan.[45]

Penyebutan *locus delicti* penting untuk menakar kadar daluwarsa suatu perkara, jangan sampai terlewat waktu, unsur *locus* menentukan menentukan kompetensi pengadilan untuk mengadili. Selain itu dalam Kepolisian untuk mengungkap kejahatan dalam menentukan *locus delicti* perlunya pembuktian dan dukungan lainnya untuk melacak kejahatan tersebut dan alat khusus untuk melacak kejahatan tersebut dan dalam persidangan nanti jaksa juga perlu adanya saksi ahli untuk dihadapkan sebagai saksi di persidangan. Dalam persidangan pun penentuan *locus delicti* juga salah satu pertimbangan hakim juga dalam mengambil keputusan dalam suatu tindak pidana. Sehingga Hakim yang ditunjuk perlu cermat dalam mempelajari kembali tersebut agar nantinya mengerti kasus tersebut dan dapat memberikan putusan yang adil.

C. Tinjauan Umum Kejahatan Siber

[45] Aliefka Albiandro, *Op.Cit*, Januari-Juni 2022, h 11

Kejahatan siber atau kejahatan dunia maya (*cybercrime*) adalah sebuah bentuk kriminal yang mana menjadikan internet dan komputer sebagai medium melakukan tindakan kriminal. Masalah yang berkaitan dengan kejahatan jenis ini misalnya hacking, pelanggaran hak cipta, pornografi anak, dan eksploitasi anak. Juga termasuk pelanggaran terhadap privasi ketika informasi rahasia hilang atau dicuri, dan lainnya.

Menurut Widodo, bahwa *cybercrime* diartikan sebagai kegiatan seseorang, sekelompok orang, badan hukum yang memakai komputer bagaikan fasilitas melakukan kejahatan, dan sebagai sasaran (target).[46] Dalam definisi lain, kejahatan dunia maya adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit, confidence fraud, penipuan identitas, pornografi anak, dan lain-lain. Walaupun kejahatan dunia maya atau cybercrime umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional dimana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.

Kejahatan komputer mencakup berbagai potensi kegiatan ilegal. Umumnya, kejahatan ini dibagi menjadi dua kategori yaitu (1) Kejahatan yang menjadikan

[46] Miftakhur Rokhman Habibi dan Isnatul Liviani, Kejahatan Teknologi Informasi (Cybercrime) dan Penanggulangannya dalam Sistem Hukum Indonesia, *Al-Qānūn: Jurnal Pemikiran dan Pembaharuan Hukum Islam*, 23 (2) Desember 2020, h 404

jaringan komputer dan *device* secara langsung menjadi target; serta (2) Kejahatan yang terfasilitasi jaringan komputer atau *device*, dan target utamanya adalah jaringan komputer independen atau *device*. Adapun beberapa tipe kejahatan yang sering terjadi dalam dunia siber antara lain:

1) *Illegal acces*/*unauthorized access to computer system and service*

   Ini adalah bentuk kejahatan yang dilakukan dengan cara meretas/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, atau tanpa izin dari pemilik sistem jaringan komputer yang dimasukinya.

2) *Illegal contents*

   Memasukkan data atau informasi tentang hal yang tidak benar, tidak etis, serta dapat dianggap melanggar hukum atau mengganggu ketertiban umum kedalam internet, itu adalah suatu modus kejahatan cybercrime ini.

3) *Data forgery*

   Ini merupakan modus kriminal di dunia maya yang dilakukan dengan memalsukan data dokumen penting yang disimpan sebagai dokumen tanpa kertas melalui internet. Kejahatan sejenis ini biasanya menargetkan dokumen e-commerce, seolah-olah ada "*typo*" yang pada akhirnya akan menguntungkan pelaku, karena korban akan memasukkan data pribadi dan nomor kartu kredit kepada pelaku.[47]

[47] Yuni Fitriani dan Roida Pakpahan, Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace, *Cakrawala: Jurnal Humaniora*, 20 (1) Maret 2020: h 22.

4) *Cyber espionage*

Ini ialah bentuk kejahatan yang memakai jaringan internet dengan cara memasuki sistem jaringan komputer pihak yang akan ditargetkan menjadi sasaran untuk dimata-matai.

5) *Cyber sabotage and extortion* (sabotase dan pemerasan dunia maya)

Dalam jenis kejahatan ini, modus biasanya dijalankan dengan mengganggu, merusak, atau menghancurkan data yang terhubung ke internet, program komputer, atau sistem jaringan komputer. Biasanya kejahatan semacam ini dilakukan dengan cara memasukkan logic bomb, virus komputer atau program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan dan tidak dapat beroperasi secara normal atau tidak dapat berjalan, tetapi telah dikendalikan oleh penjahat sesuai kebutuhan.

6) *Offense against intellectual property* (pelanggaran terhadap Hak atas Kekayaan Intelektual)

Modus operandi kejahatan ini adalah menyasar hak kekayaan intelektual yang dimiliki pihak lain di Internet. Misalnya, meniru tampilan website orang lain secara ilegal.

7) *Infringements of privacy*

Jenis kejahatan ini rata-rata menargetkan informasi pribadi yang disimpan dalam formulir data pribadi yang tersimpan secara computerized, apabila orang lain mengetahuinya, hal itu dapat menyebabkan kerugian

terhadap korban secara materiil maupun immaterial, seperti bocornya nomor PIN ATM, dan lainnya.[48]

Sifat kejahatan cybercrime dapat diklasifikasikan sebagai berikut:

1) *Cyber crime* sebagai tindakan kriminal

Cyber crime seperti yang dimaksud ialah sebuah tindak kejahatan yang dilakukan dengan konsep kriminalitas yang menggunakan internet sebagai wahana kejahatan. Misalnya carding: mencuri kode PIN ATM milik orang lain buat digunakan dalam transaksi online di internet, dan pemanfaatan media internet (*webserver*, *mailing list*) untuk mengedarkan alat-alat pembajakan. Pengirim e-mail anonim yang bermuatan iklan (*spamming*) juga dapat dicantumkan dalam contoh kejahatan yang memanfaatkan internet sebagai medianya dan dapat dituntut dengan tuduhan pelanggaran privasi.

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

Kejahatan semacam itu di Internet termasuk dalam area "abu-abu". Oleh karena itu, karena motif aktivitasnya terkadang bukan kejahatan, maka sulit untuk menentukan apakah perilaku tersebut merupakan kejahatan. Salah satu contohnya adalah *probing* atau *portscanning*. Ini adalah istilah yang digunakan untuk memantau sistem orang lain, dan disalahgunakan dengan mengumpulkan informasi sebanyak mungkin dari sistem.[49]

[48] Miftakhur Rokhman Habibi dan Isnatul Liviani, *Op.Cit,* 23 (2) Desember 2020, h 406

[49] Fiorida Mathilda, Cyber Crime dalam Sistem Hukum Indonesia, *SigmaMu,* 4 (2) September 2012, h 36-37

Dalam beberapa literatur, cybercrime umumnya dianggap sebagai *computer crime*. *The U.S. Department of Justice* mendefinisikan kejahatan komputer sebagai: "*…any illegal act requiring knowledge of computer technology for its perpe-tration, investigation, or prosecution*". *Organization of European Community Development* membagikan definisi lain, yaitu: "*any illegal, un-ethical or unauthorized behavior relating to the automatic processing and/or the transmission of data*". Hamzah mendefinisikan sebagai "kejahatan di bidang pc secara universal bisa dimaksud bagaikan pemakaian pc secara ilegal".

Dari penafsiran di atas, Wisnubroto mengartikan kejahatan PC bagaikan perbuatan melawan hukum yang dicoba dengan memakai pc bagaikan fasilitas/ perlengkapan PC bagaikan objek, baik buat memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Singkatnya, kejahatan komputer didefinisikan sebagai tindakan ilegal yang dilakukan dengan menggunakan teknologi komputer yang kompleks. Selain itu, sejak kejahatan dilakukan di dunia maya melalui internet, muncul istilah *cybercrime*.

Untuk sebagian besar warga yang terbiasa memakai media teknologi komunikasi, *cybercrime* tidaklah sebutan yang asing. *Cybercrime* ataupun kejahatan dunia maya ialah fenomena yang tidak dapat disangkal. Tidak nampak tetapi nyata. Permasalahan *cybercrime* yang bermacam-macam terus menjadi bertambah tiap harinya, paling utama di negara yang belum terdapat kepastian hukum di bidang teknologi komunikasi modern (*convergence*).

Meskipun mereka tak ingin dipanggil sebagai penjahat karena perbuatannya, namun mereka tidak berbeda dengan penjahat. Karena teknologi komunikasi ini punya kekuatan yang luar biasa untuk mengubah prilaku komunikasi manusia, tehnologi ini selain ada manfaat berwujud kemudahan komunikasi, juga memiliki sisi yang gelap. Salah satu contoh kerugian tehnologi adalah memudahkan para "penjahat" untuk melakukan kejahatan. Penjahat dunia maya (*cybercrime*) bisa memangsa korbannya, itu adalah kemungkinan dari kemajuan tehnologi itu sendiri.

Raharjo meyakini bahwa kejahatan merupakan fenomena sosial yang sudah ada di dunia mulai awal pada kehidupan manusia. Kejahatan yang lebih maju (modern) adalah suatu bentuk pengubahan kejahatan dari bentuk asli karena tehnologi komunikasi. [50] Wajah kejahatan juga sudah diperhalus dengan sedemikian rupa, kejahatan konvensional di dunia nyata timbul ke dunia maya dengan cara virtual. Pada faktanya, *cybercrime* telah menimbulkan begitu banyak korban dan kerugian moril dan materil. Korban dapat berupa netizen (penghuni *cyberspace*) dan masyarakat umum. Namun pada negara berkembang dengan ketimpangan digital seperti Indonesia, tak menganggapnya sebagai bentuk kejahatan.

Seperti halnya kehidupan nyata, ada yang hitam dan ada yang putih, ada yang berperan seperti pahlawan, dan ada pula yang seperti penjahat. Untuk memahami *cybercrime*, kita juga kudu memahami apa yang disebut dengan *hacker*, *cracker* dan lainnya. Lebih detailnya adalah sebagai berikut:

[50] Agus Raharjo, *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: Citra Aditya Bakti, 2002, h 29

1) *Hacker*

Menurut Ustadiyanto definisi hacker adalah orang-orang yang ahli dalam bidangnya. [51] *Hacker* ialah orangorang yang doyan mempelajari komplikasi sistem komputer dan melakukan eksperimen. Mereka cerdas dan mahir untuk menyusup ke dalam jaringan komunikasi suatu pranata di dunia maya. Peretas ini anti sensor, anti penipuan, dan memaksakan hasrat orang lain. Mereka bertaut prinsip bahwa *hacker* bermaksud meningkatkan keamanan jaringan internet. Mereka memuliakan etika atau norma yang berlangsung di dunia maya. Contohnya, jika ada sebuah perusahaan perbankan mengatakan tentang jaringan sistem komunikasinya sangat rumit dan mustahil untuk diretas serta tak akan ada yang berhasil menembus. Maka hacker akan menghadapi tantangan tersebut, dan selepas berhasil mereka akan memperingatkan alangkah lemahnya sistem informasi perusahaan itu. Oleh karena itu, tak sedikit dari mereka yang berakhir dengan direkrut perusahaan untuk mengamankan sistem informasi dan komunikasi di dunia maya.

2) *Cracker*

Di dunia maya, ada beberapa sisi menakutkan dari *hacker*. Mereka disebut cracker. Para *cracker* secara ilegal menyusup, menembus, serta merusak situs *web*, dan sistem keamanan jaringan internet hanya untuk tujuan

[51] Riyeke Ustadiyanto, *Framework e-Commerce*, Yogyakarta: Andi, 2001, h 304.

hiburan dan keuntungan. Setelah berhasil menghancurkan situs sebuah perusahaan, mereka merasa bangga. Serangan *cracker* juga sangat luar biasa. Ada sekitar 100 serangan *cracker* dalam sehari. Info tersebut diperoleh dari Kementerian Pertahanan Amerika Serikat di Pentagon.

3) *Carder*

Carder merupakan orang yang melakukan *cracking*, ialah pembobolan kartu kredit untuk mencuri nomor kartu orang lain dan menggunakannya untuk keuntungan pribadi. Umumnya yang menjadi korban adalah mereka yang memiliki kartu kredit dalam jumlah besar. Menurut hasil penelitian kejahatan carding, pada tahun 2002 Indonesia menduduki peringkat kedua setelah Ukraina.

4) *Deface*

Deface merupakan suatu gerakan menyusup ke suatu situs, kemudian mengganti tampilan halaman situs untuk maksud tertentu. Indonesia pernah diserang para deface yang mengubah situs TNI. Tampilan gambar Burung Garuda Pancasila diganti dengan lambang palu arit. Tampilan homepage Polri juga diubah menjadi gambar wanita telanjang.

5) *Phreaker*

Merupakan seseorang yang melaksanakan cracking yang berkenaan dengan jaringan telepon, sehingga dapat melakukan panggilan secara gratis kemana saja. Di Indonesia, kasus seperti ini pernah terjadi pada beberapa warung telepon.

Para karakter *hacker* biasanya tak berasal dari kaum bawah, mereka biasanya ialah orang-orang terpelajar, yang setidaknya mengenyam pendidikan sampai tingkat tertentu dan bisa menggunakan ataupun mengoperasikan komputer. Para *craker* juga termasuk orang yang berpendidikan, tidak buta teknologi, mampu menurut finansial, serta tidak termasuk dalam masyarakat kelas bawah. Kejahatan seperti ini dapat diklasifikasikan sebagai "*white collar crime*" (kejahatan kerah putih). Jo Ann L. Miller, membagi pelakunya menjadi 4 (empat) kategori:

1) *Organizational occupational crime*

   Penjahat melakukan tindakan ilegal atau merugikan orang lain lewat jaringan internet buat kepentingan atau keuntungan suatu perusahaan. Pelaku biasanya adalah para eksekutif.

2) *Government occupational crime*

   Melakukan suatu tindakan yang ilegal melalui internet, namun dengan persetujuan atau perintah dari negara (pemerintah), Pelakunya sendiri ialah pejabat (birokrat) meski dalam banyak kasus bilamana hal tersebut terkuak, maka akan dibantah.

3) *Professional occupational crime*

   Beragam pekerjaan yang melakukan kejahatan secara disengaja (malpraktik).

4) *Individual occupational crime*

   Ialah para pengusaha, pemilik modal atau orang-orang independen lainnya yang melakukan perbuatan menyimpang, walaupun tingkat sosial

ekonominya mungkin tidak tinggi. Dalam aspek pekerjaannya, kelompok ini mengambil jalan yang menyimpang dan melanggar hukum atau merugikan orang lain.[52]

Dibandingkan dengan kejahatan konvensional, *cybercrime* memiliki karakteristik yang unik yaitu:

1) Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang atau dunia maya, sehingga tidak mungkin untuk menentukan yurisdiksi hukum negara mana yang berlaku untuk tindakan tersebut.
2) Perbuatan tersebut dilakukan dengan menggunakan (perangkat) apapun yang dapat tersambung ke internet.
3) Kerugian material maupun non-material yang disebabkan oleh tindakan-tindakan ini seringkali lebih besar daripada kejahatan tradisional.
4) Pelakunya ialah orang yang dapat menguasai penggunaan internet dan aplikasinya.
5) Perbuatan tersebut acapkali dilakukan secara transnasional.

D. Kejahatan Siber dalam Perspektif Hukum Islam

Hukum pidana islam merupakan syariat Allah SWT yang mengandung kemaslahatan dalam kehidupan manusia di dunia dan akhirat, syariat yang dimaksud secara materil mengandung kewajiban asasi bagi setiap manusia untuk

[52] M. E. Fuady, Fenomena Kejahatan Melalui Internet di Indonesia, *Mediator*, 6 (2), Desember 2005, h 258.

melaksanakannya. Konsep kewajiban asasi syariat, yaitu menempatkan Allah SWT sebagai pemegang segala hak, baik yang ada pada diri sendiri maupun yang ada pada orang lain. Setiap orang hanya sebagai pelaksana yang berkewajiban memenuhi perintah Allah SWT. Perintah Allah SWT dimaksud harus dituntaskan untuk kemaslahatan dirinya dan orang lain.[53]

Al Qur'an merupakan penjelasan Allah SWT, tentang syariat sehingga disebut *albayan* (penjelasan). Penjelasan yang dimaksud secara garis besar mempunyai empat cara dan salah satunya adalah Allah SWT, memberikan penjelasan dalam bentuk nash (tekstual) tentang syariat, misalnya orang mengambil barang milik orang lain di tempat penyimpanan dengan cara yang tidak benar yang melebihi batas nisabnya harus dipotong tangannya atas adanya putusan dari pengadilan.

Dipahami dari pengertian dan jenis-jenis *cyber crime t*ersebut di atas, *cybercrime* merupakan bentuk kejahatan yang muncul di era modern sekarang ini. Dengan demikian, perbuatan kejahatan *cyber crime* menurut analisa hukum Islam (*jinayat*) dapat dihukum dengan *ta'zir*. *Ta'zîr* menurut pengertian bahasa berarti pencegahan (*al-man'u*). adapun menurut istilah *ta'zîr* merupakan hukuman edukatif (*ta'dîb*) dalam arti mengantisipasi dengan cara menakut-nakuti (*tankîf*). Adapun secara *syar'î*, *ta'zîr* dimaksudkan sebagai sanksi yang dijatuhkan atas dasar kemaksiatan, karena secara tegas tidak termasuk kejahatan yang termaktub dalam Al Quran dan Hadis, sebagaimana *had*, *Qisas*, atau *kafârat*.

[53] Suharyadi, dkk. Kejahatan Dunia Maya (Cyber Crime) Dalam Prespektif Hukum Islam, *Journal of Lex Generalis (JLS)*, 1 (5) Oktober 2020, h 764

Cyber crime merupakan aktivitas kejahatan dengan menggunakan fasilitas computer atau jaringan computer tanpa ijin dan melawan hukum, baik cara mengubahnya atau tanpa perubahan (kerusakan) pada fasilitas computer yang dimasuki atau digunakan atau kejahatan yang dengan menggunakan sarana media elektronik internet karena dikategorikan sebagai kejahatan dunia maya, atau kejahatan di bidang computer dengan cara illegal. Dapat pula dikategorikan sebagai kejahatan komputer yang ditujukan kepada system atau jaringan komputer, yang mencakup segala bentuk kejahatan baru yang menggunakan bantuan sarana media elektronik internet. Sanksi bagi para para pelaku cybercrime menurut syariat islam adalah ta'zir melalui proses peradilan dengan vonis hakim dengan ancaman hukuman berupa kurungan penjara, pengasingan, cambuk, sampai pada hukuman mati sesuai dengan tingkat mudharat yang telah dilakukannya.[54]

Al Qur'an merupakan penjelasan Allah SWT tentang syariat sehingga disebut albayan (penjelasan). Penjelasan yang dimaksud secara garis besar mempunyai empat cara dan salah satunya adalah Allah SWT. Memberikan penjelasan dalam bentuk *nash* (tekstual) tentang sesuatu syariat, misalnya orang yang mengambil barang milik orang lain di tempat penyimpanan dengan cara yang tidak benar yang melebihi batas nisabnya harus dipotong tangannya atas adanya putusan dari pengadilan.[55]

Bila ditelusuri lebih jauh, Allah SWT membatasi tingkah laku manusia melalui syariatnya semata mata karena ingin menegakkan keadilan, kedamaian, ketertiban dan

[54] *Ibid*
[55] *Ibid*, h 765

ketentraman masyarakat, sehingga apabila syariat itu dapat ditegakkan sudah pasti tujuan hidup dapatlah dicapai. Hal ini dimaksudkan agar tujuan syariat dapat terwujud yakni, terpeliharanya agama, jiwa, keturunan atau kehormatan, harta dan akal. Mengapa hal ini perlu diwujudkan, karena semata mata ingin menjaga manusia dari kesempurnaan yang diberikan oleh Allah SWT.

Berkaitan dengan hal tersebut, atas universal juga menyebutkan bahwa memelihara ketertiban umum di atas kepentingan pribadi merupakan suatu keharusan dan kewajiban bagi setiap manusia. Oleh karena itu, tindakan yang bertentangan dengan asas tersebut dinilai sebagai suatu pelanggaran hukum. Misalnya membuat keonaran, keributan dan pengerusakan di lingkungan masyarakat tentu mengganggu masyarakat yang lain.

Dilihat dari sudut pandang hukum pidan islam yang menjadi landasan pokok terhadap aspek yuridis, adalah teori maqasid al syariah meletakkan prinsip-prinsip yang menjadi pertimbangan pokok dari tujuan hukum, yaitu terwujudnya dan terpeliharanya al-masalih al-khamsah atau lima kebutuhan pokok dalam kehidupan manusia yang mencakup pemeliharaan agama (*hifz al-nafs*), keturunan atau kehormatan (*hifz al-nash*), harta (*hifz al-mal*) dan akal (*hifz al-aql*).[56]

Apabila dikaitkan dengan tindak pidana *cyber crime*, maka *cyber crime* menjadi bagian dari obyek yang sama dari *jarimah*, hanya *cyber crime* merupakan tindak pidana

[56] Suharyadi, dkk. *Op.Cit,* 1 (5) Oktober 2020, h 765

yang dilakukan melalui media elektronik dan sejenisnya, sementara *jarimah* dilakukan dalam dunia *real* (dunia nyata) sebagaimana dalam hukum konvensional.

Kata *jarimah* sering digunakan sebagai perbuatan dosa, bentuk, macam atau sifat dari perbuatan dosa besar tersebut. Misalnya pencurian, pembunuhan, perkosaan atau perbuatan yang berkaitan dengan politik. Keseluruhan itu dapat disebut dengan istilah *jarimah* yang kemudian dirangkaikan dengan satuan atau sifat perbuatan tersebut. Oleh karena itu, menggunakan istilah *jarimah* pencrian, *jarimah* pembunuhan, *jarimah* perkosaan dan *jarimah* politik.[57]

Melihat kenyataan dalam dunia *cyber*, hukum ruang maya haruslah juga difokuskan dalam pembahasan hukum pidana islam, karena undang-undang yang ada belumlah maksimal dalam penerapannya. Hal ini terjadi karena undang-undang yang ada sebagai produk hukum tidak di gali dari sumber yang jernih. Berbeda halnya dengan hukum islam yang jelas sumber hukumnya memiliki kejernihan, yakni sumber hukum dari Allah. Kejernihan dan kemurnian sumber inilah yang dapat melahirkan sebuah produk hukum yang dapat dipertanggungjawabkan daripada produk hukum yang bersumber dari hukum eropa kontinental.

Secara filosofis dapat digambarkan, bahwa sesuatu yang jernih itu lahir dari yang jernih, sementara sesuatu yang tidak jernih itu sulit melahirkan sebuah kejernihan dan bahkan tidak dapat menghasilkan kejernihan. Hal ini secara tersirat, menggambarkan bahwa produk hukum haruslah dibuat oleh orang-orang yang

[57] R. Hakim, *Hukum Pidana Islam (Fiqih Jinayah)*, CV. Pustaka Setia, Bandung. 2000

memiliki kredibilitas dan niat yang benar untuk bisa menghasilkan undang-undang yang benar pula sehingga dapat mencapai sebuah tujuan hukum yakni, terciptanya rasa keadilan, kesejahteraan, ketentraman dan kedamaian masyarakat.[58]

Berkaitan dengan hal tersebut, *cyber crime* tentu memiliki relevansi dengan *jarimah* karena dalam sebuah Negara yang menerapkan hukum islam tentu *cyber crime* menjadi obyek dari jarimah itu sendiri. Rumusan dalam *cyber crime* tidak jauh berbeda dengan jarimah yang membedakan di antara keduanya terletak pada modus operandinya. Selain itu, hukum pidana juga dapat menggali melalui tekhnik dan cara yang sudah dirumuskan oleh para ulama fikih, khususnya fikih *jinayah*.

Suatu perbuatan dinamakan *jarimah* (tindak pidana, peristiwa pidana atau delik apabila perbuatan tersebut mengakibatkan kerugian bagi orang lain atau masyarakat baik jasad (anggota badan atau jiwa), harta benda, keamanan, tata aturan masyarakat, nama baik, perasaan ataupun hal-hal lainyang harus dipelihara dan dijunjung tinggi keberadaannya). *Cyber crime* sampai hari ini terjadi dalam jumlah yang sulit untuk dihitung, karena lajunya lalu lintas di dunia *cyber* berdampak terhadap perilaku dari pengguna layanan internet. Hal ini tentu mengakibatka jumlah kerugian terhadap harta benda dan keamanan yang sangat besar.

Penyebab perbuatan yang merugikan tersebut di antaranya adalah tabiat manusia yang cenderung pada sesuatu yang menguntungkan bagi dirinya meskipun hasil pilihan atau perbuatan tersebut merugikan orang lain. Kenyataan ini memerlukan

[58] Suharyadi, dkk. *Op.Cit*, 1 (5) Oktober 2020, h 764

kehadiran peraturan atau perundang undangan. Akan tetapi kehadiran peraturan tersebut menjadi tidak berarti tanpa adanya dukungan yang dapat memaksa seseorang untuk mematuhi peraturan tersebut. Dukungan yang dimaksud adalah pernyataan ancaman hukuman atau sanksi yang menyertai kehadiran peraturan tersebut.[59]

Secara implikatif sanksi kejahatan siber berdasarkan perspektif hukum islam dikaitkan pada perbuatan-perbuatan yang sama pada kejahatan konvensional sesuai dengan jenis kejahatan siber yang memberikan impak seperti apa yang sama dengan sebuah kejahatan konvensional antara lain:

1) Penipuan

Sanksi pidana penipuan sebagaimana penjelasan tersebut di atas, bahwa kejahatan penipuan dilihat dari ruh syariat, menipu adalah membohongi. Berlaku dusta merupakan ciri munafik. Secara tegas dinyatakan dalam hadis nabi sebagai berikut:

> Diriwayatkan dari Abu Hurairah ra: Nabi Muhammad SAW pernah bersabda: "Ada tiga tanda/ciri orang munafik yaitu: apabila ia berkata ia dusta, apabila ia berjanji ia selalu mengingkari dan apabila ia diberi amanat, maka ia berkhianat".

Sifat pembual, pendusta, pembohong dan penipu adalah karakter yang melekat bagi orang munafik. Munafik seperti dinyatakan dalam firman Allah SWT. Q.S An-Nisa/4 : 145 sebagai berikut:

[59] *Ibid*, h 769

إِنَّ ٱلْمُنَٰفِقِينَ فِى ٱلدَّرْكِ ٱلْأَسْفَلِ مِنَ ٱلنَّارِ وَلَن تَجِدَ لَهُمْ نَصِيرًا ﴿١٤٥﴾

Artinya: Sesungguhnya orang-orang munafik itu (ditempatkan) pada tingkatan yang paling bawah dari neraka, dan kamu sekali-kali tidak akan mendapat seorang penolong pun bagi mereka.

Ayat tersebut memberikan penilaian kepada orang munafik lebih membahayakan daripada orang kafir. Jika merampas atau merampok harta hukumannya seperti hukuman orang kafir yaitu hukuman mati, maka hukuman terhadap orang munafik minimal sama dengan hukuman yang ditentukan terhadap perampok.

Berdasarkan hal tersebut, apabila pelaku tindak pidana penipuan disamakan dengan perbuatan perampok, maka sanksi hukumannya adalah dibunuh yang kemudian disalib atau dipotong tangan dan kakinya atau dibuang. Hal ini dilakukan atas dasar besar kecilnya efek yang diimbulkan dari tindakan tersebut. Apabila dilihat dari sudut pandang *Cyber crime*, maka hukuman pokok pada tindak pidana tersebut bisa berupa takzir, karena hakim memiliki otoritas terhadapnya.

2) Kesusilaan

Tindak pidana kesusilaan merupakan bagian dari tindak pidana *takzir*, yakini termasuk dalam perbuatan-perbuatan Yang tidak termasuk dalam kategori *hudud* dan *diat*. Penetapan kategori tindak pidananya diserahkan

kepada penguasa Negara untuk mengaturnya, demikian juga dengan sanksi pidananya. Tindak pidana *takzir* adalah keseluruhan tindak pidana yang terdapat dalam nas Al Qur'an dan hadis, tetapi tidak ditetapkan sanksi pidananya. Karena tindak pidana kesusilaan muncul di dunia *cyber*, maka tindak pidana ini juga ditetapkan oleh penguasa, karena modus operandinya yang dinilai baru. Kewenangan diberikan kepada para legislator untuk merumuskannya.

3) Perjudian

Sebagaimana telah dijelaskan sebelumnya, bahwa apabila dilihat dari aspek hukum islam, larangan tentang perjudian dan undian dirangkaikan dengan *khamar*. Dengan dasar itu perjudian dan undian sanksi hukumnya disejajarkan dengan tindak pidana *khamar*. Hal ini didasarkan atas firman Allah SWT, Q.S Al Maidah/5: 90 sebagai berikut:

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُوٓاْ إِنَّمَا ٱلۡخَمۡرُ وَٱلۡمَيۡسِرُ وَٱلۡأَنصَابُ وَٱلۡأَزۡلَٰمُ رِجۡسٞ مِّنۡ عَمَلِ ٱلشَّيۡطَٰنِ فَٱجۡتَنِبُوهُ لَعَلَّكُمۡ تُفۡلِحُونَ ٩٠

Artinya: Wahai orang-orang yang beriman, sesungguhnya (meminum) khamar, berjudi (berkurban untuk) berhala, mengundi nasib dengan panah adalah perbuatan keji termasuk perbuatan setan. Maka jauhilah perbuatan-perbuatan itu agar kamu mendapat keberuntungan.

Mencermati ayat tersebut, bahwa kedua tindak pidana (perjudian dan *khamar*) dinilai sebagai suatu perbuatan keji dan biadab. Oleh karena itu dalam ayat tersebut menyejajarkan atas hukuman terhadap kedua tindak pidana

tersebut. Sanksi pidana terhadap peminum *khamar* telah disepakati oleh para ulama, yaitu berupa *had*. Hal ini juga berlaku Pada pelaku tindak pidana perjudian yakni hukuman *had*. Berkaitan dengan bentuk hukumannya para ulama berbeda pendapat, sebagian menyatakan hukumannya akan dijilid sebanyak 80 kali jilid seperti dikatakan oleh Imam Malik dan Abu Hanifah, sebagian lagi mengatakan 40 kali jilidan seperti yang dipahami oleh Imam Syafi'i. Meskipun demikian pendapat terakhir ini membolehkan (kalau dikehendaki pengusaha/*ulil amri*) penambahan 40 kali lagi, sebagai hukuman takzir. Pelaksanaan hukuman jilid bagi pelaku *jarimah* ini seperti hukuman jilid pada *jarimah* lain yang mengharuskan hukuman jilid.[60]

Hukuman jilid (cambuk) juga di adopsi oleh Negara Republik Indonesia, dimana Negara Indonesia yang mengkhususkan daerah tertentu dengan menggunakan aturan ekonomi khusus untuk menerapkan hukuman cambuk atau jilid sebagai hukuman yang dinilai cukup efektif. Hal ini dilakukan semata-mata untuk mewujudkan rasa keadilan dan kemanusiaan yang sekaligus menjadi ciri dari pemidanaan dalam islam.[61]

4) Pemerasan/Pengancaman

Pemerasan yang disertai pengancaman pada dasarnya mengambil harta atau pemindahan hak kepemilikan harta benda milik orang lain dalam penguasaannya tanpa transaksi yang sah disertai dengan pemaksaan sehingga

[60] Suharyadi, dkk. *Op.Cit*, 1 (5) Oktober 2020, h 770
[61] *Ibid* h 771

modus yang dilakukan terhadap kejahatan ini bermacam-macam. Tetapi substansinya ingin memiliki harta dengan cara yang tidak benar. Tindak pidana ini dapat pula dikiaskan dengan penodongan atau perampokan dengan ilat mengambil harta atau pemindahan hak kepemilikan harta benda milik orang lain dalam penguasaannya tanpa transaksi yang sah disertai dengan pemaksaan.

Penodongan lebih lazim dipakai terhadap tindak pidana yang dilakukan di luar rumah, sedangkan perampokan dilakukan di dalam rumah atau kantor, sehingga sanksi hukumannya dapat dijatuhi berdasarkan ketentuan pokok dalam pencurian dan perampokan yaitu dibunuh yang kemudian disalib atau pidana amputasi tangan dan kaki yang merupakan sebagai sanksi pidana pokok tindak pidana *takzir*.

Akan tetapi dengan melihat kenyataan terhadap perbuatan pidana yang dilakukannya sanksi hukumannya dapat berupa hukuman yang lebih ringan seperti misalnya pidana cambuk, pidana penjara, pidana denda, pidana pengawasan dan lain-lain bahkan bebas dari segala Tuntutan hukum. Penjatuhan hukuman tentu setelah melalui proses peradilan (persidangan) dan memenuhi syarat-syaratnya.

BAB III

HASIL PENELITIAN DAN PEMBAHASAN

A. Politik Hukum Pidana Nasional dalam Mengakomodir Kejahatan Siber

Indonesia ialah negara hukum berdasarkan pada Pasal 1 ayat (3) Undang-Undang Dasar 1945 hasil amandemen.[62] Negara hukum merupakan negara yang

[62] Anirut Chuasanga and Ong Argo Victoria, *Op.Cit*, 2 (1), March 2019, h 131

menjadikan hukum sebagai landasan dan keadilan bagi warganya, memiliki arti bahwa seluruh kewenangan dan kebijakan alat alat perlengkapan negara atau penguasa itu berdasarkan hukum atau dengan kata lain diatur oleh hukum.

Dalam Pembukaan UUD 1945 alinea ke-4 merumuskan bahwa melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum. dalam Rumusan kalimat melindungi segenap bangsa Indonesia memiliki arti bahwa negara turut serta bertanggungjawab dalam upaya menaikan harkat dan martabat manusia yang merupakan perwujudan perlindungan terhadap hak hak asasi manusia.[63]

Di dalam memberikan perlindungan hukum bagi individu maupun masyarakat di Indonesia, pidana menjadi salah satu pilihan sarana yang dipilih oleh pembentuk undang-undang. Berbagai peraturan perundang-undangan yang memuat "ketentuan pidana" merupakan wujud konkret pilihan kebijakan yang dimaksud. Ketentuan pidana yang dimuat dalam berbagai produk legislatif salah satunya memuat aturan/ketentuan hukum pidana materiil/substantif.[64]

Untuk melindungi hak-hak rakyat yang berorientasi kepada keadilan dan kesejahteraan rakyat, perlu diambil Kebijakan oleh Badan Negara Legislatif dan Eksekutif, dalam memformulasi regulasi hukum yang merupakan bagian dari sistem penegakan hukum secara *In abstracto* yang tidak jarang dalam memformulasi hukum

[63] Arief Amrullah, *Politik Hukum Pidana (Dalam Perlindungan Korban Kejahatan Ekonomi Di Bidang Perbankan)*, Bayumedia, Malang, 2007, h 2

[64] Edi Ribut Harwanto, *Politik Hukum Pidana*, Sai Wawai Publishing, 2019, h 4

pihak Perguruan Tinggi diminta pendapatnya yang disebut dengan naskah akademik, dalam konteks hukum pidana kebijakan seperti ini disebut dengan Kebijakan Hukum Pidana (*Penal Policy*) atau kebijakan kriminal (*criminal policy*).[65]

Politik merupakan perwujudan dari daya pikir manusia untuk mewujudkan apa yang menjadi tujuan hidup manusia, segala daya dan upaya dikristalkan pada politik guna menciptakan apa yang menjadi tujuan melalui apa yang kita sebut dengan politik. Politik merupakan seni dalam menggapai apa yang menjadi visi dan harapan dalam kehidupan, dengan politik kitab isa membuat suatu kehidupan sangat tentram dan sejahtera begitu juga sebalikanya, bisa menghancurkan suatu peradaban.[66] Politik menurut Hoogerwerf adalah usaha mencapai tujuan tertentu dengan sarana tertentu dan dalam urutan waktu tertentu.[67] Politik atau dengan kata lain "kebijakan" juga dapat dipahami sebagai keputusan yang menggariskan cara yang paling efektif dan efisien untuk mencapai tujuan yang ditetapkan bersama.[68]

Hukum merupakan satuan yang kompleks meliputi keberagaman masyarakat yang memiliki banyak aspek, dimensi, dan fase. Bernard Arief Sidharta berpendapat bahwa hukum memiliki iti dalam satuan aspen dalam interaksi di dalam masyarakat (politik, ekonomi, sosial, budaya, teknologi, keagamaan, dan sebagainya) dibentuk dan

---

[65] *Ibid*, h 5

[66] Boediono. *Teori Hukum*. Yrama Widya. Bandung. 2016. h 213

[67] Mudzakir dkk, *Perencanaan Pembangunan Hukum Nasional Bidang Politik Hukum Pidana dan Sistem Pemidanaan*, Jakarta, Badan Pembinaan Hukum Nasional, 2012, h 8-9

[68] Robert R.Mayer dan Ernest Greenwood dalam Sultan Zan Arbi dan Wayan Ardana, *Rancangan Penelitian Dan Kebijakan Sosial,* Jakarta, CV. Rajawali, 1997, h 63

ikut membentuk tatanan masyarakat, bentuknya ditentukan oleh masyarakat yang mana secara otomatis membentuk masyarakat itu sendiri.[69]

Terdapat korelasi yang sangat dekat dan saling keterkaitan antara politik dan Hukum, yang mana hukum diharapkan mampu membuat pelaksanaan kekuasaan dan politik menjadi lebih manusiawi, sementara politik kekuasaan diharapkan mampu mengkonvergensikan perilaku manusia menjadi lebih teratur dan juga harapan keadilan bisa diwujudkan. Sehingga bisa dikatakan bahwa hukum berperan dalam bagaimana memanusiakan penggunaan hukum.[70]

Norma hukum dapat dinyatakan berlaku secara politis bilamana pemberlakuannya itu didukung oleh faktor-faktor kekuatan politik yang nyata atau *riele machtsfactoren*. Walaupun suatu norma didukung oleh semua lapisan masyarakat, sesuai dengan cita-cita filosofis negara, dan mempunyai landasan yuridis yang jelas, tetapi kurang mendapatkan dukungan dari paremen maka norma tersebut tidak dapat berlaku sebagai hukum. Dengan kata lain perana politik ini berkaitan dengan teori kekuasaan (*power theory*) memberikan legitimasi pada keberlakuan suatu norma hukum hanya dari sudut pandang kekuasaan. Apabila suatu norma hukum telah mendapat dukungan kekuasaan maka norma hukum tersebut dapat berlaku, bagaimanapun wujudnya.

---

[69] Imam Syaukani dan A. Ahsin Thohari. *Dasar-Dasar Politik Hukum*. Jakarta: RajaGrafindo Persada, 2010. h 2

[70] Endri Susanto, dkk. Politik Hukum dalam Penegakan Undang-Undang Informasi dan Transaksi Elektronik, *Jurnal Kompilasi Hukum*, 6 (2) Desember 2021, h 108

Hukum merupakan produk politik sehingga karakter setiap produk hukum akan sangat ditentukan atau diwarnai oleh pertimbangan kekuatan atau konfigurasi politik yang melahirkannya. Hal ini berdasarkan kenyataan bahwa setiap produk hukum merupakan keputusan politik sehingga hukum dapat dilihat sebagai kristalisasi dari pemikiran politik yang saling berinteraksi dikalangan para politisi. Meskipun dari sudut "*das sollen*" ada pandangan bahwa politik harus tunduk pada ketentuan hukum, namun dari sudut "*das sein*" bahwa hukumlah yang dalam kenyataannya ditentukan oleh konfigurasi politik yang melahirkannya.

Akibatnya adalah nantinya ada kecenderungan pada ilmu hukum untuk "meremehkan" kekuatan-kekuatan social dan budaya. Tetapi, kekuatan yang "memaksa" inilah ilmu politik berpendapat bahwa penting untuk mengungkap kesadaran maupun partisipasi politik. Hal ini sesuai dengan pendapat Hans Kelsen, bahwa negara sebagai suatu badan hukum atau *Rechtsperson* (*juristicperson*).[71]

Politik dan Hukum adalah dua hal yang berbeda tetapi saling membutuhkan karena memang Hukum ada pada kenampakan dan kenyataan sementara Politik merupakan cara untuk mencapai tujuan termasuk hukum adalah merupakan tujuan yang juga yang harus digapai melalui proses politik.[72] Sebagaimana juga politik kemudian membutuhkan hukum untuk melegalisasi apa yang menjadi tujuannya sehingga apa yang dilakukan secara politik diterima oleh masyarakat sebagai sesuatu

[71] *Ibid*, h 109

[72] Imawanto, et.al. Pengaruh Politik dalam Pembentukan Hukum di Indonesia. *Meida Keadilan Jurnal Ilmu Hukum*. 12 (1) 2021, h 164

yang legal secara hukum walaupun secara kasat mata itu tidak benar tapi hukum bisa memainkan perannya dalam mengcover isu supaya Nampak menjadi benar – benar legal secara konstitusi. Sehingga bisa dikatakan antara hukum dan politik itu tidak bisa terpisahkan didalam suatu kehidupan ataupun negara, keduanya akan saling melengkapi dan saling membutuhkan.

Secara terminologi, dalam kepustakaan asing istilah "politik hukum pidana" ini sering dikenal dengan berbagai istilah, antara lain "*penal policy*", "*criminal law policy*" atau "*strafrechtspolitiek*".[73] Lebih lanjut Sudarto menjelaskan bahwa melaksanakan politik hukum pidana berarti mengadakan pemilihan untuk mencapai hasil perundang-undangan pidana yang paling baik dalam arti memenuhi syarat keadilan dan daya guna. Selanjutnya juga dikemukakan bahwa melaksanakan politik hukum pidana berarti usaha mewujudkan peraturan perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa-masa yang akan datang.[74]

Lebih lanjut Barda Nawawi Arief menjelaskan bahwa setiap usaha dan kebijakan untuk membuat peraturan hukum pidana yang baik pada hakekatnya tidak dapat dilepaskan dari tujuan penanggulangan kejahatan. Jadi, kebijakan atau politik hukum pidana juga merupakan bagian dari politik kriminal. Dengan perkataan lain, dilihat dari sudut politik kriminal, maka politik hukum pidana identik dengan pengertian "kebijakan penanggulangan kejahatan dengan hukum pidana. Usaha penanggulangan kejahatan lewat bantuan pembuatan undang-undang (hukum) pidana

[73] Barda Nawawi Arief, *Op.Cit*, 2010, h 24
[74] Edi Ribut Harwanto, *Op.Cit*, 2019, h 23

pada hakekatnya juga merupakan bagian integral dari usaha perlindungan masyarakat (*sosial defence*) dan usaha mencapai kesejahteraan masyarakat (*sosial welfare*). Oleh karena itu, wajar pulalah apabila kebijakan atau politik hukum pidana juga merupakan bagian integral dari kebijakan atau politik sosial (*social policy*). Kebijakan sosial (*social policy*) dapat diartikan sebagai segala usaha yang rasional untuk mencapai kesejahteraa masyarakat dan sekaligus mencakup perlindungan masyarakat. Jadi di dalam pengertian "*social policy*", sekaligus tercakup di dalamnya "*social welfare policy*", dan "*social defence policy*".[75] Kebijakan hukum pidana dapat juga dilihat sebagai bagian dari politik kriminal.

Hal ini didasarkan pada pemikiran bahwa usaha dan kebijakan untuk membuat peraturan hukum pidana yang baik pada hakikatnya tidak dapat dilepaskan dari tujuan penanggulangan kejahatan atau perbuatan yang dilarang. Jadi kebijakan atau politik hukum pidana juga merupakan bagian dari politik kriminal. Politik kriminal merupakan usaha yang rasional dalam masyarakat untuk menanggulangi kejahatan. Dirumuskan oleh Marc Ancel, politik kriminal adalah *the rational organization of the control of crime by society*.[76]

Dalam kaitannya dengan politik hukum pidana pada jenis kejahatan yang akan dibahas pada sub bab ini memiliki relevansi pada sebuah fenomena perkembangan jaman modern dengan diikuti oleh sebuah kemajuan teknologi yang memiliki polemik berupa polarisasi pada perilaku dan tindakan pada ruang lingkup sosial.

[75] Barda Nawawi Arief, *Op.Cit*, 2010, h 27
[76] Sudarto, *Hukum dan Hukum Pidana*, Bandung, Alumni, 1981, h 162

Globalisasi jadi salah satu pemicu teknologi memasuki sendi kehidupan masyarakat bangsa di dunia, ini tidak terlepas dari adanya interaksi global yang menyebabkan akselerasi dan perubahan. Era globalisasi memberikan pengaruh terhadap perkembangan teknologi dan internet bagi kehidupan manusia. Globalisasi dapat dimaknai sebagai suatu tindakan proses atau kebijakan membuat sesuatu di seluruh dunia dalam ruang lingkup pengaplikasian.[77]

Kemajuan teknologi adalah sesuatu yang tidak bisa kita hindari dalam kehidupan ini, karena kemajuan teknologi akan berjalan sesuai dengan kemajuan ilmu pengetahuan. Teknologi yang sebenarnya merupakan alat bantu/ekstensi kemampuan diri manusia. Kemajuan teknologi menghasilkan sejumlah situasi yang tak pernah terpikirkan sebelumnya oleh manusia. Dewasa ini, telah menjadi sebuah kekuatan yang justru membelenggu perilaku dan gaya hidup kita sendiri. Dengan daya pengaruhnya yang sangat besar, karena ditopang pula oleh sistem-sistem sosial yang kuat dan dalam kecepatan yang makin tinggi, teknologi telah menjadi pengarah hidup manusia.[78]

A. Nawawi Rambe memandang globalisasi sebagai proses sosial, proses sejarah, dan juga sebagai proses alamiah yang membuat segala semua negara di dunia terikat satu sama lain yang akan mewujudkan satu tatanan kehidupan baru ataupun kesatuan konsistensi dengan menghilangkan batas-batas geogragfis, ekonomi serta

[77] Aim Abdulkarim, *Pendidikan Kewarganegaraan: Membangun Warga Negara yang Demokratis,* Grafindo Media Pratama, Bandung, 2008, h 81

[78] Uni Sabadina, Politik Hukum Pidana Penanggulangan Kejahatan Teknologi Informasi Terkait Kebocoran Data Pribadi Oleh Korporasi Berbasis Online, *LEX Renaissan*, 4 (6) Oktober 2021, h 800

budaya di dalam masyarakat dunia[79] perihal hal tersebut adalah suatu pergeseran pola lintas komunikasi global.

Perkembangan teknologi memang sangat diperlukan. Setiap inovasi diciptakan untuk memberikan manfaat positif bagi kehidupan manusia. Mulai dari bermain game, transfer antar bank, mendengarkan musik, kegiatan fotografi, mencari berbagai informasi, dan lain sebagainya.[80] Selain dari pada itu perkembangan teknologi informasi dapat meningkatkan kinerja dan memungkinkan berbagai kegiatan dapat dilaksanakan dengan cepat, tepat dan akurat, sehingga akhirnya akan meningkatkan produktivitas. Perkembangan teknologi informasi memperlihatkan bermunculannya berbagai jenis kegiatan yang berbasis pada teknologi ini, seperti *e-government*, *e-commerce, e-education*, *e-medicine*, *e-laboratory*, dan lainnya yang kesemuanya itu berbasiskan elektronika.

Namun seperti yang kita ketahui, bahwasanya dibalik kelebihan dan kemudahan yang ditawarkan oleh komputer dan internet, ternyata kemajuan dari tekonologi ini mempunyai sisi gelapnya sendiri atau masih mempunyai kekurangannya tersendiri.[81] Namun demikian tidak dapat dipungkiri teknologi informasi saat ini seakan menjadi pedang bermata dua, karena selain memberikan kontribusi bagi

[79] Aris Saefulloh, Kebangkitan Agama Di Tengah Peradaban Global, *Jurnal Al-Ulum*, 11 (1) 2011, h 174.

[80] Intan Trivena Maria Daeng, Penggunaan Smartphone dalam Menunjang Aktivitas Perkuliahan oleh Mahasiswa Fispol Unsrat Manado, *E-Journal Acta Diurna*, 6 (1), 2017, h 1.

[81] Brisilia Tumalun, Upaya Penanggulangan Kejahatan Komputer dalam Sistem Elektronik Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008, *Jurnal Lex Et Societatis*, 6 (2) 2018, h 24

peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan untuk melawan hukum.[82]

Kemajuan teknologi berimplikasi pada perkembangan kejahatan. Kejahatan-kejahatan tradisional kini bertransformasi menjadi kejahatan di dunia maya (*cybercrime*) dengan menggunakan media internet dan alat-alat elektronik lainnya. Internet memberikan peluang bagi pelaku-pelaku kejahatan di dunia maya untuk melakukan kejahatan dengan lebih rapi, tersembunyi, terorganisasi serta dapat menembus ruang dan waktu dengan jangkauan yang sangat luas. Sebagai salah satu bentuk globalisasi kejahatan, kejahatan siber (*cybercrime*) dapat dilakukan dengan melibatkan beberapa pelaku yang berada di beberapa wilayah yurisdiksi negara yang berbeda dengan target korban yang berada di negara lain pula.

Kejahatan siber (*cybercrime*) merupakan salah satu permasalahan yang muncul dari kemajuan teknologi yang memiliki akibat negatif dari kejahatan masa saat ini dan menjadi perhatian di dunia internasional. Umumnya kejahatan ini dikenal sebagai kejahatan dunia maya (*cyberspace or virtual ruang offence*), merupakan dimensi baru dari *high tech crime*, dimensi baru dari *transnational crime*, serta terakhir adalah dimensi baru dari *white collar crime*.

Secara terminologi, menurut Widodo, bahwa *cybercrime* diartikan sebagai kegiatan seseorang, sekelompok orang, badan hukum yang memakai komputer

[82] A. Aco Agus dan Riskawati, Penanganan Kasus Cybercrime di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar), *Jurnal Supremasi*, 10 (1) 2016, h 20

bagaikan fasilitas melakukan kejahatan, dan sebagai sasaran (target).[83] Dalam definisi lain, kejahatan dunia maya adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit, confidence fraud, penipuan identitas, pornografi anak, dan lain-lain. Walaupun kejahatan dunia maya atau cybercrime umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional dimana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.

Kejahatan siber dapat dilakukan tanpa memerlukan kontak antara pelaku dengan korban. Kejahatan dapat dilakukan dimana saja, tanpa memperhitungkan jarak antara pelaku dengan target kejahatan, sepanjang ada jaringan internet dan peralatan yang memadai. Mengenai karakteristik kejahatan siber tersebut Roderic Broadhurst, Peter Grabosky, Mamoun Alazab dan Steve Chon mengatakan mengatakan "*Cyber criminals may operate as loose networks, but evidence suggests that members are still located in close geographic proximity even when their attacks are cross-national. For example, small local networks, as well as groups centred on relatives and friends, remain significant actors*". (Penjahat siber dapat beroperasi sebagai jaringan longgar, namun bukti menunjukkan bahwa anggota masih berada dalam jarak dekat yang dekat

[83] Miftakhur Rokhman Habibi dan Isnatul Liviani, *Op.Cit*, 23 (2) Desember 2020, h 404

bahkan ketika serangan mereka lintas negara. Misalnya, jaringan lokal kecil, serta kelompok yang berpusat pada saudara dan teman, tetap merupakan aktor penting).[84]

Kejahatan yang dilakukan di ruang maya pada umumnya bertujuan untuk menghasilkan keuntungan finansial bagi pelakunya. Berbagai tindakan dilakukan untuk menyerang sistem keamanan di dunia maya untuk mendapatkan uang. Adapula pelaku yang menggunakan internet sebagai media untuk menghasilkan uang, misalnya penggunaan internet untuk perdagangan gelap senjata dan organ tubuh, prostitusi dan pornografi. Dalam perkembangannya, pelaku kejahatan menggunakan media internet sebagai sarana untuk menyerang pribadi seseorang tanpa secara langsung atau memang tidak bertujuan untuk keuntungan finansial, misalnya pencemaran nama baik melalui internet, *political hacking*, *cyberterrorism*, *cyberbullying* dan sebagainya.

Dalam *Federal Bureau of Investigation* (FBI) *Internet Crime Report* tahun 2024, merilis 20 negara tertinggi yang menjadi korban *cybercrime*. Data tersebut dapat dilihat pada tabel berikut ini:

Top 20 Foreign Countries with Citizens Submitting Complaints to IC3					
No	**Country**	**Complaints**	**No**	**Country**	**Complaints**
1	United Kingdom	102,692	**11**	Mexico	1,116
2	Canada	6,951	**12**	South Africa	1,075
3	India	4,189	**13**	Pakistan	979
4	France	2,223	**14**	Indonesia	895
5	Philippines	1,790	**15**	Italy	761
6	Australia	1,533	**16**	Sweden	732
7	Germany	1,524	**17**	China	651

[84] Roderic Broadhurst, Peter Grabosky, Mamoun Alazab dan Steve Chon, Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime, *International Journal of Cyber Criminology*, 8 (1) January-June 2014, h 3

8	Japan	1,492	**18**	Turkey	649
9	Brazil	1,472	**19**	Spain	639
10	Honduras	1,352	**20**	Netherlands	598

Sumber: FBI: Internet Crime Report 2024[85]

Indonesia sendiri termasuk dalam deretan 20 negara yang menjadi korban kejahatan siber tertinggi, namun juga menjadi negara asal dimana kejahatan siber dilakukan. Lona Olavia melaporkan "*Indonesia has received greater scrutiny from cybercrime authorities in recent years, especially since a 2013 survey by Akamai Technologies*, *an IT security firm, reported that Indonesia had overtaken China as the number one source of hacking traffic in the world*." (Indonesia telah mendapat pengawasan yang lebih besar dari pihak otoritas kejahatan siber beberapa tahun terakhir, terutama sejak survei tahun 2013 oleh *Akamai Technologies*, sebuah perusahaan keamanan TI, melaporkan bahwa Indonesia telah berhasil mengalahkan China sebagai sumber *hacking traffic* terbesar di dunia).[86]

Data tersebut tidak semata-mata diartikan bahwa pelaku berasal dari Indonesia, namun ada pelaku Warga Negara Asing yang melakukan kejahatan tersebut di Indonesia dengan menggunakan server Indonesia. Hal ini dilakukan karena pelaku melihat celah-celah hukum yang dapat diterobos oleh pelaku untuk terhindar dari jeratan hukum.[87]

[85] Chad Yarbrough, Federal Bureau of Investigation Internet Crime Report 2024, Washington DC, *Internet Crime Complaint Center (IC3) Annual Report*, 2024, h 16

[86] Dewi Bunga, Politik Hukum Pidana Terhadap Penanggulangan Cybercrime, *Jurnal Legislasi Indonesia,* 16 (1) Maret 2019, h 3

[87] *Ibid*

Berdasarkan jenis aktifitas yang dilakukannya, kejahatan siber dapat digolongkan menjadi beberapa jenis sebagai berikut:

No	Jenis Kejahatan Siber	Elaborasi
1	*Illegal Acces*/*Unauthorized access to Computer System and Service*	Merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. *Probing* dan *port* merupakan contoh kejahatan ini.[88]
2	*Illegal Contents*	Merupakan kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau menggangu ketertiban umum, contohnya adalah penyebaran pornografi, penjualan senjata api ilegal, jual beli narkotika, perjudian dan lain sebagainya.[89]
3	Penyebaran virus secara sengaja	Penyebaran virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.[90]
4	*Data Forgery*	Kejahatan jenis ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis *web database*.[91]
5	*Cyber Espionage*	Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak

[88] Dodo Zaenal Abidin, Kejahatan dalam Teknologi Informasi dan Komunikasi, *Jurnal Ilmiah Media Processor*, 10 (2) Oktober 2015, h 510

[89] Agung Yoga, Cyber Crime dan Upaya Penanggulangannya, *JAHE - Jurnal Akuntansi Hukum dan Edukasi*, 1 (1) Mei 2024, h 25

[90] Dodo Zaenal Abidin, *Op.Cit*, 10 (2) Oktober 2015, h 511

[91] *Ibid*

		lain, dengan memasuki sistem jaringan komputer pihak sasaran.[92]
6	*Cyber Sabotage and Extortion* (sabotase dan pemerasan dunia maya)	Dalam jenis kejahatan ini, modus biasanya dijalankan dengan mengganggu, merusak, atau menghancurkan data yang terhubung ke internet, program komputer, atau sistem jaringan komputer. Biasanya kejahatan semacam ini dilakukan dengan cara memasukkan *logic bomb*, virus komputer atau program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan dan tidak dapat beroperasi secara normal atau tidak dapat berjalan, tetapi telah dikendalikan oleh penjahat sesuai kebutuhan.[93]
7	*Cyberstalking*	Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya.[94]
8	*Carding*	Merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.[95]
9	*Hacking* dan *Cracker*	Istilah *hacker* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut

[92] *Ibid*
[93] Fiorida Mathilda, *Op.Cit,* 4 (2) September 2012, h 36
[94] Dodo Zaenal Abidin, *Op.Cit*, 10 (2) Oktober 2015, h 511
[95] *Ibid*

		cracker. Boleh dibilang *cracker* ini sebenarnya adalah *hacker* yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas *cracking* di internet memiliki lingkup yang sangat luas, mulai dari pembajakan *account* milik orang lain, pembajakan situs *web*, *probing*, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (*Denial Of Service*). *Dos attack* merupakan serangan yang bertujuan melumpuhkan target (*hang*, *crash*) sehingga tidak dapat memberikan layanan.[96]
10	*Cybersquatting and Typosquatting*	*Cybersquatting* merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun *typosquatting* adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan.[97]
11	*Hijacking*	*Hijacking* merupakan kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah *Software Piracy* (pembajakan perangkat lunak).[98]
12	*Cyber Terorism*	Suatu tindakan *cybercrime* termasuk *cyber terorism* jika mengancam pemerintah atau warganegara, termasuk cracking ke situs pemerintah atau militer. Beberapa contoh kasus *Cyber Terorism* antara lain Ramzi Yousef, dalang penyerangan pertama ke gedung WTC diketahui menyimpan detail serangan dalam file yang di enkripsi di

[96] *Ibid*
[97] *Ibid*
[98] *Ibid*

		laptopnya, suatu website yang dinamai *Club Hacker Muslim* diketahui menuliskan daftar tip untuk melakukan hacking ke Pentagon.[99]
13	*Defacing*	Di antara tindakan *cyber crime* sebelumnya, *Defacing* bisa dibilang menjadi aktivitas kejahatan online yang paling ringan. Hal tersebut salah satunya karena para pelaku *deface* biasanya menyasar *website-website non-profit* seperti situs pemerintahan, sekolah, atau universitas.[100]

Untuk mengatasi Kejahatan siber (*cybercrime*) dibutuhkan keberadaan dari hukum siber (*cyber*) ataupun diketahui dengan nama *cyber law*. Di era perkembangan teknologi dewasa ini dalam pembuatan peraturan perundang- undangan dibutuhkan pertimbangan pembuatan peraturan tersebut dari berbagai aspek. Contohnya dapat kita telaah melalui ranah pemanfaatan dan pengembangan jurudiksi serta konflik hukum, internet beserta *rule of law*, legalitas hukum tentang dokumen beserta tanda tangan elektronik, metode penyelesaian sengketa domain dan pengaturan konten, dan proteksi konsumen melalui privasi, lebih lanjut hal yang berkaitan dengan Kejahatan siber (*cybercrime*).[101]

Oleh karenanya muncul aturan hukum tentang kejahatan siber yang di latar belakangi oleh alasan perkembangan zaman dan perubahan sosial di masyarakat yang memacu Indonesia untuk memiliki *Cyber Law* mengingat hukum-hukum tradisional

[99] Dodo Zaenal Abidin, *Op.Cit*, 10 (2) Oktober 2015, h 512
[100] Agung Yoga, *Op.Cit,* 1 (1) Mei 2024, h 25
[101] Lalu Heru Sujamawardi, Analisis Yuridis Pasal 27 Ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, *Dialogia Juridica: Jurnal Hukum Bisnis dan Investasi*, 9 (2) 2018, h 84-100.

sudah tidak dapat dan tidak mampu mengantisipasi perkembangan dunia siber atau dunia maya yang semakin pesat.[102]

Transformasi politik hukum di Indonesia menjadi elemen krusial dalam memperkuat regulasi *cyber law* untuk menghadapi perkembangan teknologi dan meningkatnya ancaman kejahatan siber. Perkembangan pesat teknologi informasi telah mendorong Indonesia untuk segera menyesuaikan regulasi hukum guna melindungi masyarakat dan infrastruktur digital dari berbagai bentuk kejahatan siber. Kondisi ini menuntut peran aktif politik hukum dalam membentuk kerangka regulasi yang adaptif dan efektif.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diperbarui melalui Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024, menjadi produk politik hukum nasional dalam mengakomodir norma hukum pidana terhadap beberapa jenis kejahatan siber yang terjadi di Indonesia.

1. Kesusilaan

Jenis kejahatan ini yang diterapkan pada ruang lingkup siber diakomodir pada ketentuan dalam Pasal 27 Ayat (1) bahwa setiap Orang dengan sengaja dan tanpa hak menyiarkan, mempertunjukkan, mendistribusikan,

[102] Sherly Nelsa Fitri, Politik Hukum Pembentukan Cyber Law Undang-Undang Informasi dan Transaksi Elektronik di Indonesia, *Jurnal Justisia: Jurnal Ilmu Hukum, Perundang-undangan dan Pranata Sosial,* 7 (1) 2022, h 113

mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan untuk diketahui umum dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rpl.000.000.000,00 (satu miliar rupiah).[103]

2. Perjudian Online

Jenis kejahatan ini yang diterapkan pada ruang lingkup siber diakomodir pada ketentuan dalam Pasal 27 Ayat (2) bahwa setiap Orang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).[104]

3. Penghinaan atau pencemaran nama baik

Jenis kejahatan ini yang diterapkan pada ruang lingkup siber diakomodir pada ketentuan dalam Pasal 27A bahwa setiap Orang dengan sengaja menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal, dengan maksud supaya hal tersebut diketahui umum

[103] Pasal 27 Ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[104] Pasal 27 Ayat (2) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

dalam bentuk Informasi Elektronik dan/ atau Dokumen Elektronik yang dilakukan melalui Sistem Elektronik dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/ atau denda paling banyak Rp400.000.000,00 (empat ratus juta rupiah). Adapun ketentuan tersebut merupakan tindak pidana aduan yang hanya dapat dituntut atas pengaduan korban atau orang yang terkena tindak pidana dan bukan oleh badan hukum.[105]

Pembuat undang-undang sendiri kelihatannya mau mengarahkan perbuatan penghinaan dari media internet tersebut sebagai pencemaran. Menurut Adami Chazawi, kejahatan penghinaan terdiri dari penghinaan umum dan penghinaan khusus. Penghinaan umum mengacu pada obyek harga diri dan derajat orang pribadi, termasuk juga pencemaran. Sedangkan penghinaan khusus mengacu pada penghinaan yang memiliki obyek harga diri, kehormatan dan nama baik terbuka (umum).[106]

Tindakan penghinaan ataupun pencemaran dalam ruang siber dapat ditemukan di berbagai kolom komentar di media sosial, terutama ketika korban memindai identitas, foto, atau video pribadinya. Pelaku juga dapat menulis teks yang menghina atau memfitnah di dinding pernyataan untuk membuat pernyataan atau menghubungkan pernyataan tersebut dengan korban.[107]

---

[105] Pasal 27A dan Pasal 45 Ayat (5) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[106] Adami Chazawi, *Hukum Pidana Positif Penghinaan*, Edisi Revisi, Malang: Media Nusa Creative, 2013, h 81.

[107] Miftakhur Rokhman Habibi dan Isnatul Liviani, *Op.Cit*, 23 (2) Desember 2020, h 416

4. Pemerasan

Jenis kejahatan ini yang diterapkan pada ruang lingkup siber diakomodir pada ketentuan dalam Pasal 27B bahwa setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik, dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa orang dengan ancaman kekerasan untuk (a) memberikan suatu barang, yang sebagian atau seluruhnya milik orang tersebut atau milik orang lain; atau (b) memberi utang, membuat pengakuan utang, atau menghapuskan piutang dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).[108]

5. Penyebaran berita palsu atau bohong (*hoax*) mengakibatkan kerugian Konsumen

Jenis kejahatan ini yang diterapkan pada ruang lingkup siber diakomodir pada ketentuan dalam Pasal 28 Ayat (1) bahwa setiap Orang dengan sengaja mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/ atau Dokumen Elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiel bagi konsumen dalam

[108] Pasal 27B dan Pasal 45 Ayat (5) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Transaksi Elektronik dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).[109]

6. **Penyebaran berita palsu atau bohong (*hoax*) menimbulkan kerusuhan masyarakat**

   Jenis kejahatan ini yang diterapkan pada ruang lingkup siber diakomodir pada ketentuan dalam Pasal 28 Ayat (3) bahwa setiap Orang dengan sengaja menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik yang diketahuinya memuat pemberitahuan bohong yang menimbulkan kerusuhan di masyarakat dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).[110]

7. **Ujaran kebencian SARA**

   Jenis kejahatan ini yang diterapkan pada ruang lingkup siber diakomodir pada ketentuan dalam Pasal 28 Ayat (2) bahwa setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang sifatnya menghasut, mengajak, atau memengaruhi orang lain sehingga menimbulkan rasa kebencian atau permusuhan terhadap individu dan/atau kelompok masyarakat tertentu berdasarkan ras, kebangsaan, etnis, warna kulit, agama, kepercayaan, jenis

[109] Pasal 28 Ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[110] Pasal 28 Ayat (3) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

kelamin, disabilitas mental, atau disabilitas fisik dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).[111]

8. Penguntitan (*cyberstalking*)

Jenis kejahatan ini yang diterapkan pada ruang lingkup siber diakomodir pada ketentuan dalam Pasal 29 bahwa setiap Orang dengan sengaja dan tanpa hak Informasi Elektronik dan/atau Dokumen Elektronik secara langsung kepada korban yang berisi ancaman kekerasan dan/ atau menakut-nakuti dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/ atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).[112]

9. *Cracking*, *Hacking*, *Illegal Access*

Jenis kejahatan ini yang diterapkan pada ruang lingkup siber diakomodir pada ketentuan dalam Pasal 30 bahwa setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan dipidana berdasarkan perbuatan Pasal 30 Ayat (1) dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam

[111] Pasal 28 Ayat (2) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[112] Pasal 29 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

ratus juta rupiah), dipidana berdasarkan perbuatan Pasal 30 Ayat (2) dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah), dipidana berdasarkan perbuatan Pasal 30 Ayat (3) dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).[113]

10. Penyadapan (Intersepsi)

Jenis kejahatan ini yang diterapkan pada ruang lingkup siber diakomodir pada ketentuan dalam Pasal 31 Ayat (1) dan (2) bahwa setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).[114]

[113] Pasal 30 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[114] Pasal 31 Ayat (1) dan (2) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Dalam Penjelasan Pasal tersebut yang dimaksud dengan "intersepsi atau penyadapan" adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi.[115]

11. Perusakan data atau Informasi elektronik (*Data interference*)

Jenis kejahatan ini yang diterapkan pada ruang lingkup siber diakomodir pada ketentuan dalam Pasal 32 bahwa setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik dan mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya dipidana berdasarkan perbuatan Pasal 32 ayat (1) dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah), dipidana berdasarkan perbuatan Pasal 32 ayat (2) dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah,

[115] Dewi Bunga, *Op.Cit,* 16 (1) Maret 2019, h 7

serta dipidana berdasarkan perbuatan Pasal 32 ayat (3) dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).[116]

12. Mengganggu sistem elektronik (*System interference*)

Jenis kejahatan ini yang diterapkan pada ruang lingkup siber diakomodir pada ketentuan dalam Pasal 33 bahwa setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

13. Penyalahgunaan perangkat atau *misuse of devices*

Jenis kejahatan ini yang diterapkan pada ruang lingkup siber diakomodir pada ketentuan dalam Pasal 34 Ayat (1) bahwa 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 dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan pada Pasal 27 sampai Pasal 33 serta sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan

[116] Pasal 32 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

tujuan memfasilitasi perbuatan dalam Pasal 27 sampai Pasal 33 dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).[117]

14. Penipuan situs/ *Phising* (Data Forgery)

Jenis kejahatan ini yang diterapkan pada ruang lingkup siber diakomodir pada ketentuan dalam Pasal 35 bahwa setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).[118]

Terdapat beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku kejahatan siber terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana, antara lain:

1) KUHP
2) Undang-Undang Nomor 44 tahun 2008 tentang Pornografi
3) Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi
4) Undang-undang Nomor 28 Tahun 2014 tentang Hak Cipta

[117] Pasal 34 Ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[118] Pasal 35 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

5) Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan.
6) Undang-undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang;
7) Undang-undang Nomor 5 Tahun 2018 tentang Perubahan atas Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang.[119]

Dalam lingkup *cyber terrorism*, Undang-Undang Pemberantasan Tindak Pidana Terorisme mengatur mengenai alat bukti elektronik sesuai dengan Pasal 27 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu. *Digital evidence* atau alat bukti elektronik sangatlah berperan dalam penyelidikan kasus terorisme. Karena saat ini komunikasi antara para pelaku di lapangan dengan pimpinan atau aktor intelektualnya dilakukan dengan memanfaatkan fasilitas di Internet untuk menerima perintah atau menyampaikan kondisi di lapangan karena para pelaku mengetahui. pelacakan terhadap Internet lebih sulit dibandingkan pelacakan melalui handphone. Fasilitas yang sering digunakan adalah e-mail dan chat roomselain mencari informasi dengan menggunakan *search engine* serta melakukan propaganda melalui *bulletin board* atau *mailing list.*

[119] Bonaventura Deogratia Manorek, dkk. Penegakan Hukum Pidana dalam Memberantas Kejahatan Pencurian Data Elektronik (Phising), *Lex Privatum,* 15 (2) Februari 2025, h 4

Kejahatan siber memerlukan penindakan dan perhatian khusus dari pemerintah sebab kejahatan tersebut bisa terjadi dari wilayah atau negara manapun. Adanya ketergantungan dan kurangnya pengetahuan terhadap fungsi teknologi membuat masyarakat khususnya menjadi pihak yang paling rentan atau mudah menjadi korban kejahatan siber yang dapat merugikan mereka baik secara materiil maupun moriil.[120] Banyak kejahatan siber yang sering terjadi dan merugikan masyarakat. Hal ini disebabkan besarnya ketergantungan masyarakat terhadap teknologi yang semakin berkembang serta kurangnya pengetahuan tentang teknologi. Ketergantungan dan kurang pengetahuan inilah yang membuat masyarakat mudah untuk dijadikan korban kejahatan siber yang merugikan.

Dari berbagai telaah produk kebijakan hukum pidana tersebut, maka dapat teramati dengan jelas bahwasanya perlindungan dunia digital di Indonesia masih bersifat parsial dan belum terintegrasi secara optimal. Faktor tersebut pada akhirnya memunculkan tantangan berkaitan dengan sumber daya manusia yang berkualitas dapat menciptakan cara berpikir yang positif terhadap perubahan lingkungan global serta meningkatkan kesadaran terhadap perkembangan teknologi dan informasi.[121] Selain itu, Indonesia juga perlu memiliki fasilitas atau perangkat pengamanan negara yang lebih memadai. Fasilitas tersebut mencakup infrastruktur dan teknologi yang

[120] Kristiani Virgi Kusuma Putri, Kerja Sama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime, *Rewang Rencang : Jurnal Hukum Lex Generalis*, 2 (7), 2021

[121] Handrini Ardiyanti, Cyber-Security dan Tantangan Pengembangannya di Indonesia, *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, 5 (1) Juni 2014, h 108

diperlukan untuk mendeteksi, mencegah, dan menanggulangi serangan siber. Investasi dalam pengembangan fasilitas pengamanan negara yang mutakhir dan efektif menjadi penting guna menghadapi ancaman kejahatan siber yang semakin kompleks dan terus berkembang.

B. Skema Penentuan Locus Delicti dalam Penyidikan Kejahatan Siber

Pada ruang lingkup peradilan pidana suatu negara, Dasar Hukum Acara Pidana membentang sebagai fondasi yang kokoh, menentukan kerangka hukum yang mengatur seluruh proses penegakan hukum terhadap tindak pidana. Merangkum prinsip-prinsip yang mengikat dan norma-norma yang mendasari, Dasar Hukum Acara Pidana tidak hanya menjadi panduan praktis bagi pelaksanaan keadilan, tetapi juga mencerminkan nilai-nilai mendasar yang harus dijunjung tinggi dalam menjaga keseimbangan antara penegakan hukum yang tegas dan perlindungan hak asasi individu.[122]

Di dalam penegakan hukum pada hakikatnya tidak terlepas dengan bagaimana negara menjamin atau memberikan ketentraman kepada warga masyarakat apabila tersangkut masalah hukum. Penegakan hukum juga merupakan usaha atau upaya untuk menciptakan keadilan. Menurut Bagir Manan pengertian penegakan hukum adalah mencakup tugas dan wewenang mempertahankan hukum (*and having can het recht*) terhadap seseorang atau sekelompok orang yang melanggar hukum atau melakukan

[122] Husamuddin, et.al. *Hukum Acara Pidana dan Pidana Cyber*, Medan: PT Media Penerbit Indonesia, 2024, h 17

perbuatan melawan hukum atau pengingkaran sesuatu perikatan hukum termasuk menegakkan hukum, yaitu perbuatan menetapkan hukum mengenai hal-hal seperti status objek atau benda. Baik secara teori maupun praktek, pengertian tradisional ini tidak lengkap karena konotasi penegak hukum hanya dengan tindakan represif (penindakan) belaka. Sedangkan dalam pengertian yang lebih luas, penegakan hukum mencakup juga tindakan preventif pencegahan bahkan lebih luas dari itu.[123]

Penegakan hukum sebagai bentuk konkrit penegakan hukum sangat mempengaruhi perasaan hukum secara nyata, kepuasan hukum, manfaat hukum atau keadilan hukum baik secara individu maupun dalam masyarakat. Tetapi karena penegakan hukum tidak terlepas dari aturan-aturan hukum yang ada, para penegak hukum tempat terjadinya hukum diproses maka tidak mungkin masalah penegak hukum bisa dipandang sebagai suatu hal yang tegak berdiri sendiri. [124] Menurut Sudarto, penegakan hukum di bidang hukum pidana didukung oleh alat perlengkapan dan peraturan yang relatif lebih lengkap dari penegakan hukum di bidang-bidang lainnya. Aparatur yang dimaksud disini adalah Kepolisian, Kejaksaan, peradilan dan aparat eksekusi pidana, sedang peraturan-peraturan yang ada dikatakan lebih lengkap.[125]

---

[123] Bagir Manan, Varia Peradilan, *Majalah Hukum*, Tahun ke XXI No.243, Februari 2006, h 4

[124] Hibnu Nugroho, Merekonstruksi Sistem Penyidikan dalam Peradilan Pidana (Studi tentang Kewenangan Penyidik Menuju Pluralisme Sistem Penyidikan di Indonesia), *Jurnal Hukum Pro Justitia*, 26 (1) Januari 2008, h 16

[125] Sudarto, *Kapita Selekta Hukum Pidana*, Bandung: Alumni, 1986, h 112

Pada sistem hukum modern ini, keadilan (*justice*) sudah dianggap diberikan dengan membuat hukum positif (undang-undang). Dengan kata lain, keadilan yang akan ditegakkan ditentukan melalui hukum positif (undang-undang). Dalam konteks sosial kemasyarakatan, hubungan-hubungan dan tindakan-tindakan pemerintah ke pada warga negaranya didasarkan pada peraturan dan prosedur yang bersifat inpersonal dan impartial. Berdasarkan ini kemudian muncul konsepsi *the rule of law*.[126]

Penyidikan merupakan bagian awal dari proses penegakan hukum pidana, kedudukan penyidikan sangat penting mengingat proses ini menentukan berhasil tidaknya proses selanjutnya. Penyidikan adalah suatu sebutan yang memiliki persamaan makna atau pengertian dengan definisi dari Bahasa belanda yaitu *opsporing* dan dalam Bahasa Inggris *investigation* serta dalam Bahasa Malaysia *Penyiasatan*.[127] Istilah penyidikan dalam Bahasa Indonesia memiliki kata dasar "sidik". Sidik berarti terang, jadi menyidik berarti membuat terang atau jelas. Kata sidik berarti juga berkas yang kita jumpai dalam sidik jari, bekas jari atau telapak jari, sehingga menyidik juga berarti mencari bekas, dalam hal ini berarti bekas-bekas kejahatan.[128]

Secara lebih rinci, R. Soesilo mengemukakakn pendapatnya bahwa:

Bertolak dari kedua arti yaitu "terang dan "bekas", maka menyidik berarti membuat terang kejahatan. Untuk itu, kadangkala digunakan kata mengusut atau menyelidiki. Orang Belanda mengistilahkan *Opsporen*, dalam Bahasa Inggris disebut *Investigation*,

[126] Adji Samekto, Perkembangan Ranah Kajian Ilmu Hukum, Semarang: UNDIP, *Orasi Ilmiah*, 9 Januari 2005, h 14

[127] Dani Septian Nugroho dan Margo Hadi Pura, Faktor Hambatan Penyidikan dalam Kasus Tindak Pidana Cybercrime, *Veritas: Jurnal Program Pascasarjana Ilmu Hukum*, 8 (1) 2022, h 39

[128] Hibnu Nugroho, *Op.Cit*, 26 (1) Januari 2008, h 17

arti lengkapnya adalah mengusut sehingga dapat diketahui peristiwa pidana apa yang telah terjadi dan siapakah orang yang telah berbuat.[129]

Menurut de Pinto, menyidik (*opsporing*) berarti "pemeriksaan permulaan oleh pejabat-pejabat yang untuk itu ditunjuk oleh undang-undang segera setelah mereka dengan jalan apapun mendengar kabar yang sekedar beralasan, bahwa ada terjadi sesuatu pelanggaran hukum". Sementara itu, Rahmadhan Kasim dan Apriyanti Nusa menyatakan bahwa filosofi tindakan penyidikan esensinya untuk mencari dan mengumpulkan bukti, yang dengan bukti tersebut ditemukan siapa tersangkanya.[130]

Dari kutipan tersebut dapat disimpulkan bahwa menyidik yaitu kegiatan yang dilakukan oleh pejabat-pejabat dengan mendengar telah terjadi suatu tindak pidana untuk dilakukan pemeriksaan permulaan sesuai dengan peraturan yang mengatur. Dan penyidikan memiliki fungsi dimana dilakukan penyidikan untuk mencari dan mengumpulkan bukti-bukti yang ada dalam tindak pidana yang terjadi sehingga dari bukti-bukti yang didapatkan ditemukan pelaku dalam tindak pidana tersebut.

Secara yuridis berdasarkan Pasal 1 angka 2 KUHAP (Kitab Undang-Undang Hukum Acara Pidana) 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 menentukan tersangkanya.

---

[129] R. Soesilo, *Taktik dan Teknik Penyidikan Perkara Kriminal,* Bandung: Karya Nusantara, 1980, h 17

[130] Febri dan Yetisma Saini. *Op.Cit*. 2022. h 30.

Menurut Pasal 1 angka 1 KUHAP (Kitab Undang-Undang Hukum Acara Pidana) penyidik adalah Pejabat polisi Negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh undang-undang untuk melakukan penyidikan.

Penyidik pejabat polisi negara republik Indonesia karena kewajibannya dalam melaksanakan penyidikan memiliki wewenang sebagai berikut:

a. Menerima laporan atau pengaduan dari seorang tentang adanya tindak pidana;
b. Melakukan tindakan pertama pada saat di tempat kejadian;
c. Menyuruh berhenti seorang tersangka dan memeriksa tanda pengenal diri tersangka;
d. Melakukan penangkapan, penahanan, penggeledahan, dan penyitaan;
e. Melakukan pemeriksaan dan penyitaan surat;
f. Mengambil sidik jari dan memotret seorang;
g. Memanggil orang untuk didengar dan diperiksa sebagai tersangka atau saksi;
h. Mendatangkan orang ahli yang diperlukan dalam hubungannya dengan pemeriksaan perkara;
i. Mengadakan penghentian penyidikan;
j. Mengadakan tindakan lain menurut hukum yang bertanggung jawab.[131]

Wewenang yang disebutkan di atas merupakan kegiatan penyidik yang diatur dalam kitab undang-undang hukum acara pidana dalam melakukan penyidikan.

[131] Pasal 7 ayat 1 KUHAP

Penyidik dalam melaksanakan tugas penyidikan harus berpegang teguh dengan wewenang yang telah diberikan oleh undang-undang sehingga tidak terjadinya penyimpangan wewenang yang dilakukan oleh penyidik dalam melaksanakan tugasnya.

Pada tahap penyelidikan, penekanan diletakkan pada "mencari dan menemukan suatu peristiwa tindak pidana". Sedangkan pada tahap penyidikan, penekanannya diletakkan pada tindakan "mencari dan mengumpukan bukti-bukti" agar tindak pidana menjadi terang serta agar dapat menemukan siapa pelakunya. Pada Pasal 184 Undang-Undang No.8 Tahun 1981 dalam hal mencari serta mengumpulkan alat-alat bukti yang sah meliputi keterangan saksi, keterangan ahli, surat, petunjuk, keterangan terdakwa.

Pelaksanaan penyidikan yang baik akan dapat menentukan keberhasilan penuntutan oleh Jaksa Penuntut Umum di depan persidangan, namun tentunya penegakan hukum itu sendiri tergantung pada komitmen para hakim yang memutus dan memeriksa perkaranya.[132]

Dalam bidang reserse kriminal penyidikan dibedakan menjadi dua, yaitu:

a. Penyidikan dalam arti luas yang meliputi penyidikan, pengusutan dan pemeriksaan, yang sekaligus rangkaian dari tindakan-tindakan terus menerus, tidak ada pangkal permulaan dan penyelesaiannya.

[132] Hibnu Nugroho, *Op.Cit*, 26 (1) Januari 2008, h 20

b. Penyidikan dalam arti sempit, yaitu semua tindakan-tindakan yang merupakan suatu bentuk operasi represif dari reserse kriminal Polri yang merupakan permulaan dari pemeriksaan perkara pidana.[133]

Penyidikan dijelaskan pada Undang-Undang No. 8 Tahun 1981 tentang Hukum Acara Pidana sebagai hukum formil pidana secara umum, dan selain KUHAP juga dalam Undang-Undang No. 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia menjelaskan mengenai penyelidikan dan penyidikan yang mana penjelasannya juga merujuk pada KUHAP. Pada penyidikan tindak pidana, Polri menggunakan parameter alat bukti yang sah sesuai dengan Pasal 184 KUHAP yang dikaitkan dengan segi tiga pembuktian/*evidence triangle* untuk memenuhi aspek legalitas dan aspek legitimasi untuk membuktikan tindak pidana yang terjadi, adapun rangkaian kegiatan penyidik dalam melakukan penyidikan adalah Penyelidikan, Penindakan, pemeriksaan dan penyelesaian berkas perkara.

Dalam konteks peradilan pidana, pintu masuk untuk dapat ditegakkannya hukum dan keadilan (*access to justice*) adalah melalui penyelidikan dan penyidikan. Hal ini diawali dengan adanya Laporan atau Pengaduan yang disampaikan kepada aparat penegak hukum. Kemudian berdasarkan Laporan atau Pengaduan tersebut dilakukan tindakan lebih lanjut berupa Penyelidikan yang dilakukan oleh Penyelidik. Proses Penyelidikan dan Penyidikan secara rinci diatur dalam Bab XIV mengenai

[133] R. Soesilo, *Op.Cit*, 1980

Penyidikan yaitu Pasal 102-136 KUHAP.[134] Terdapat juga wewenang lainya yang harus berdasarkan perintah dari Penyidik, yaitu:

1) Penangkapan, larangan meninggalkan tempat, penggeledahan dan penahanan;
2) Pemeriksaan dan penyitaan surat;
3) Mengambil sidik jari dan memotret seorang;
4) Membawa dan menghadapkan seorang pada penyidik.

Seorang Penyelidik membuat dan menyampaikan laporan hasil dari tindakannya tersebut kepada Penyidik. Setelah menerima laporan dari Penyelidik, dalam hal Penyidik telah memulai Penyidikan terhadap peristiwa yang merupakan tindak pidana, Penyidik memberitahukan hal tersebut kepada penuntut umum, terlapor, korban/pelapor paling lambat 7 (tujuh) hari setelah dikeluarkannya Surat Perintah Dimulainya Penyidikan (SPDP).[135]

Lebih lanjut seorang Penyidik kemudian melakukan kegiatan pemeriksaan dengan memanggil tersangka dan saksi yang dianggap perlu untuk diperiksa berdasarkan surat panggilan yang sah. Orang yang dipanggil wajib datang kepada Penyidik, dan jika orang tersebut tidak dapat datang, kemudian dipanggil kembali berdasarkan pemanggilan yang patut, apabila tidak kunjung datang, maka berdasarkan Pasal 112 ayat (2) Penyidik dapat memberikan perintah kepada petugasnya untuk membawa orang tersebut kepadanya.

---

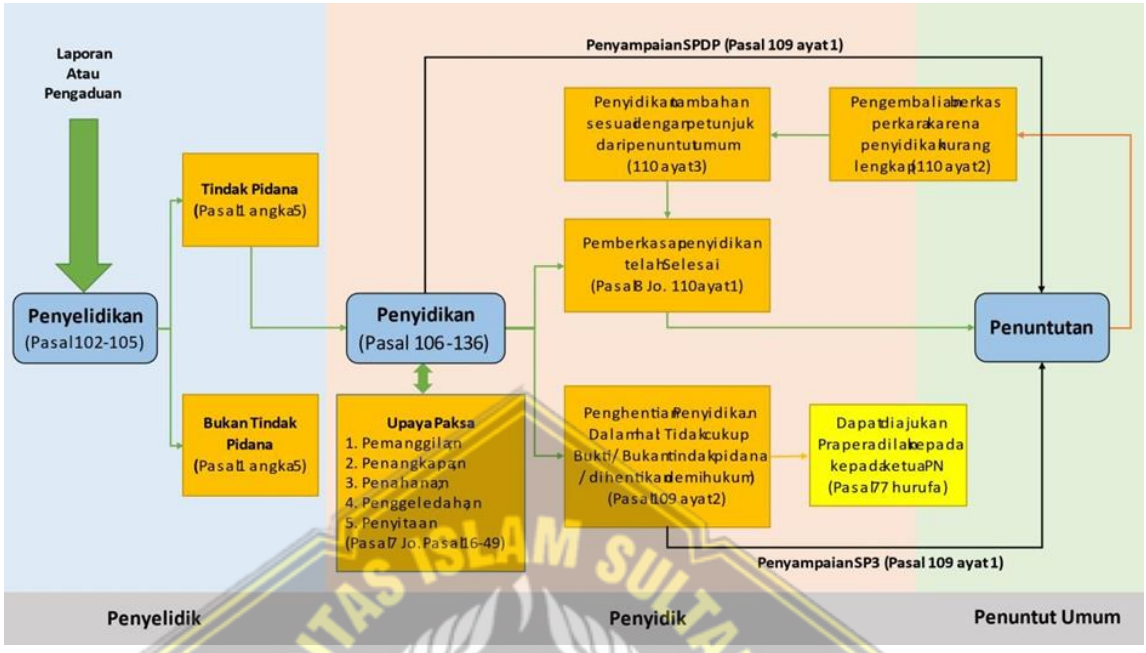
[134] Kementerian Hukum dan HAM RI, Analisis dan Evaluasi Hukum Acara Pidana: Penyelidikan dan Penyidikan (Undang-Undang No 8 Tahun 1981 tentang Hukum Acara Pidana), Pusat Analisis dan Evaluasi Hukum Nasional, BPHN Kemenkumham, *Laporan Akhir*, 2022, h 24

[135] Putusan Mahkamah Konstitusi Nomor 130/PUU-XIII/2015

Setelah proses Penyidikan telah selesai, Penyidik wajib segera untuk menyerahkan berkas perkara tersebut kepada Penuntut Umum. Apabila penuntut umum berpendapat hasil Penyidikan yang telah dilakukan masih kurang lengkap, Penuntut umum segera mengembalikan berkas perkara tersebut kepada Penyidik dan disertai dengan Petunjuk untuk dilengkapi. Kemudian setelah menerima kembali berkas tersebut, Penyidik wajib segera melakukan Penyidikan tambahan sesuai dengan petunjuk dari Penuntut Umum.

Berdasarkan Pasal 100 ayat (4) KUHAP Penyidikan dianggap telah selesai apabila dalam waktu 14 (empat belas) hari Penuntut Umum tidak mengembalikan hasil Penyidikan atau apabila sebelum batas waktu tersebut berakhir terdapat pemberitahuan mengenai hal tersebut dari Penuntut Umum kepada Penyidik. Berdasarkan hal tersebut, agar lebih mudah dipahami, gambaran alur proses Penyidikan berdasarkan KUHAP adalah sebagai berikut:[136]

[136] Kementerian Hukum dan HAM RI, *Op.Cit*, 2022, h 27



Bagan Alur Proses Penyidikan

Adapun kewenangan melakukan Penyidikan pada perkara tindak pidana khusus oleh Kepolisian diatur pula pada Undang-Undang Nomor 8 Tahun 1981 Tentang KUHAP, dijelaskan bahwa Penyidik adalah Pejabat Polisi Negara Republik Indonesia. Penyidik menurut KUHAP berwenang melakukan penyidikan tindak pidana yang terjadi, dimana Pasal 1 ayat (1) dan (2) dan di dalam ketentuan tersebut belum mengenal istilah pidana umum atau pidana khusus, dengan demikian setiap perbuatan yang melawan hukum dan diancam dengan pidana baik yang ada di dalam maupun di luar KUHP (pidana khusus).[137]

Dalam hal ini kejahatan siber merupakan tindak pidana yang bersifat khusus dengan diakomodirnya tindak pidana tersebut dengan sebuah produk hukum undang-

[137] Wawan Sanjaya, Sinkronasi Penyelidikan dan Penyidikan oleh POLRI, Kejaksaan dan KPK Terhadap Pelaku Tindak Pidana Korupsi, *Jurnal de Jure*, 1 (15) Januari 2018, h 17

undang tersendiri guna menerapkan norma-norma hukum berupa ketentuan formil dan materiil. Tindak pidana siber merupakan tindakan tindak pidana yang berhubungan dan berkaitan dengan dunia maya dan tindakan tindak pidana yang menggunakan komputer. Bila seseorang menggunakan komputer atau bagian dari jaringan komputer secara menyalahi Undang-Undang maka tindakan tersebut sudah tergolong pada tindak pidana siber. Indonesia tidak memiliki definisi hukum untuk kejahatan siber. Sebenarnya, Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) adalah undang-undang administratif. Namun, legislator memasukkan beberapa ketentuan tentang tindak pidana.[138] Dengan adanya ketentuan tindak pidana muncul pula sanksi pidana sebagai relevansi kedua aspek norma hukum pidana tersebut. Artinya setiap ketentuan pidana menciptakan sistem bekerjanya subsistem peradilan pidana dalam melaksanakan proses kriminalisasi sebagai representasi penegakan hukum terhadap kejahatan siber.

Proses penyidikan kejahatan siber merupakan langkah-langkah kritis yang dilakukan oleh aparat penegak hukum untuk mengungkap dan menindaklanjuti kejahatan siber. Keberhasilan dalam menangani kejahatan siber melibatkan penggunaan metodologi khusus dan kolaborasi yang erat dengan pihak-pihak terkait.[139] Menurut Michael R. Overly menekankan pentingnya proses penyelidikan dan

[138] Marselinus Goa dan Hudi Yusuf, Analisis Penipuan Online Melalui Media Sosial Dalam Kasus Kejahatan Belanja Online di Wilayah Jawa Timur, *Media Hukum Indonesia (MHI),* 3 (3) July 2025, h 759

[139] Husamuddin, et.al. *Op.Cit*, 2024, h 79

penyidikan *cybercrime* yang proaktif. Ia menyoroti bahwa organisasi perlu memiliki tim yang terlatih dan prosedur yang efektif untuk merespons serangan siber.[140]

Proses penyidikan tindak pidana siber melibatkan pelaporan korban kepada penyidik, yang kemudian melanjutkan kasus ke penuntut umum untuk dibawa ke pengadilan. Jika penyidik berasal dari PPNS, hasil penyidikan disampaikan melalui penyidik POLRI. Proses ini berlaku baik untuk tindak pidana siber dalam arti luas maupun sempit.[141] Selain UU ITE, dasar hukum penanganan tindak pidana siber di Indonesia juga mencakup peraturan pelaksana UU ITE, KUHAP, dan berbagai aturan teknis di masing-masing instansi penyidik. Pengaturan ini memastikan kelancaran proses hukum sembari tetap menjaga kepentingan publik dan keutuhan sistem elektronik.[142]

Mekanisme penyidikan tindak pidana siber diatur dalam UU ITE dan beberapa peraturan pelaksanaannya. Kepolisian memiliki peran utama dalam penyidikan, mulai dari penerimaan laporan, pengumpulan bukti digital, hingga identifikasi dan penangkapan pelaku. [143] Namun demikian kejahatan-kejahatan siber (cybercrime) memiliki kompleksitas masing-masing ketika proses penyidikan berlangsung mengharuskan adanya *locus delicti* yang jelas. *Locus Delicti* ini penting karena selain

---

[140] Georgia Institute of Technology, *Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers*, Chicago, Illinois; Caxton Business & Legal, Inc. 2015

[141] Andi Rania Risya Zamayya, dkk. Kajian Teoritis Implikasi The United Nations Convention Against Cybercrime Terhadap Pengaturan Tindak Pidana Siber Indonesia, *Ikraith-Humaniora*, 9 (2) Juli 2025, h 349

[142] *Ibid*

[143] Siti Hailatul Umami dan Abshoril Fithry, Mekanisme Penyidikan dan Penuntutan Tindak Pidana Cybercrime: Tinjauan Hukum Indonesia, *Prosiding Seminar Nasional Penelitian dan Pengabdian Masyarakat 2 Tahun 2023*, Sumenep 5-6 Desember 2023, h 116

undang-undang mengharuskan surat dakwaan menyebutkan *locus delicti* yang jelas, *locus delicti* juga penting untuk menentukan keberlakuan hukum, yurisdiksi atau kompetensi relatif. Padahal dalam kasus-kasus *cyber crime*, penentuan locus delicti tidak sesederhana pada kasus-kasus kejahatan-tradisional atau kejahatan yang lainnya.

Fenomena kejahatan siber ini juga menjadi polemik untuk menjatuhkan pidana pada kejahatan siber nantinya yang dipakai apakah KUHP atau Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang akan dipakai untuk menjerat pelaku kejahatan siber. Hal ini masih menjadi perdebatan juga yakni mengenai penentuan *locus delicti* yang nantinya diperlukan untuk menentukan apakah undang-undang pidana Indonesia dapat diberlakukan dan juga peradilan mana yang berhak untuk memeriksa dan mengadili orang yang melakukan tindak pidana tersebut (kompetensi relatif).[144]

Perbuatan melawan hukum cybercrime sangat tidak mudah diatasi hanya dengan mengandalkan hukum positif konvensional. Hal ini tidak dapat dilepaskan dari lima faktor yang saling berkaitan, antara lain pelaku kejahatan, modus kejahatan, korban kejahatan, reaksi sosial terhadap kejahatan dan hukum. Penentuan locus *delicti* penting untuk menentukan yurisdiksi penegak hukum yang berwenang menangani kasus kejahatan siber.

Locus Delicti, *Locus* (Inggris) yang berarti lokasi atau tempat, secara istilah yaitu berlakunya hukum pidana yang dilihat dari segi lokasi terjadinya perbuatan

[144] O. Yanto, *Pemidanaan atas Kejahatan yang Berhubungan dengan Teknologi Informasi*. Samudra Biru. 2021

pidana[145] atau secara sederhana *locus delicti* adalah tempat terjadinya tindak pidana. *Locus Delicti*, atau yang sering disebut tempat kejadian perkara, adalah lokasi di mana tindak pidana terjadi dan digunakan untuk menentukan yurisdiksi pengadilan yang berwenang untuk memeriksa kasus tersebut.[146]

Dari istilah ini muncul penyebutan dalam hukum dengan *locus regit actum* yang berarti "tempat dari perbuatan menentukan hukum yang berlaku terhadap perbuatan yang dilakukan". *Locus delicti* perlu di dalam penerapan hukum pidana, beberapa hal yang penting diketahui mengenai *locus delicti* adalah:

a. Menentukan apakah hukum pidana Indonesia berlaku terhadap perbuatan pidana tersebut atau tidak (Pasal 2-8 KUHP);
b. Menentukan Kejaksaan dan Pengadilan mana yang harus mengurus perkaranya (kompetensi relatif);
c. Sebagai syarat mutlak sah atau tidaknya surat dakwaan.[147]

Kejahatan siber memanfaatkan jaringan teknologi informasi secara global. Aspek global menimbulkan kondisi seolah-olah dunia tidak ada batasnya (*borderless*). Permasalahan muncul dalam menentukan *locus delicti cyber crime* ini, sehubungan dengan sifat dari internet yang lintas batas. Keadaan ini dapat mengakibatkan pelaku, korban serta tempat dilakukannya tindak pidana (lo*cus delicti*) terjadi di wilayah yang

[145] Adami Chazawi, *Op.Cit* 2002, h 70
[146] Teguh Prasetyo. *Op.Cit*, 2014. h 63
[147] Arthur Simada, dkk. Penentuan Locus Delictie dalam Tindak Pidana Cyber Crime (Merusak dan Mengganggu Sistem Elektronik dan Komunikasi Milik Orang Lain), *Locus Journal of Academic Literature Review*, 3 (4) April 2024, h 351

berbeda-beda.[148] Penentuan *locus delicti* secara umum yang digunakan oleh ilmu hukum pidana saat ini apakah masih relevan bila diterapkan dalam penentuan *locus delicti cyber crime* mengingat sifat *cyber crime* yang lintas batas wilayah dan negara.

Kejahatan siber ini menjadi sebuah tantangan terbaru bagi penyidik guna menjabarkan *locus delicti*, karena pada dasarnya hakim dalam melakukan pemeriksaan mengacu pada surat dakwaan Jaksa yang di dalamnya terkandung *locus* serta *tempus delicti* dari tindak pidana tersebut, sehingga terdakwa dapat didakwakan dengan seadil-adilnya sesuai dengan peraturan perundang-undangan yang berlaku. Lain hal nya jika terdakwa terbukti, akan tetapi tidak didakwakan, maka pengadilan berwenang tidak akan menjerat terdakwa dengan sanksi pidana.[149]

Dalam proses penyidikan, menentukan *locus delicti* pada kejahatan siber, prosesnya pada dasarnya serupa dengan penentuan *locus delicti* pada kejahatan konvensional. Perbedaannya terletak pada media yang digunakan dalam kejahatan siber, yaitu media elektronik seperti laptop, komputer, ponsel, dan berbagai perangkat elektronik canggih lainnya. Oleh karena itu, kejahatan siber digolongkan sebagai kejahatan khusus. Untuk memperluas pemahaman mengenai hal ini, perlu dipahami bahwa kejahatan siber melibatkan penggunaan teknologi canggih yang memungkinkan pelaku melakukan tindakan kriminal dari jarak jauh, sering kali tanpa meninggalkan

[148] Wahid Abdul. *Kejahatan Mayantara (Cyber Crime)*. Malang: Fakultas Hukum Unisma, 2005.

[149] Arthur Simada, dkk. Penentuan Locus Delictie dalam Tindak Pidana Cyber Crime (Merusak dan Mengganggu Sistem Elektronik dan Komunikasi Milik Orang Lain). *Locus Journal of Academic Literature Review*, 3 (4) April 2024, h 353

jejak fisik. Media elektronik yang digunakan dalam kejahatan siber mencakup berbagai perangkat dan platform, seperti jaringan komputer, internet, serta perangkat lunak khusus yang dirancang untuk mengakses, mencuri, atau merusak data.[150]

Secara yuridis, mekanisme penyidikan kejahatan siber diakomodir baik dari segi materil dan formil pada UU ITE yaitu Pasal 42 dan Pasal 43 menyatakan penyidikan terhadap tindak pidana sebagaimana dimaksud dalam undang-undang ini, dilakukan berdasarkan ketentuan dalam hukum acara pidana dan ketentuan dalam undang-undang ini. Hal ini berarti segala ketentuan dalam KUHAP dan undang-undang lainnya yang berkaitan dengan hukum acara pidana, berlaku dalam rangka penyidikan dalam upaya mengungkap tindak pidana yang terjadi dalam dunia siber. Perkara *cybercrime* merupakan perkara khusus yang cara penyidikannya dapat berbeda sebagaimana penyidikan dalam perkara umum. Dalam melaksanakan tugas dan peranannya maka fungsi Kepolisian khususnya satuan siber mendasarkan pada beberapa undang-undang yang terkait dengan tindak pidana *cybercrime* yang terjadi.

Secara fungsi struktural kewenangan penyidikan kejahatan siber oleh Kepolisian, institusi Polri telah melakukan antisipasi sejak dua puluh tahun yang lalu, yang mana pada Tahun 2002 Polri membentuk Subdit IT dan *Cyber Crime* berdasarkan Surat Keputusan Kapolri Nomor 53 dan 54 tahun 2002, yang saat itu bernama Unit Cyber Crime, dipimpin seorang Pamen berpangkat Komisaris Polisi, dan berada

[150] Aldo Satrio Wibowo dan Benny Sumardiana, Tantangan Hukum dalam Penentuan Locus dan Tempus Delicti Pada Tindak Pidana Revenge Porn di Indonesia, *JRH: Reformasi Hukum*, 29 (1) April 2025, h 29

dibawah Direktorat Tindak Pidana Ekonomi dan Khusus Bareskrim Polri. Nomenklatur ini kemudian dirubah berdasarkan Perkap Nomor 21 Tahun 2010 tentang Susunan Organisasi Dan Tata Kerja pada tingkat Markas Besar Kepolisian Negara Republik Indonesia dan Perkap Nomor 22 Tahun 2010 tentang Susunan Organisasi Dan Tata Kerja Pada Tingkat Kepolisian Daerah, menjadi Subdirektorat IT dan Cyber Crime Dit Tipideksus Bareskrim Polri. Untuk di tingkat Kepolisian Daerah, struktur organisasi cyber crime statusnya pada leveling Subdirektorat, artinya kedudukan struktur organisasi cyber crime dibawah kendali Direktorat Kriminal Khusus (Krimsus) sebagai Subdit V. Kepala Subdit V cyber crime membawahi 4 Unit dan Kepala Team IT. Team IT dalam melaksanakan tugas siber dibantu oleh Team Analis, Team Direction Finder, dan Team Digital Forensik.[151]

Fungsional unit khusus dalam tubuh Kepolisian tersebutlah yang berperan menjalankan prosedur penyidikan kejahatan siber yang mana dalam hal ini berimplikasi dengan sistem khusus yang dilakukan guna memenuhi penentuan *locus delicti* sebuah kejahatan siber yang terjadi dalam proses penyidikan.

Secara faktual pelaksanaan penegakan hukum kejahatan siber sangat berhubungan dengan yurisdiksi yang mana hal tersebut berimplikasi pada penentuan *locus delicti* kejahatan tersebut. Salah satu masalah paling krusial yang dimunculkan oleh cybercrime (tindak pidana siber) adalah masalah yurisdiksi yang berkaitan dengan sejauh mana suatu negara dapat menerapkan kedaulatan hukumnya atau dengan kata

[151] Marselinus Goa dan Hudi Yusuf*, Op.Cit,* 3 (3) July 2025, h 759

lain sejauh mana kemampuan suatu negara menyidangkan suatu perkara bernuansa Internasional. Persoalan hukum dalam hal konflik yurisdiki antar negara seringkali muncul dengan adanya *cybercrime* ini , karena salah satu keunikan tindak pidana siber adalah bahwa satu tindak pidana yang dilakukan di suatu negara dapat menimbulkan akibat yang dilarang di negara lain. Ketika delik (perbuatan pidana) siber terjadi, maka permasalahan yang muncul adalah mengenai yurisdiksi penegakan hukumnya terhadap tindak pidana siber tersebut karena setiap negara memiliki kedaulatan penuh terhadap wilayahnya.[152]

Secara representasi sebagai contoh, A Warga Negara Indonesia pada waktu liburan di India, sehari sebelum dia pulang ke Indonesia, A melakukan kejahatan siber berupa *hacking* (menerobos program komputer milik orang/pihak lain) milik B (Warga Negara Cina), C (Warga Negara Malaysia) dan D (Warga Negara Singapore). Adapun data server (data sendiri digunakan untuk menyimpan data baik yang digunakan client secara langsung maupun data yang diproses oleh server aplikasi) di Malaysia. Dalam hal ini terjadi konflik yurisdiksi kriminal antara masing-masing negara, karena terhadap suatu tindak pidana siber tersebut tunduk pada yurisdiksi kriminal masing masing negara atau lebih dari satu Negara. Atas tindak pidana siber hacking yang dilakukan A ini berlakulah yurisdiksi kriminal berdasarkan asas territorial dari Negara India dan Yurisdiki kriminal berdasarkan asas kewarganegaraan aktif dari Negara

[152] Evi Retno Wulan, Teori Server Territorial dalam Penyelesaian Yurisdiksi Kriminal Tindak Pidana Siber, Fak Hukum, Ekonomi dan Pendidikan Univ Narotama Surabaya, *Laporan Akhir Penelitian*, 2022. h 9

Indonesia. Sedangkan tiga orang (B,C,D) yang masing-masing dari Negara Cina, Malayia dan Singapore berlaku yurisdiksi criminal berdasarkan asas kewarganegaraan pasif. [153] Yurisdiksi merupakan refleksi dari kedaulatan suatu Negara, yang dilaksanakan dalam batas-batas wilayahnya. Kata Yuridiksi berasal dari kata *jurisdiction* dalam bahasa Inggris berarti "*authority to carry out justice and to interret and aly laws* ".[154]

Pengertian yurisdiksi yang lebih luas dikemukakan oleh B. James George Jr., yang mendefinisikan yuridiksi sebagai "*the authority of nations or states to create or prescribe penal or regulatory norms and to enforce them through administrative and judicial action*".[155] Pengertian Yurisdiksi menurut James George meliputi kekuasaan Negara untuk menetapkan hukum pidana dan hukum yang bersifat regulative serta menegakkan hukum melalui tindakan administrative dan yudisial. Dengan perkataan lain lingkup yurisdiksi meliputi yurisdiksi untuk menetapkan hukum, yurisdiksi untuk menerapkan hukum dan yurisdiksi untuk menuntut atau mengadili. Salah satu dari peristiwa hukum yang tunduk pada ketiga macam yurisdiksi (yurisdiksi untuk menetapkan hukum, yurisdiksi untuk menerapkan hukum dan yurisdiksi untuk menuntut atau mengadili).

---

[153] *Ibid* h 10

[154] A.P. Cowie (ed), *Oxford Advance Learner's Dictionary*, Oxford University Press, Oxford, 1989, h 679

[155] Sanford H. Kadish, *Encycloedia of Crime and Justice,* The Free Press, New York, 1983, h 922

Memperhatikan mekanisme secara normatif, peneliti mencoba menjabarkan skema penyidikan kejahatan siber yang mana dapat menggambarkan secara terang terkait penentuan *locus delicti* melalui serangkaian skema penyidikan tersebut antara lain:

1. Penyelidikan Awal

   Penyelidikan awal merupakan tahap penting yang dilakukan oleh tim penyelidik *cybercrime* untuk memahami dan merespons kejahatan yang dilaporkan. Proses ini mencakup serangkaian langkah-langkah yang bertujuan untuk mengumpulkan informasi dasar terkait dengan laporan kejahatan siber. Menurut Michael Brown seorang peneliti keamanan, penyelidikan awal dalam kejahatan siber sangat penting untuk memahami cara serangan terjadi dan mengidentifikasi jejak digital pelaku. Penyelidikan awal dapat membantu mengumpulkan bukti yang diperlukan untuk mengidentifikasi pelaku dan mengembangkan strategi keamanan yang lebih baik.[156]

   Langkah pertama dalam penyelidikan awal adalah verifikasi identitas pelapor. Hal ini melibatkan konfirmasi keaslian laporan dan memastikan bahwa informasi yang diberikan oleh pelapor dapat dipercaya. Validasi identitas pelapor menjadi krusial untuk memastikan keabsahan informasi dan keberlanjutan proses penyelidikan. Selanjutnya, tim penyelidik akan mengumpulkan bukti awal yang terkait dengan kejahatan yang dilaporkan. Ini

[156] Michael Brown, et.al. Measuring Attitude Towards Personal Data for Adaptive Cybersecurity, *Information & Computer Security*, 25 (5) November 2017, h 560-579

dapat melibatkan analisis jejak digital, pemeriksaan log aktivitas online, atau pengumpulan informasi teknis lainnya yang dapat mendukung proses penyelidikan lebih lanjut. Bukti awal ini menjadi dasar untuk merinci kronologi kejadian dan mengidentifikasi metode yang mungkin digunakan oleh pelaku kejahatan.[157]

Selama penyelidikan awal, tim juga menganalisis informasi yang mungkin sudah ada, baik yang terkait dengan laporan pelapor maupun yang dapat ditemukan dalam sumber-sumber terbuka. Ini membantu dalam memahami konteks kejadian, melacak asal usul serangan, dan mengidentifikasi potensi ancaman yang dapat muncul. Penyelidikan awal memberikan landasan yang kuat untuk memandu langkah-langkah selanjutnya dalam menangani kejahatan siber. Dengan informasi yang diperoleh selama tahap ini, tim penyelidik dapat mengembangkan strategi penyelidikan yang lebih terinci dan merinci rencana tindakan yang sesuai. Dengan demikian, penyelidikan awal menjadi langkah kritis dalam menjaga keberlanjutan dan keberhasilan respons terhadap kejahatan siber.[158]

Pada skala transnasional mengenai informasi untuk melakukan penyelidikan biasanya didapat dari *National Central Bureau* (NCB) /Interpol yang menerima surat pemberitahuan atau laporan dari negara lain yang kemudian diteruskan ke Unit cyber crime/ satuan Kepolisian yang ditunjuk.

[157] Husamuddin, et.al. *Op.Cit*, 2024, h 81
[158] *Ibid* h 82

Dalam penyelidikan kasus-kasus cyber crime yang modusnya seperti contoh kasus carding metode yang digunakan hampir sama dengan penyelidikan dalam menangani kejahatan narkotika terutama dalam undercover dan control delivery. Petugas setelah menerima informasi atau laporan dari Interpol atau merchant yang dirugikan melakukan koordinasi dengan pihak shipping untuk melakukan pengiriman barang.[159]

2. Koordinasi dan Kolaborasi

Koordinasi dan kolaborasi berperan kunci dalam menangani kejahatan siber, di mana aspek lintas batas dan kompleksitas ancaman membutuhkan keterlibatan berbagai pihak terkait. Kolaborasi efektif melibatkan kerjasama antara berbagai entitas, termasuk penyedia layanan internet, lembaga pemerintah, dan lembaga keamanan siber. Menurut Wall[160], kolaborasi antara lembaga penegak hukum, sektor swasta, dan pihak-pihak terkait lainnya sangat penting dalam mengatasi ancaman cybercrime. Dalam jurnalnya yang berjudul "*Cybercrime and the Culture of Fear*," Wall menekankan perlunya kemitraan lintas sektor untuk menyusun strategi yang efektif dalam melawan kejahatan dunia maya.

[159] Renni Sartika, dkk. Kekhususan Proses Penyidikan Tindak Pidana Cyber Crime, *Jurnal Aktual Justice*, 5 (1) Juni 2020, h 42

[160] David S. Wall, Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime, *Information, Communication & Society*, 11 (6) July 2008, h 861-884

Pentingnya kolaborasi menjadi semakin jelas karena kejahatan siber tidak terbatas oleh batas geografis atau yurisdiksi. Tim penyelidik yang bekerja sama dengan penyedia layanan internet dapat mengakses data yang diperlukan untuk melacak aktivitas online dan mengidentifikasi pelaku kejahatan. Kerjasama dengan lembaga pemerintah memungkinkan akses ke sumber daya dan keahlian tambahan yang mungkin diperlukan dalam menangani kejahatan siber yang kompleks. Kolaborasi juga memfasilitasi pertukaran informasi yang cepat dan efektif antara pihak-pihak yang terlibat. Berbagi informasi ini mencakup data teknis, jejak digital, atau indikator serangan yang dapat digunakan untuk mempercepat proses penyelidikan dan mengidentifikasi potensi ancaman keamanan siber.[161]

Kolaborasi memungkinkan pemanfaatan sumber daya yang lebih besar dan beragam. Melibatkan lembaga keamanan siber, baik dari sektor publik maupun swasta, memberikan akses ke keahlian khusus dalam menghadapi ancaman siber tertentu. Ini memperkuat respons dan memastikan bahwa penyelidikan dapat dilakukan dengan cara yang paling efisien dan efektif. Dengan menggabungkan kekuatan dan sumber daya dari berbagai pihak, koordinasi dan kolaborasi menciptakan landasan yang solid untuk menanggapi kejahatan siber dengan lebih baik. Tim penyelidik yang bekerja bersama dapat menghadapi tantangan yang lebih besar dan lebih kompleks, meningkatkan

[161] Husamuddin, et.al. *Op.Cit*, 2024, h 83

peluang untuk mengidentifikasi, menangkap, dan menuntut pelaku kejahatan siber.

3. Pengumpulan Bukti Digital

Pengumpulan bukti digital menjadi inti dari penanganan kejahatan siber, dan keterlibatan ahli forensik digital menjadi krusial dalam memastikan validitas dan integritas bukti. Proses ini melibatkan serangkaian langkah-langkah yang dirancang untuk mengumpulkan, menganalisis, dan menginterpretasi jejak digital yang dapat menjadi kunci dalam membongkar kejahatan siber.

Menurut Fred Cohen seorang pakar keamanan komputer, mungkin menyoroti pentingnya pengumpulan bukti digital dalam menangani kejahatan siber. Menurut Cohen [162], metode pengumpulan bukti yang cermat dan penggunaan teknik forensik yang tepat dapat berperan kunci dalam membuktikan pelanggaran hukum yang terjadi dalam ruang siber.

Ahli forensik digital berperan utama dalam mengumpulkan bukti, karena memiliki pengetahuan mendalam tentang teknologi dan metode yang digunakan oleh pelaku kejahatan siber. Langkah awal melibatkan pemantauan jejak digital, di mana ahli forensik akan mengidentifikasi dan merekam setiap aktivitas atau interaksi dalam lingkungan digital terkait dengan kejahatan yang diselidiki. Analisis log menjadi langkah berikutnya, di mana ahli forensik

[162] Fred Cohen, *Digital Forensic Evidence Examination*, Pebble Beach, California: ASP Press, 2009

memeriksa catatan elektronik seperti log aktivitas sistem, log jaringan, dan log aplikasi. Analisis ini membantu dalam membangun kronologi kejadian, mengidentifikasi potensi celah keamanan, dan melacak rute yang diambil oleh pelaku kejahatan. Ahli forensik digital berfokus pada identifikasi alat atau teknik yang digunakan oleh pelaku kejahatan. Ini melibatkan pemahaman mendalam tentang metode penyerangan yang mungkin digunakan, seperti contoh serangan *malware* atau teknik peretasan tertentu. Pengetahuan ini membantu dalam menyusun profil pelaku dan mengidentifikasi tindakan spesifik yang dilakukan.[163]

4. Penyidikan Lanjutan

Setelah tahap awal pengumpulan bukti digital, jika tim penyelidik telah mengumpulkan bukti yang cukup untuk memvalidasi dugaan kejahatan siber, proses penyidikan akan memasuki tahap lanjutan. Tahap ini melibatkan upaya untuk mendapatkan pemahaman yang lebih dalam tentang pelaku, motivasi di balik kejahatan, dan kemungkinan jaringan atau koneksi yang terlibat dalam peristiwa tersebut.

Menurut Wall seorang ahli di bidang kejahatan siber, telah menyoroti pentingnya penyidikan lanjutan dalam menghadapi serangan siber yang semakin canggih. Menurutnya, kecepatan perkembangan teknologi

[163] Husamuddin, et.al. *Op.Cit*, 2024, h 84

memerlukan peningkatan kapasitas penyidikan dan pemahaman teknis yang mendalam untuk melacak dan menangani pelaku kejahatan siber.[164]

Pada tahap penyidikan lanjutan, tim penyidik akan memperluas cakupan penyidikan dengan melakukan pengembangan informasi lebih lanjut. Ini mencakup analisis yang lebih mendalam terhadap jejak digital yang telah dikumpulkan, serta pencarian informasi tambahan yang dapat membantu mengisi celah pengetahuan tentang kejadian tersebut. Ahli forensik digital dapat melakukan analisis yang lebih mendalam terhadap file, log, dan struktur sistem yang terlibat. Penyidikan lanjutan juga dapat melibatkan kerjasama dengan berbagai lembaga atau entitas yang terkait, termasuk lembaga keamanan siber, lembaga penegak hukum, atau bahkan lembaga internasional jika kejahatan tersebut melibatkan aspek lintas batas.[165] Kolaborasi semacam ini memperluas sumber daya dan perspektif, memungkinkan tim penyelidik untuk mendapatkan wawasan lebih komprehensif tentang latar belakang dan konteks kejahatan siber.

Penyidikan lanjutan juga dapat melibatkan upaya untuk mengidentifikasi potensi ancaman keamanan yang lebih besar atau pola perilaku yang dapat menjadi indikator potensi serangan yang lebih luas. Pada akhirnya, penyidikan lanjutan bertujuan untuk membentuk dasar yang kuat

[164] David S. Wall, Understanding Transnational Organised Crime, *University of Leeds: Policing*, 6 (4) 2018

[165] Husamuddin, et.al. *Op.Cit*, 2024, h 85

untuk memahami secara menyeluruh kejahatan siber yang terjadi dan memastikan bahwa langkah-langkah penegakan hukum yang tepat dapat diambil untuk menanggapi kejadian tersebut.

Pada kasus-kasus kejahatan siber seperti situs porno maupun perjudian para pelaku melakukan *hosting*/pendaftaran diluar negeri yang memiliki yuridiksi yang berbeda dengan negara kita sebab pornografi secara umum dan perjudian bukanlah suatu kejahatan di Amerika dan Eropa walaupun alamat yang digunakan berbahasa Indonesia dan operator dari pada website ada di Indonesia sehingga kepolisian tidak dapat melakukan tindakan apapun terhadap mereka sebab *website* tersebut bersifat universal dan dapat di akses dimana saja, banyak rumor beredar yang menginformasikan adanya penjebolan bank-bank swasta secara online oleh hacker tetapi korban menutup-nutupi permasalahan tersebut. Hal ini berkaitan dengan kredibilitas bank bersangkutan yang takut apabila kasus ini tersebar akan merusak kepercayaan terhadap bank tersebut oleh masyarakat. Dalam hal ini penyidik tidak dapat bertindak lebih jauh sebab untuk mengetahui arah serangan harus memeriksa server dari bank yang bersangkutan.[166]

Locus delicti ini tidak ada ketentuannya di dalam produk hukum nasional yang berkaitan dengan penanganan kejahatan siber yaitu UU ITE dan KUHAP. Dalam menentukan *locus delicti* dalam tindak pidana *cyber crime* yaitu sama atau relevan

[166] Balian Zahab. Penyidikan Terhadap Tindak Pidana Cyber Crime. *E-jurnal Paparan Masalah Hukum*, 1 (2) Mei 2017. h 45-47

dengan teori penentuan tempat kejadian pada tindak pidana konvensional yaitu berdasarkan pendapat para ahli hukum pidana (doktrin) salah satunya teori yang di kemukakan oleh Van Hamel dan juga berdasarkan putusan-putusan hakim terdahulu (yurisprudensi), dalam tindak pidana *cyber crime* yaitu terdapat beberapa teori yang digunakan oleh penyidik *cyber crime* yakni:

1) *Theory of The Uploader and The Downloader*

Teori ini sama dengan teori perbuatan dan teori akibat hanya saja disesuaikan dengan praktek pada ruang lingkup teknologi informasi, teori ini digunakan dalam penentuan tempat kejadian perkara dalam tindak pidana *cyber crime* dan pada teori ini menekankan bahwa dalam dunia siber terdapat 2 (dua) hal utama yaitu *uploader* (pihak yang memberikan informasi ke dalam *cyber space*) dan *downloader* (pihak yang mengakses informasi)[167], maka dalam hal penentuan tempat terjadinya tindak pidana *cyber crime* dapat melihat berdasarkan tempat pengiriman (tempat pelaku) dan dapat juga berdasarkan tempat penerimaan (tempat korban).

Berdasarkan teori ini suatu negara dapat melarang di dalam wilayahnya, suatu kegiatan *downloading* dan *uploading* materi-materi yang diperkirakan dapat bertentangan dengan kepentingan umum negara tersebut. Sebagai contoh Negara Indonesia melarang setiap orang di dalam wilayahnya untuk melakukan *downloading* segala jenis kegiatan perjudian. Teori ini dapat dikategorikan juga

[167] Sahat Maruli T. Situmeang, *Op.Cit*, 2020, h 36

ke dalam teori yurisdiksi territorial. Karena teori ini terletak pada *locus delicti* pelaku *upload* maupun pelaku *download*.[168]

2) Yurisdiksi Teritorial

Dalam teori ini menjelaskan terdapat lima aspek yaitu:

a. Lokasi terjadinya perbuatan, dalam ajaran ini Penyidik menggunakan ajaran perbuatan materiil (*leer van delicha melijkedaad* atau *tiori corporeal action*), yang dimaksud dengan tempat kejadian adalah tempat dimana pelaku melakukan tindak pidana dan telah selesai akibat dari perbuatan tindak pidana tersebut.[169]

b. Lokasi Komputer, selain itu juga menggunakan ajaran tempat bekerjanya alat (*leer van het instrument*), tempat kejadian adalah tempat dimana alat (dalam hal ini komputer) yang digunakan bekerja dan telah membuat suatu tindak pidana kejahatan. Seperti pada contoh sederhana kejahatan konvensional penyelundupan kuda dari Negeri Belanda ke Negeri Jerman, pada hakikatnya tempat perbuatan sudah dianggap selesai ditempat dimana tali itu dipergunakan. Oleh karena itu *Hoge Raad* (Mahkamah Agung Belanda) menentukan, *locus delicti*-nya ialah di Negeri Belanda.[170]

[168] Arthur Simada, dkk. *Op.Cit,* 3 (4) April 2024, h 355

[169] Bobby R. Tamaka, Pentingnya Tempat Kejadian Perkara Menurut Hukum Pidana di Indonesia, *Lex et Societatis,* II (5) Juni 2014, h 12

[170] *Ibid*

c. Lokasi Orang, dalam ajaran ini terdapat dua prinsip yang menggunakan pendekatan lokasi. Kemungkinan pertama yurisdiksi ditentukan dengan mengarah ke lokasi korban. Kemungkinan kedua, yurisdiksi ditentukan dengan mengarah dimana lokasi perlaku kejahatan berada.[171]

d. Lokasi akibat, kemudian ada juga menggunakan ajaran akibat dari tindakan (*leer van het gevoig*), tempat kejadian adalah tempat dimana suatu akibat telah terjadi sehingga membuat suatu tindak pidana yang dilakukan oleh pelaku.[172]

e. *Location of Anything*, karena ajaran-ajaran tersebut diatas bisa saja tidak sesuai dengan perbuatan yang dilakukan maka ada ajaran lain yang digunakan, adalah ajaran berbagai tempat tindak pidana. Ajaran ini merupakan gabungan dari semua ajaran-ajaran tersebut diatas, sehingga aparat penegak hukum dimungkinkan untuk menentukan dimana saja tempat tindak pidana dilakukan.[173]

3) Yurisdiksi *Ratione Personae* (berdasarkan alasan orang atau person)

Kriteria ini digunakan untuk menentukan yurisdiksi suatu organ yudisial dengan memastikan tentang siapa yang dapat dimintai pertanggungjawaban hukum di muka organ yudisial tersebut. Nasionalitas Pelaku, dalam menentukan yurisdiksi tindak pidana *cybercrime*, pendekatan

[171] Arthur Simada, dkk. *Op. Cit,* 3 (4) April 2024, h 355

[172] M. Yahya Harahap, *Pembahasan Permasalahan dan Penerapan KUHAP*, Jilid II, PT. Sarana Bakti Semesta 1985, h. 624

[173] Arthur Simada, dkk. *Op.Cit,* 3 (4) April 2024, h 355

nasionalitas pelaku juga dapat dilakukan. Nasionalitas Korban, juga dapat dijadikan pendekatan dalam menentukan yurisdiksi kejahatan siber. Dengan pendekatan ini, suatu negara dapat mengklaim kewenangan yurisdiksi terahdap kejahatan-kejahatan yang menyangkutkonten di internet (*content related offence*), dengan argument bahwa ada warganya telah menjadi target kejahatan tersebut.[174]

4) *Theory of Law of The Server*

Teori ini dalam hal penentuan tempat kejadian suatu tindak pidana *cyber crime*, penyidik memperlakukan server di mana halaman *web* atau secara fisik berlokasi yang dilacak berdasarkan IP address tempat mereka dicatat atau disimpan sebagai data elektronik, maka dalam hal ini penyidik dapat menentukan tempat kejadian tindak pidana *cyber crime* berdasarkan dari mana alamat IP yang digunakan pelaku berasal. Secara sederhana berdasarkan teori ini, tempat dimana secara fisik server diletakkan, maka disitulah hukum yang akan diberlakukan. Namun teori ini akan sulit digunakan jika uploader berada di dalam yurisdiksi asing.[175]

5) *Theory of International Space*

Menurut teori ini dalam penentuan tempat terjadinya kejahatan siber yang mana kejahatan siber tersebut sudah diluar teritorial Indonesia yakni

[174] *Ibid*

[175] Yuliana Surya Galih, Yurisdiksi Hukum Pidana dalam Dunia Maya, *Jurnal Ilmiah Galuh Justisi*, 7 (1) Maret 2019, h 69

tindak pidana *cyber crime* transnasional, maka dalam penentuan tempat kejadian perkara harus melihat hukum yang berlaku dilintas negara yang mana *cyber space* dianggap sebagai suatu lingkungan hukum yang terpisah dengan hukum konvensional dimana setiap negara memiliki kedaulatan yang sama, namun pada prakteknya tindak pidana cyber crime transnasional tidak terlalu sulit dalam proses penegakan hukumnya jika suatu negara memiliki kerjasa dalam hal penegakan hukum khususnya dalam hal tindak pidana *cyber crime*.[176]

Teori-teori tersebut digunakan sebagai acuan oleh penyidik pada wilayah hukum Indonesia, mengingat belum adanya pengaturan jelas mengenai *locus delicti*, maka sulit rasanya bagi aparat penegak hukum guna mengetahui peraturan atau pasal yang akan dikenakan terhadap tersangka, mengingat untuk mengetahui locus delicti tersebut penyidik dalam hal ini memerlukan pegangan atau dasar hukum agar tidak terjadi kerancuan pemahaman guna menyelesaikan kejahatan siber secara adil dan berkepastian hukum.

Meskipun belum ada ketentuan yang jelas terkait penentuan *Locus Delicti* dalam kejahatan dunia maya (*cyber crime*) di Indonesia, namun pandangan ahli hukum dapat menjadi acuan dalam menentukan *Locus Delicti* dalam kasus cyb*er crime*. Penentuan *Locus Delicti* dalam Tindak Pidana Kejahatan di Internet (C*yber crime*) menurut Hukum Pidana Nasional di Indonesia menjadi penting karena perkembangan

[176] Muhammad Permana Shidiq, et.al. Characteristics of Cybercrime and Dynamics of the implementation Locus Delicti Theory by Law Enforcement Officials in Indonesia, *Adjudication : Journal Knowledge Law*, 8 (2) December 2024, h 177

teknologi yang pesat telah menyebabkan munculnya kejahatan siber (*cyber crime*), yang merupakan tantangan bagi aparat penegak hukum dalam menentukan *locus delicti* dalam kasus kejahatan siber. Penentuan *locus delicti* penting untuk menentukan yurisdiksi pengadilan yang berwenang menangani kasus kejahatan siber.[177]

Secara teoritis, penentuan *locus delicti* kejahatan siber pada proses penyidikan dengan menggunakan berbagai teori yang dikombinasikan dengan hukum positif sebagai pedoman formil oleh penyidik dalam bekerja memberikan representasi teori bahwa bekerjanya hukum dalam perspektif sosial, hukum bekerja bukan pada ruang yang hampa.[178] Terdapat hubungan resiprositas antara hukum dengan variabelvariabel lain dalam masyarakat. "Di samping hukum berfungsi sebagai alat untuk pengendalian sosial (*as a tool of social control*) hukum juga dapat dimanfaatkan sebagai sarana untuk rekayasa sosial (*as a tool of social engineering*) sebagaimana dideskripsikan oleh Roscou Pound".[179]

C. Problematika Hukum dalam Penentuan Locus Delicti pada Penyidikan Kejahatan Siber

Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa dala kurun waktu sepanjang tahun 2024 terdapat peningkatan signifikan dalam jumlah insiden kejahatan siber yang dilaporkan, dengan berbagai jenis kejahatan. Total

[177] J. F. Kemit & K. L. Kleden. Yurisdiksi Kejahatan Siber: Borderless. *Seminar Nasional-Hukum Dan Pancasila*, 2, Juli 2023, h 55-70

[178] Fithriatus Shalihah, *Op.Cit*, 2015, h 72

[179] Ronny Hanitijo Soemitro, *Op.Cit*, 1989, h 23

trafik anomali di Indonesia selama tahun 2024 adalah 330.527.636 anomali dengan jenis trafik anomali tertinggi yaitu *Mirai Botnet* dengan total sebanyak 81.286.596 aktivitas. *Mirai Botne*t merupakan salah satu jenis *Botnet* yang menargetkan perangkat *Internet of Things* (IoT) dan dibuat untuk melakukan serangan *Distributed Denial of Service* (DDoS) pada situs web atau layanan online, sehingga mengakibatkan adanya gangguan atau *downtime*. Pada tahun 2024 Terdapat 2.487.041 aktivitas *Advanced Persistent Threat* (APT), 514.508 aktivitas *Ransomware* dan 26.771.610 aktivitas *phishing*. BSSN telah mengirimkan 1.367 notifikasi indikasi insiden ke stakeholder dengan jenis notifikasi terbanyak dikirimkan adalah Data Breach. Adapun pengelompokan sektor dilakukan berdasarkan Peraturan Presiden No. 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (IIV). Berdasarkan hasil pemantauan dan analisis *Cyber Threat Intelligence*, BSSN juga melakukan penelusuran dugaan insiden siber dengan jumlah total 241 dugaan insiden kebocoran data. Hasil penelusuran pada *darknet*, ditemukan adanya 56.128.160 temuan data *exposure* yang berdampak pada 461 stakeholder di Indonesia. Pada kasus *web defacement* ditemukan sebanyak 5.780 kasus yang menargetkan beberapa domain dan sebanyak 4.071 *web defacement* terkait judi online yang menargetkan situs pemerintah. Berdasarkan laporan yang diterima dari stakeholder pada layanan aduan siber, diperoleh sebanyak 1.814 aduan pada tahun 2024.[180]

[180] https://csirt.bangkalankab.go.id/posts/lanskap-keamanan-siber-indonesia-tahun-2024, Diakses Pada Tanggal 15 September 2025

Lonjakan kasus kejahatan siber tersebut diatas yang memiliki dampak di wilayah hukum Indonesia akan terus meningkat jika tidak dibarengi dengan penyesuaian langkah kebijakan hukum terhadap fenomena berkembangnya operandi sistem kejahatan siber dengan mengakomodir penegakan hukum dalam hal ini penyidikan yang ideal dan presisi dalam memproses hukum para pelaku kejahatan siber. Kejahatan-kejahatan siber tersebut sering kali melibatkan pelaku yang berada di lokasi berbeda dari korban, sehingga menyulitkan penegak hukum dalam menentukan *locus delicti*. Selain itu, penggunaan alat-alat canggih dan anonimitas di dunia maya menambah kompleksitas dalam menentukan *locus delicti*. Dalam konteks internasional, kejahatan siber sering kali melibatkan pelaku dan korban dari berbagai negara, sehingga memerlukan kerjasama internasional dalam penegakan hukum. Harmonisasi kebijakan antar negara menjadi penting untuk menangani kejahatan siber secara efektif.

Dalam penentuan *locus delicti* pada proses penyidikan kejahatan siber memiliki problematika dalam aspek yurisdiksi, yang mana tindak pidana *cyber crime* ini merupakan tindak pidana yang pelaku dan korban tidak hanya di negara yang sama dan juga tidak selalu berkewarganegaraan yang sama yakni tindak pidana cyb*er crime* ini juga merupakan tindak pidana transnasional, pada sistem hukum pidana yang berlaku saat ini, hukum pidana pada umumnya hanya berlaku di wilayah negaranya sendiri (asas teritorial) dan untuk warga negaranya sendiri (asas personal/nasional aktif), hanya delik-delik tertentu yang dapat digunakan asas nasional pasif dan asas universal yang mana delik-delik tersebut termasuk kejahatan *cyber crime*.

Meskipun penentuan *locus delicti* dalam kejahatan siber sangat penting, hingga saat ini belum ada kesepakatan internasional yang komprehensif menjangkau kewenangan penyidikan kejahatan siber yang melintasi batas negara. Akibatnya, proses penegakan hukum lintas negara menjadi sulit dilakukan.[181] Secara keseluruhan, penentuan *locus delicti* dalam kejahatan siber merupakan isu yang kompleks dan krusial yang memerlukan perhatian serius dari inisiasi pemerintah. Sebab ruang lingkup kejahatan siber yang memiliki jangkauan lintas negara memerlukan kebijakan diplomatik dengan berbagai negara dalam koridor penegakan hukum kejahatan siber.

Untuk menangani kejahatan siber, kerjasama internasional menjadi suatu keharusan yang mendesak. Kejahatan siber sering kali tidak terbatas oleh batas nasional, dan para pelaku dapat beroperasi dari berbagai negara, menggunakan infrastruktur digital yang melibatkan server dan alamat IP di seluruh dunia. Oleh karena itu, dalam penentuan *locus delicti* pada proses penyidikan kejahatan siber harus dapat beradaptasi dengan kerangka kerja kerjasama global untuk mengatasi tantangan lintas batas yang dihadapi.

Menurut Dorothy E. Denning seorang pakar keamanan komputer terkenal, menyoroti pentingnya kerjasama internasional dalam menanggapi kejahatan siber. Ia mengemukakan bahwa karena kejahatan siber tidak mengenal batas negara, kerjasama yang erat antara negara-negara dan lembaga-lembaga internasional menjadi kunci.

[181] Herman B, dkk. Peran Locus dan Tempus Delicti dalam Menentukan Kompetensi Pengadilan pada Kasus Kejahatan Siber, *JULIA: Jurnal Litigasi Amsir*, 11 (3) Agustus 2024, h 394

Pendekatannya menekankan perlunya standar internasional yang seragam untuk memandu penegakan hukum lintas batas.[182]

Hal ini juga ditegaskan oleh David R. Johnson dan David G.Post dalam buku berjudul "And How Should the Internet Be Governed?" mengemukakan 4 model, yaitu:

1) Pelaksanaan kontrol dilakukan oleh badan-badan pengadilan yang saat ini ada (*the existing judicial forums*)
2) Penguasa Nasional melakukan kesepakatan internasional mengenai "*the governance of Cyberspace*".
3) Pembentukan suatu organisasi internasional baru (*A New International Organization*) yang secara khusus menangani masalah-masalah di dunia internet
4) Pemerintah/ pengaturan tersendiri (*self-governance*) oleh para pengguna internet.[183]

Johnson dan Post berpendapat penerapan prinsip-prinsip tradisional dari "*Due Process and personal jurisdiction*" tidak sesuai dan mengacaukan apabila diterapkan pada *cyberspace*. Menurutnya, *cyberspace* harus diperlakukan sebagai suatu ruang yang terpisah dari dunia nyata dengan menerapkan hukum yang berbeda untuk

[182] Dorothy E. Denning, The Rise of Hacktivism, *Georgetown Journal of International Affairs*, 8, September 2015.

[183] David R. Johnson and David G.Post, *And How Should the Internet Be Governed?a Meditation on the Relative Virtues of Decentralized*, *Emergent Law*. Cambridge, MA, United States: MIT Press, 1997

cyberspace (*cyberspace should be treated as a separate "space" from the "real world" by applying distinct law to cyberspace*).[184]

Kerjasama internasional dalam penegakan hukum kejahatan siber mencakup pertukaran informasi, bukti, dan keahlian antara negara-negara yang terlibat. Peningkatan kolaborasi ini memungkinkan otoritas penegak hukum di satu negara untuk mendapatkan dukungan dari negara-negara lain dalam mengidentifikasi, menangkap, dan menuntut pelaku kejahatan siber. Kerjasama ini juga mencakup pembentukan tim investigasi bersama yang terdiri dari ahli keamanan siber, forensik digital, dan penegak hukum dari berbagai negara. Tim-tim ini bekerja bersama-sama untuk menyusun kasus, memahami taktik pelaku kejahatan siber, dan berbagi informasi tentang ancaman siber yang mungkin memengaruhi banyak negara.[185]

UNESCO dalam terbitannya berjudul "*The International Dimensions of Cyberspace Law*" berpendapat bahwa tidak dapat dipungkiri bahwa keberadaan sebuah organisasi internasional akan mempunyai peran yang penting dalam perkembangan *cyberspace*.[186] Alasan yang mendasari gagasan ini adalah bahwa dengan adanya organisasi internasional ini semua negara dapat menyesuaikan atau menyeragamkan peraturan mengenai segala sesuatu yang berkaitan dengan *cyberspace*. Namun UNESCO dalam hal ini mengingatkan bahwa pembentukan organisasi internasional

---

[184] *Ibid*

[185] Kirill Kostiantyn Klevtsov, International Cooperation in the Fight Against Cyberpression in the Context of Response to New Challenges and Threats. *Vestnik of Saint Petersburg University Law*, 1 (3) 2022, h 684

[186] UNESCO, *The International Demension of Cyberspace Law.* England. Ashgate Publishing Ltd., 2000, h 42.

baru juga memiliki permasalahan-permasalahan yang harus dijawab. Beberapa permasalahan yang dimaksud antara lain berkaitan dengan dasar kewenangan, jaminan obyektifitas, jaminan perlindungan terhadap golongan minoritas, dan sebagainya.[187]

Dengan adanya *The United Nations Convention Against Cybercrime*, terdapat beberapa implikasi yang perlu dipertimbangkan untuk memperkuat kerangka hukum domestik yaitu dengan melakukan harmonisasi ruang lingkup penegakan hukum kejahatan siber. Konvensi PBB menetapkan ruang lingkup kejahatan siber yang lebih komprehensif. Hal ini memerlukan penyelarasan dalam UU ITE dan peraturan terkait lainnya untuk memastikan bahwa semua bentuk kejahatan siber yang diatur dalam konvensi juga tercakup dalam hukum domestik.

Konvensi ini menuntut negara anggota untuk menyelaraskan hukum domestik mereka dengan standar internasional yang diatur dalam perjanjian tersebut. Dalam konteks Indonesia, UU ITE telah menjadi dasar hukum utama dalam menangani kejahatan siber, seperti akses ilegal (illegal access), penyadapan ilegal (illegal interception), penyebaran konten pornografi anak, perjudian online dan lain sebagainya. Namun, beberapa aspek dalam konvensi, seperti kerja sama lintas negara dalam pengumpulan bukti elektronik dan ekstradisi pelaku kejahatan siber, memerlukan penyesuaian lebih lanjut pada UU ITE maupun regulasi terkait lainnya. Sebagai contoh, konvensi ini mengatur bahwa negara anggota harus dapat meminta data elektronik dari penyedia layanan internet di negara lain selama penyidikan

[187] *Ibid*

terhadap kejahatan serius yang mana berkaitan pula dalam penentuan locus delicti sebuah kejahatan siber. Hal ini membutuhkan pembaruan mekanisme hukum di Indonesia agar sesuai dengan prosedur internasional yang cepat dan terpercaya.

Salah satu prinsip utama konvensi adalah kerja sama internasional dalam penegakan hukum. Indonesia perlu memperkuat mekanisme kerja sama kerja sama dalam hal ini perihal ekstradisi dengan negara lain, bantuan hukum timbal balik, dan pertukaran informasi intelijen. Namun hal tersebut memerlukan revisi terhadap UU yang sudah ada ataupun pembentukan UU baru yang mengatur kerja sama internasional dalam penanganan kejahatan siber. Konvensi ini juga menekankan pentingnya menjaga keseimbangan antara penegakan hukum dan perlindungan HAM, termasuk hak atas privasi. Indonesia perlu memastikan bahwa UU tindak pidana domestik tidak hanya efektif dalam memerangi kejahatan siber, tetapi juga menghormati hak-hak dasar warga negara. Hal ini dapat dilakukan dengan memperkuat pengawasan terhadap penggunaan data pribadi dan mencegah penyalahgunaan wewenang oleh aparat penegak hukum.[188]

Bagi Indonesia, harmonisasi hukum nasional dengan standar internasional menjadi langkah penting. Konvensi ini mendorong penyesuaian peraturan domestik, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP), sehingga dapat menciptakan kerangka hukum yang relevan dan efektif dalam penentuan *locus delicti* kejahatan siber.

[188] Andi Rania Risya Zamayya, dkk. *Op.Cit,* 9 (2) Juli 2025, h 350

Harmonisasi ini akan memastikan keseragaman standar hukum yang mendukung penegakan hukum yang lebih efisien dan berkepastian hukum.

Selain itu, penguatan kerjasama internasional merupakan aspek krusial dari konvensi ini. Indonesia dapat memperkuat hubungan dengan lembaga penegak hukum di negara lain untuk berbagi informasi, melakukan ekstradisi pelaku, serta mengadakan penyidikan lintas yurisdiksi. Kerjasama semacam ini akan meningkatkan kemampuan Indonesia dalam menangani kejahatan siber yang melibatkan pelaku dan korban dari berbagai negara. Dalam konteks ini, penyesuaian prosedur penyidikan juga menjadi hal yang esensial.[189]

Untuk memberlakukan regulasi khusus dalam mengakomodir penentuan *locus delicti* pada proses penyidikan kejahatan siber, terdapat beberapa asas yang dapat menjadi dasar pemberlakuannya serta menjadi konsepsi bagi kebijakan nasional dalam lingkup penegakan hukum kejahatan siber secara global, meliputi asas khusus dalam hukum pidana Internasional dan asas yurisdiksi pemberlakuan hukum pidana nasional[190] yang diijabarkan antara lain:

1) Asas-Asas Khusus dalam Hukum Pidana Internasional

    a. Asas *au dedere au punere*

        Terhadap pelaku tindak pidana internasional dapat dipidana oleh negara tempat terjadinya tindak pidana (*locus delicti*) dalam batas

[189] *Ibid*, h 351

[190] Dian Sinaga, Kejahatan Terhadap Buku dan Perpustakaan, *Jurnal Visi Pustaka*, 6 (1) 2004, h 23

teritorial negara tersebut atau diserahkan atau diekstradisikan kepada negara peminta yang memiliki yurisdiksi untuk mengadili pelaku tersebut.

b. Asas *au dedere au judicare*

Setiap negara berkewajiban untuk menuntut dan mengadili pelaku tindak pidana internasional dan berkewajiban untuk melakukan kerja sama dengan negara lain di dalam menangkap, menahan, dan menuntut serta mengadili pelaku tindak pidana internasional.[191]

2) Asas Teritorial Diperluas dan Asas Nasional Sebagai Dasar Yurisdiksi Pemberlakuan Hukum Pidana Nasional

Asas Teritorial, berdasarkan asas berlakunya hukum pidana suatu negara pada umumnya yang dianut oleh semua negara dunia adalah asas teritorial. Menurut Moeljatno, asas ini diartikan hukum pidana suatu negara berlaku bagi semua orang yang melakukan perbuatan di negara tersebut, baik oleh warga negaranya maupun warga negara asing. Dalam konteks hukum pidana nasional, hal ini tercantum jelas dalam Pasal 2 KUHP "aturan pidana Indonesia berlaku bagi setiap orang yang melakukan perbuatan pidana di dalam Indonesia".

Lalu pertanggungjawaban negara terhadap warga negaranya yang melakukan tindak pidana di luar negara yang bersangkutan dapat dijangkau

[191] Anis Widyawati, *Hukum Pidana Internasional*, Sinar Grafika, Jakarta, 2014, h 24-25

dengan asas nasional. Regulasi khusus tindak pidana siber ini nantinya memberlakukan asas nasional sebagai upaya untuk menegakkan hukum nasional terhadap warga negara Indonesia yang melakukan tindak pidana siber dari luar negara Indonesia yang dapat mengancam keamanan serta pertahanan Indonesia.[192]

Secara teoritis dalam teori postivisme hukum, menurut Hart ukum harus bersumber dari sesuatu yang abstrak. Ini adalah konsekuensi logis cara berpikir dalam ajaran positivisme, yang bersumber dari hubungan sebab akibat suatu gejala dengan gejala lain secara kongkrit (kasat mata). Oleh karenanya pertimbangan-pertimbangan moral tidak harus terkait dengan terbitnya hukum positif, karena pertimbangan moral bukanlah hal yang konkrit. Begitu kuatnya logika positivisme menjadi pedoman berpikir Hart, tercermin dari ajarannya bahwa "*... the analysis or study of legal consepts in an important study to be distinguished from historical inquiries, sociological inquiries and the critical appraisal of law is terms or moral, socials aims...*".[193]

Cara pandang Hart di atas sama dengan cara pandang John Austin (1790- 1859) yang menyatakan bahwa norma hukum harus memuat; pemerintah, kewajiban dan sanksi. Terkait dengan perintah (*command*) harus memenuhi dua (2) syarat sebagaimana disampaikan John Austin[194], yakni:" *Command are laws if two conditions*

[192] Supanto, Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) dan Antisipasinya dengan Penal Policy, *Jurnal Yustusia*, 1 (5) 2016, h 34

[193] Asep Bambang Hermanto, *Op.Cit*, 2 (4), Desember 2016, h 112

[194] David Dyzenhaus, Sophia Reibentanz Moreau and Arthur Ripstein (ed.), *Op.Cit*, 2007, h. 30-31.

are satisfied: firts, they must be general: second they must be commended by what exists in very political society, whatever its contitutional form, namely, a or a group of person who are in receipt of habitual obedience from most of the society...".

Banyak ahli pikir penganut ajaran positivisme hukum, salah satunya adalah H.L.A Hart, yang mengatakan bahwa hukum itu harus kongkrit, maka harus ada pihak yang menuliskan. Pengertian "yang menuliskannya" itu menunjuk pengertian bahwa hukum harus dikeluarkan oleh suatu pribadi (subjek) yang memang mempunyai otoritas untuk menerbitkan dan menuliskannya. Otoritas tersebut adalah negara. Otoritas negara ditunjukan dengan adanya atribut negara, berupa kedaulatan negara. Berdasarkan kedaulatannya, secara internal negara berwenang untuk mengeluarkan dan memberlakukan apa yang disebut sebagai hukum positif. Selanjutnya H.L.A. Hart, mengatakan : (1) hukum (yang sudah dikonkritisasi dalam bentuk hukum positif) harus mengandung perintah; (2) tidak selalu harus ada kaitanya antara hukum dengan moral dan dibedakan dengan hukum yang seharusnya diciptakan (*there is no necessary connection between law and morals or law as it ougt so be*).[195]

[195] Teguh Prasetyo dan Abdul Hakim Barkatullah, *Op.Cit*, 2007, h 97-99.

BAB IV

PENUTUP

A. Kesimpulan

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diperbarui melalui Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024, menjadi produk politik hukum nasional dalam mengakomodir norma hukum pidana terhadap beberapa jenis kejahatan siber yang terjadi di Indonesia. Dalam UU ITE menerapkan norma hukum pidana dalam berbagai jenis kejahatan siber yang ditentukan dalam Pasal 27 hingga Pasal 35 yang terdiri dari perbuatan (1) kesusilaan; (2) perjudian online; (3) penghinaan atau pencemaran nama baik; (4) pemerasan; (5) penyebaran berita palsu atau bohong (*hoax*) yang menagkibatkan kerugian konsumen; (6) Penyebaran berita palsu atau bohong (*hoax*) menimbulkan kerusuhan masyarakat; (7) Ujaran kebencian SARA; (8) Penguntitan (*cyberstalking*); (9) *Cracking, Hacking, Illegal Access*; (10) Penyadapan (Intersepsi); (11) Perusakan data atau Informasi elektronik (*Data interference*); (12) Mengganggu sistem elektronik (*System interference*); (13) Penyalahgunaan perangkat atau *misuse of devices*; (14) Penipuan situs/ *Phising*

(*Data Forgery*). Dalam lingkup *cyber terrorism*, Undang-Undang Pemberantasan Tindak Pidana Terorisme mengatur mengenai alat bukti elektronik sesuai dengan Pasal 27 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu. *Digital evidence* atau alat bukti elektronik sangatlah berperan dalam penyelidikan kasus terorisme. Karena saat ini komunikasi antara para pelaku di lapangan dengan pimpinan atau aktor intelektualnya dilakukan dengan memanfaatkan fasilitas di Internet untuk menerima perintah atau menyampaikan kondisi di lapangan karena para pelaku mengetahui. pelacakan terhadap Internet lebih sulit dibandingkan pelacakan melalui *handphone*. Fasilitas yang sering digunakan adalah *e-mail* dan *chat room* selain mencari informasi dengan menggunakan *search engine* serta melakukan propaganda melalui *bulletin board* atau *mailing list*.

2. *Locus delicti* ini tidak ada ketentuannya di dalam produk hukum nasional yang berkaitan dengan penanganan kejahatan siber yaitu UU ITE dan KUHAP. Dalam menentukan *locus delicti* dalam tindak pidana *cyber crime* yaitu sama atau relevan dengan teori penentuan tempat kejadian pada tindak pidana konvensional yaitu berdasarkan pendapat para ahli hukum pidana (doktrin). Dalam tindak pidana *cyber crime* yaitu terdapat beberapa teori yang digunakan oleh penyidik *cyber crime* yakni Pertama, *theory of the uploader and the downloader* digunakan dalam penentuan tempat kejadian perkara dalam tindak pidana *cyber crime* dan pada teori ini menekankan bahwa dalam dunia siber

terdapat 2 (dua) hal utama yaitu *uploader* (pihak yang memberikan informasi ke dalam *cyber space*) dan *downloader* (pihak yang mengakses informasi). Kedua, teori yurisdiksi teritorial yang mana dalam teori ini menjelaskan terdapat lima aspek yaitu lokasi terjadinya perbuatan (*leer van delicha melijkedaad*), lokasi komputer (*leer van het instrument*), lokasi orang, lokasi akibat (*leer van het gevoig*) dan *location of anything*. Ketiga, yurisdiksi *ratione personae* yaitu menentukan yurisdiksi suatu organ yudisial dengan memastikan tentang siapa yang dapat dimintai pertanggungjawaban hukum di muka organ yudisial tersebut. Keempat, *theory of law of the server* yaitu tempat dimana secara fisik server diletakkan, maka disitulah hukum yang akan diberlakukan. Kelima, *theory of International Space* yaitu penentuan tempat terjadinya kejahatan siber yang mana kejahatan siber tersebut sudah diluar teritorial Indonesia yakni tindak pidana *cyber crime transnasional*, maka dalam penentuan tempat kejadian perkara harus melihat hukum yang berlaku dilintas negara yang mana *cyber space* dianggap sebagai suatu lingkungan hukum yang terpisah dengan hukum konvensional dimana setiap negara memiliki kedaulatan yang sama, namun pada prakteknya tindak pidana *cyber crime* transnasional tidak terlalu sulit dalam proses penegakan hukumnya jika suatu negara memiliki kerjasa dalam hal penegakan hukum khususnya dalam hal tindak pidana *cyber crime*.

3. Dalam penentuan *locus delicti* pada proses penyidikan kejahatan siber memiliki problematika dalam aspek yurisdiksi, yang mana tindak pidana *cyber crime* ini

merupakan tindak pidana yang pelaku dan korban tidak hanya di negara yang sama dan juga tidak selalu berkewarganegaraan yang sama yakni tindak pidana cyb*er crime* ini juga merupakan tindak pidana transnasional, pada sistem hukum pidana yang berlaku saat ini, hukum pidana pada umumnya hanya berlaku di wilayah negaranya sendiri (asas teritorial) dan untuk warga negaranya sendiri (asas personal/nasional aktif), hanya delik-delik tertentu yang dapat digunakan asas nasional pasif dan asas universal yang mana delik-delik tersebut termasuk kejahatan *cyber crime*. Bagi Indonesia, harmonisasi hukum nasional dengan standar internasional menjadi langkah penting. Konvensi Internasional mendorong penyesuaian peraturan domestik, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP), sehingga dapat menciptakan kerangka hukum yang relevan dan efektif dalam penentuan l*ocus delicti* kejahatan siber. Harmonisasi ini akan memastikan keseragaman standar hukum yang mendukung penegakan hukum yang lebih efisien dan berkepastian hukum.

B. Saran

Perlunya peningkatan upaya diplomatik pemerintah Indonesia dalam memperkuat kerjasama lintas negara dalam ruang lingkup penegakan hukum kejahatan siber lintas negara. Pelaku kejahatan siber sering menggunakan infrastruktur yang tersebar di berbagai negara untuk melancarkan serangan. Oleh karena itu, kolaborasi internasional menjadi kunci untuk mengejar dan menuntut pelaku kejahatan siber, serta

berbagi intelijen yang dapat mencegah serangan yang lebih luas. Koordinasi yang baik antara pihak-pihak terkait, baik di tingkat nasional maupun internasional, diperlukan untuk memastikan respons yang efektif terhadap ancaman siber. Proses penyidikan dan pertukaran informasi harus berlangsung secara efisien, memungkinkan penangkapan pelaku dan pengembangan strategi keamanan siber yang lebih baik.

DAFTAR PUSTAKA

A. Buku

Adami Chazawi, *Pelajaran Hukum Pidana*, Raja Grafindo Persada, Jakarta 2002

_____, *Hukum Pidana Positif Penghinaan*, Edisi Revisi, Malang: Media Nusa Creative, 2013

Agus Raharjo, *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: Citra Aditya Bakti, 2002

Aim Abdulkarim, *Pendidikan Kewarganegaraan: Membangun Warga Negara yang Demokratis,* Grafindo Media Pratama, Bandung, 2008

Anis Widyawati, *Hukum Pidana Internasional*, Sinar Grafika, Jakarta, 2014

A.P. Cowie (ed), *Oxford Advance Learner's Dictionary*, Oxford University Press, Oxford, 1989

Arief Amrullah, *Politik Hukum Pidana (Dalam Perlindungan Korban Kejahatan Ekonomi Di Bidang Perbankan)*, Bayumedia, Malang, 2007

Bambang Poernomo. *Asas-Asas Hukum Pidana*. Yogyakarta. Seksi Kepidanaan Fakultas Hukum Universitas Gajah Mada, 1996

Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, PT. Citra Aditya Bakti, Bandung, 2010

Boediono. *Teori Hukum*. Yrama Widya. Bandung. 2016

C.S.T. Kansil, *Pengantar Ilmu Hukum*, Balai Pustaka, Jakarta, 2002

David Dyzenhaus, Sophia Reibentanz Moreau and Arthur Ripstein (ed.), *Law and Morality; Readings in Legal Philosophy*. 3rd edition, Toronto, University of Toronto Press, 2007

David R. Johnson and David G.Post, *And How Should the Internet Be Governed?a Meditation on the Relative Virtues of Decentralized*, *Emergent Law*. Cambridge, MA, United States: MIT Press, 1997

Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, ctk. Kedua, PT Refika Aditama, Bandung, 2009

Edi Ribut Harwanto, *Politik Hukum Pidana*, Sai Wawai Publishing, 2019

Febri dan Yetisma Saini. *Hukum Acara Pidana Indonesia*. Sumbar. Penerbit LPPM Universitas Bung Hatta. 2022

Fithriatus Shalihah, *Buku Ajar Sosiologi Hukum*, Fakultas Hukum Universitas Islam Riau, Pekanbaru, 2015

Fred Cohen, *Digital Forensic Evidence Examination*, Pebble Beach, California: ASP Press, 2009

Georgia Institute of Technology, *Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers*, Chicago, Illinois; Caxton Business & Legal, Inc. 2015

Husamuddin, et.al. *Hukum Acara Pidana dan Pidana Cyber*, Medan: PT Media Penerbit Indonesia, 2024

Imam Syaukani dan A. Ahsin Thohari. *Dasar-Dasar Politik Hukum*. Jakarta: RajaGrafindo Persada, 2010

Joko Sriwidodo. *Pengantar Hukum Acara Pidana*. Cet.1. Yogyakarta. Penerbit Kepel Press. 2023

L.J. Van Apeldoorn, *Pengantar Ilmu Hukum*, Djakarta : Noor Komala, 1962

Moeljatno, *Asas-Asas Hukum Pidana*, Bina Aksara, Jakarta, 1987

Mudzakir dkk, *Perencanaan Pembangunan Hukum Nasional Bidang Politik Hukum Pidana dan Sistem Pemidanaan*, Jakarta, Badan Pembinaan Hukum Nasional, 2012

Muladi dan Barda Nawawi Arief, *Pidana dan Pemidanaan*, Semarang, Banda Penyediaan Bahan Kuliah, 1984

Muladi, *Demokratisai*, *Hak Asasi Manusia, dan Reformasi Hukum di Indonesia*, The Habibie Centre, Jakarta, 2002

M. Yahya Harahap, *Pembahasan Permasalahan dan Penerapan KUHAP*, Jilid II, PT. Sarana Bakti Semesta 1985

O. Yanto, *Pemidanaan atas Kejahatan yang Berhubungan dengan Teknologi Informasi*. Samudra Biru. 2021

P.A.F Lamintang, *Dasar-Dasar Hukum Pidana*, Sinar Baru, Bandung, 2013

R. Hakim, *Hukum Pidana Islam (Fiqih Jinayah)*, CV. Pustaka Setia, Bandung. 2000

Riyeke Ustadiyanto, *Framework e-Commerce*, Yogyakarta: Andi, 2001

Robert R.Mayer dan Ernest Greenwood dalam Sultan Zan Arbi dan Wayan Ardana, *Rancangan Penelitian Dan Kebijakan Sosial,* Jakarta, CV. Rajawali, 1997

Ronny Hanitijo Soemitro, *Perpektif Sosial dalam Pemahaman Masalah-Masalah Hukum*, CV Agung, Semarang, 1989

_____, *Metodologi Penelitian Hukum dan Jurimetri*, Ghalia Indonesia, Jakarta, 1990

R. Soesilo, *Taktik dan Teknik Penyidikan Perkara Kriminal,* Bandung: Karya Nusantara, 1980

Sahat Maruli, *Cyber Law,* Cet.1, Cakra, Bandung, 2020

Sanford H. Kadish, *Encycloedia of Crime and Justice,* The Free Press, New York, 1983

Satjipto Rahardjo, *Ilmu Hukum,* Alumni, Bandung, 1992

Soerjono Soekanto, *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum*, PT. Raja Grafindo, Jakarta 1993

Sudarto, *Kapita Selekta Hukum Pidana*, Bandung: Alumni, 1986

Surayin, *Analisis Kamus Umum Bahasa Indonesia*, Bandung, Yrama Widya, 2005

Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya*, Cet. I; Yogyakarta: Laksbang Pressindo, 2007

Teguh Prasetyo dan Abdul Hakim Barkatullah, *Ilmu Hukum dan Filsafat Hukum*, Yogyakarta, Pustaka Pelajar, 2007

Teguh Prasetyo. *Hukum Pidana Edisi Revisi*. Jakarta. Raja Grafindo Persada, 2014

UNESCO, *The International Demension of Cyberspace Law.* England. Ashgate Publishing Ltd., 2000

Wahid Abdul. *Kejahatan Mayantara (Cyber Crime).* Malang: Fakultas Hukum Unisma, 2005

B. Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

Kitab Undang-Undang Acara Hukum Pidana

Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Republik Indonesia

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

C. Jurnal dan Dokumen Ilmiah

A. Aco Agus dan Riskawati, Penanganan Kasus Cybercrime di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar), *Jurnal Supremasi*, 10 (1) 2016

Adji Samekto, Perkembangan Ranah Kajian Ilmu Hukum, Semarang: UNDIP, *Orasi Ilmiah*, 9 Januari 2005

Agung Yoga, Cyber Crime dan Upaya Penanggulangannya, *JAHE - Jurnal Akuntansi Hukum dan Edukasi*, 1 (1) Mei 2024

Aldo Satrio Wibowo dan Benny Sumardiana, Tantangan Hukum dalam Penentuan Locus dan Tempus Delicti Pada Tindak Pidana Revenge Porn di Indonesia, *JRH: Reformasi Hukum*, 29 (1) April 2025

Aliefka Albiandro, Analisis Hukum dalam Menentukan Locus Delicti dalam Perkara Tindak Pidana Pemalsuan Akta Otentik, *JOM Fakultas Hukum Universitas Riau*, IX (1) Januari-Juni 2022

Andi Rania Risya Zamayya, dkk. Kajian Teoritis Implikasi The United Nations Convention Against Cybercrime Terhadap Pengaturan Tindak Pidana Siber Indonesia, *Ikraith-Humaniora*, 9 (2) Juli 2025

Anirut Chuasanga and Ong Argo Victoria, Legal Principles Under Criminal Law in Indonesia Dan Thailand, *Jurnal Daulat Hukum*, 2 (1), March 2019

Aris Saefulloh, Kebangkitan Agama Di Tengah Peradaban Global, *Jurnal Al-Ulum*, 11 (1) 2011

Arthur Simada, dkk. Penentuan Locus Delictie dalam Tindak Pidana Cyber Crime (Merusak dan Mengganggu Sistem Elektronik dan Komunikasi Milik Orang Lain). *Locus Journal of Academic Literature Review*, 3 (4) April 2024

Asep Bambang Hermanto, Ajaran Positivisme Hukum Di Indonesia: Kritik Dan Alternatif Solusinya, *Selisik*, 2 (4), Desember 2016

Bagir Manan, Varia Peradilan, *Majalah Hukum*, Tahun ke XXI No.243, Februari 2006

Balian Zahab. Penyidikan Terhadap Tindak Pidana Cyber Crime. *E-jurnal Paparan Masalah Hukum*, 1 (2) Mei 2017

Bobby R. Tamaka, Pentingnya Tempat Kejadian Perkara Menurut Hukum Pidana di Indonesia, *Lex et Societatis,* II (5) Juni 2014

Bonaventura Deogratia Manorek, dkk. Penegakan Hukum Pidana dalam Memberantas Kejahatan Pencurian Data Elektronik (Phising), *Lex Privatum,* 15 (2) Februari 2025

Brisilia Tumalun, Upaya Penanggulangan Kejahatan Komputer dalam Sistem Elektronik Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008, *Jurnal Lex Et Societatis*, 6 (2) 2018

Chad Yarbrough, Federal Bureau of Investigation Internet Crime Report 2024, *Internet Crime Complaint Center (IC3) Annual Report*, 2024

Daniel F. T. Popal, Upaya Penanggulangan Tindak Pidana Mayantara (Cybercrime), *Lex Administratum*, XII (5) September 2023

Dani Septian Nugroho dan Margo Hadi Pura, Faktor Hambatan Penyidikan dalam Kasus Tindak Pidana Cybercrime, *Veritas: Jurnal Program Pascasarjana Ilmu Hukum*, 8 (1) 2022

David S. Wall, Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime, *Information, Communication & Society*, 11 (6) July 2008

_____, Understanding Transnational Organised Crime, *University of Leeds: Policing*, 6 (4) 2018

Dian Sinaga, Kejahatan Terhadap Buku dan Perpustakaan, *Jurnal Visi Pustaka*, 6 (1) 2004

Dewi Bunga, Politik Hukum Pidana Terhadap Penanggulangan Cybercrime, *Jurnal Legislasi Indonesia,* 16 (1) Maret 2019

Dodo Zaenal Abidin, Kejahatan dalam Teknologi Informasi dan Komunikasi, *Jurnal Ilmiah Media Processor*, 10 (2) Oktober 2015

Dorothy E. Denning, The Rise of Hacktivism, *Georgetown Journal of International Affairs*, 8, September 2015

Endri Susanto, dkk. Politik Hukum dalam Penegakan Undang-Undang Informasi dan Transaksi Elektronik, *Jurnal Kompilasi Hukum*, 6 (2) Desember 2021

Fiorida Mathilda, Cyber Crime dalam Sistem Hukum Indonesia, *SigmaMu,* 4 (2) September 2012

Handrini Ardiyanti, Cyber-Security dan Tantangan Pengembangannya di Indonesia, *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, 5 (1) Juni 2014

Herman B, dkk. Peran Locus dan Tempus Delicti dalam Menentukan Kompetensi Pengadilan pada Kasus Kejahatan Siber, *JULIA: Jurnal Litigasi Amsir*, 11 (3) Agustus 2024

Hibnu Nugroho, Merekonstruksi Sistem Penyidikan dalam Peradilan Pidana (Studi tentang Kewenangan Penyidik Menuju Pluralisme Sistem Penyidikan di Indonesia), *Jurnal Hukum Pro Justitia*, 26 (1) Januari 2008

https://csirt.bangkalankab.go.id/posts/*lanskap-keamanan-siber-indonesia-tahun-2024*

Imawanto, et.al. Pengaruh Politik dalam Pembentukan Hukum di Indonesia. *Meida Keadilan Jurnal Ilmu Hukum*. 12 (1) 2021

Intan Trivena Maria Daeng, Penggunaan Smartphone dalam Menunjang Aktivitas Perkuliahan oleh Mahasiswa Fispol Unsrat Manado, *E-Journal Acta Diurna*, 6 (1), 2017

J. F. Kemit & K. L. Kleden. Yurisdiksi Kejahatan Siber: Borderless. *Seminar Nasional-Hukum Dan Pancasila*, 2, Juli 2023

Kementerian Hukum dan HAM RI, Analisis dan Evaluasi Hukum Acara Pidana: Penyelidikan dan Penyidikan (Undang-Undang No 8 Tahun 1981 tentang Hukum Acara Pidana), Pusat Analisis dan Evaluasi Hukum Nasional, BPHN Kemenkumham, *Laporan Akhir*, 2022

Kirill Kostiantyn Klevtsov, International Cooperation in the Fight Against Cyberpression in the Context of Response to New Challenges and Threats. *Vestnik of Saint Petersburg University Law*, 1 (3) 2022

K. Permata, dkk. Analisis Yuridis dalam Fenomena Revenge Porn di Indonesia dan Upaya Perlindungan Hukum terhadap Korban. *Jurnal Pendidikan Tambusai*, 8 (1) 2024

Kristiani Virgi Kusuma Putri, Kerja Sama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime, *Rewang Rencang : Jurnal Hukum Lex Generalis*, 2 (7), 2021

Lalu Heru Sujamawardi, Analisis Yuridis Pasal 27 Ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, *Dialogia Juridica: Jurnal Hukum Bisnis dan Investasi*, 9 (2) 2018

Lastary Okvania, dkk. Analisis Putusan Pengadilan Negeri Payakumbuh Nomor 4/Pid.Sus/2022/PN Pyh dengan Putusan Mahkamah Agung Republik Indonesia Tentang Tindakan Pidana Konten Asusila lewat Media WhatsApp, *Unes Law Review*, 5 (4) Juni 2023

Lita Sari Marita, Cyber Crime dan Penerapan Cyber Law dalam Pemberantasan Cyber Law di Indonesia, *Cakrawala: Jurnal Humaniora Universitas Bina Sarana Informatika*, 15 (2) 2015

Marselinus Goa dan Hudi Yusuf, Analisis Penipuan Online Melalui Media Sosial Dalam Kasus Kejahatan Belanja Online di Wilayah Jawa Timur, *Media Hukum Indonesia (MHI),* 3 (3) July 2025

M. E. Fuady, Fenomena Kejahatan Melalui Internet di Indonesia, *Mediator*, 6 (2), Desember 2005

Michael Brown, et.al. Measuring Attitude Towards Personal Data for Adaptive Cybersecurity, *Information & Computer Security*, 25 (5) November 2017

Miftakhur Rokhman Habibi dan Isnatul Liviani, Kejahatan Teknologi Informasi (Cybercrime) dan Penanggulangannya dalam Sistem Hukum Indonesia, *Al-Qānūn: Jurnal Pemikiran dan Pembaharuan Hukum Islam*, 23 (2) Desember 2020

Muhammad Adrian Fitra Yamazaki. Analisis Prosedural Penegakan Hukum Pidana dalam Situasi Pandemi Covid-19 Penyesuaian Terhadap Ancaman Kejahatan Yang Timbul Akibat Pandemi Covid-19. *Jurnal Hukum dan Kewarganegaraan*, 6 (7) 2024

Muhammad Dhika Silva Pradana. Proses Penyidikan Terhadap Pelaku Tindak Pidana Kecelakaan Lalu Lintas Yang Mengakibatkan Korban Meninggal Dunia Di Kepolisian Resor Kota Pati, *Doctoral Dissertation*, Universitas Islam Sultan Agung Semarang. 2023

Muhammad Permana Shidiq, et.al. Characteristics of Cybercrime and Dynamics of the implementation Locus Delicti Theory by Law Enforcement Officials in Indonesia, *Adjudication : Journal Knowledge Law*, 8 (2) December 2024

Renni Sartika, dkk. Kekhususan Proses Penyidikan Tindak Pidana Cyber Crime, *Jurnal Aktual Justice*, 5 (1) Juni 2020

Roderic Broadhurst, Peter Grabosky, Mamoun Alazab dan Steve Chon, Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime, *International Journal of Cyber Criminology*, 8 (1) January-June 2014

Sarah Barber, Westminster Hall Debate on the Computer Misuse Act 1990. *House of Commons Library*, 2022

Sherly Nelsa Fitri, Politik Hukum Pembentukan Cyber Law Undang-Undang Informasi dan Transaksi Elektronik di Indonesia, *Jurnal Justisia: Jurnal Ilmu Hukum, Perundang-undangan dan Pranata Sosial,* 7 (1) 2022

Siti Hailatul Umami dan Abshoril Fithry, Mekanisme Penyidikan dan Penuntutan Tindak Pidana Cybercrime: Tinjauan Hukum Indonesia, *Prosiding Seminar Nasional Penelitian dan Pengabdian Masyarakat 2 Tahun 2023*, Sumenep 5-6 Desember 2023

Suharyadi, dkk. Kejahatan Dunia Maya (Cyber Crime) Dalam Prespektif Hukum Islam, *Journal of Lex Generalis (JLS)*, 1 (5) Oktober 2020

Sulistiyawan Doni Ardiyanto, Eko Soponyono, and Achmad Sulchan, Judgment Considerations Policy in Decree of the Court Criminal Statement Based On Criminal Destination, *Jurnal Daulat Hukum*: 3 (1), March 2020

Supanto, Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) dan Antisipasinya dengan Penal Policy, *Jurnal Yustusia*, 1 (5) 2016

Uni Sabadina, Politik Hukum Pidana Penanggulangan Kejahatan Teknologi Informasi Terkait Kebocoran Data Pribadi Oleh Korporasi Berbasis Online, *LEX Renaissan*, 4 (6) Oktober 2021

Wawan Sanjaya, Sinkronasi Penyelidikan dan Penyidikan oleh POLRI, Kejaksaan dan KPK Terhadap Pelaku Tindak Pidana Korupsi, *Jurnal de Jure*, 1 (15) Januari 2018

Yuliana Surya Galih, Yurisdiksi Hukum Pidana dalam Dunia Maya, *Jurnal Ilmiah Galuh Justisi*, 7 (1) Maret 2019

Yuni Fitriani dan Roida Pakpahan, Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace, *Cakrawala: Jurnal Humaniora*, 20 (1) Maret 2020