FUNGSIONAL DIGITAL FORENSIK DALAM TAHAP PENYIDIKAN TINDAK PIDANA CYBERCRIME

TESIS

Oleh:

MUHAMMAD IBNU SINA

NIM : 20302400499

Konsentrasi : Hukum Pidana

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

FUNGSIONAL DIGITAL FORENSIK DALAM TAHAP PENYIDIKAN TINDAK PIDANA CYBERCRIME

TESIS

Diajukan untuk penyusunan Tesis
Program Studi Ilmu Hukum

Oleh:

MUHAMMAD IBNU SINA
NIM : 20302400499
Konsentrasi : Hukum Pidana

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

FUNGSIONAL DIGITAL FORENSIK DALAM TAHAP PENYIDIKAN TINDAK PIDANA CYBERCRIME

Diajukan Untuk Penyusunan Tesis

Program Magister Hukum

Oleh:

Nama : MUHAMMAD IBNU SINA

NIM : 20302400499

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

FUNGSIONAL DIGITAL FORENSIK DALAM TAHAP PENYIDIKAN TINDAK PIDANA CYBERCRIME

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

Tim Penguji
Ketua,
Tanggal,

Prof. Dr. Bambang Tri Bawono, S.H., M.H.
NIDN. 06-0707-7601

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:

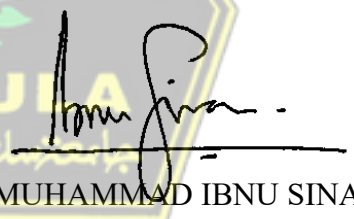
Nama : MUHAMMAD IBNU SINA
NIM : 20302400499

Dengan ini saya nyatakan bahwa Karya Tulis Ilmiah yang berjudul:

FUNGSIONAL DIGITAL FORENSIK DALAM TAHAP PENYIDIKAN TINDAK PIDANA CYBERCRIME

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.



(MUHAMMAD IBNU SINA)

PERNYATAAN PERSETUJUAN UNGGAH KARYA ILMIAH

Saya yang bertanda tangan di bawah ini:

Nama	:	MUHAMMAD IBNU SINA
NIM	:	20302400499
Program Studi	:	Magister Ilmu Hukum
Fakultas	:	Hukum

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

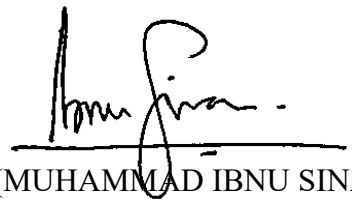
FUNGSIONAL DIGITAL FORENSIK DALAM TAHAP PENYIDIKAN TINDAK PIDANA CYBERCRIME

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.



(MUHAMMAD IBNU SINA)

*Coret yang tidak perlu

KATA PENGANTAR

Segala Puji tercurahkan kepada Allah Subhanahu Wataala yang telah melimpahkan Rahmat dan Taufik serta Hidayahnya kepada Peneliti, sehingga peneliti dapat menyelesaikan Tesis yang berjudul: FUNGSIONAL DIGITAL FORENSIK DALAM TAHAP PENYIDIKAN TINDAK PIDANA CYBERCRIME dapat diselesaikan peneliti secara tepat waktu.

Pengambilan judul tersebut, berdasarkan pada fungsional bukti digital dalam beberapa kasus *cybercrime* memang sangat kompleks. Penggunaan bukti digital juga masih sering memunculkan perdebatan. Uji forensik digital yang harus ada sebagai pendukung bukti digital tersebut juga masih kurang mendapatkan kepastian hukum. Pembuktian menggunakan bukti elektronik dalam perkara pidana khusus yang dalam undang-undang secara khusus mengatur bukti elektronik sebagai salah satu alat bukti yang sah memang lebih menjamin kepastian hukum dari penggunaan bukti elektronik. Namun, terkait dengan hasil uji forensik digital yang dihadirkan ke dalam persidangan sebagai alat bukti masih menjadi pertanyaan besar. Perdebatan lain yang sering kali muncul terkait dengan proses pengujian bukti elektronik, proses pemeliharaan bukti elektronik dan juga sering diperdebatkan kemampuan seorang ahli forensik digital dalam melakukan pengujian bukti elektronik karena serangkaian proses ini belum ada pengaturan secara lebih rinci.

Maksud dan tujuan dari penelitian 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 menganalisis (1) bentuk politik hukum dalam mengkualifikasikan cybercrime dalam norma hukum pidana, (2) prosedur hukum upaya digital forensik dalam tahap penyidikan tindak pidana cybercrime, (3) problematika hukum yang terjadi dalam fungsional digital forensik pada proses penyidikan tindak pidana cybercrime.

Peneliti 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, Agustus 2025
Peneliti

M. Ibnu Sina

ABSTRAK

Lembaga penegak hukum di berbagai negara mulai memprioritaskan pengembangan unit khusus digital forensik sebagai bentuk respons terhadap ancaman dunia maya yang kian masif. Di Indonesia, peningkatan kapasitas laboratorium forensik digital melalui Lembaga Kepolisian juga tengah dilakukan, seiring dengan maraknya kasus pencurian data, serangan ransomware, perjudian online, industri pornografi anak dan kejahatan siber lainnya. Dengan demikian, digital forensik tidak lagi dianggap sebagai opsi tambahan, melainkan menjadi kebutuhan esensial dalam sistem peradilan pidana era digital.

Tujuan Penelitian ini adalah untuk mengetahui dan menganalisis (1) bentuk politik hukum dalam mengkualifikasikan cybercrime dalam norma hukum pidana, (2) prosedur hukum upaya digital forensik dalam tahap penyidikan tindak pidana cybercrime, (3) problematika hukum yang terjadi dalam fungsional digital forensik pada proses penyidikan tindak pidana cybercrime.

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.

Hasil penelitian dan Pembahasan dapat disimpulkan: (1) UU ITE memperjelas cakupan tindak pidana siber dengan menyebutkan jenis-jenis kejahatan yang secara spesifik berkaitan dengan aktivitas di ruang digital. Pasal 27 hingga Pasal 37 UU ITE secara spesifik mengatur tentang kejahatan terkait konten ilegal akses tidak sah, penyadapan, dan serangan terhadap integritas sistem lainnya. (2) Menurut Pasal 187 b KUHAP, hasil pemeriksaan forensik digital berupa BAP laboratorium forensik dan BAP ahli forensik harus dibuat sesuai dengan ketentuan peraturan perundang-undangan atau undang-undang. Hal ini menunjukan bahwa hasil uji forensik digital menghasilkan surat dari seorang pejabat tentang suatu hal yang terdapat dalam pemerintahan yang menjadi tanggung jawabnya dan dimaksudkan untuk membuktikan suatu hal atau keadaan. (3) Standar pembuktian yang tinggi dalam sistem peradilan pidana Indonesia terkadang sulit dipenuhi dalam kasus kejahatan siber, mengingat sifat bukti digital yang mudah dimanipulasi, bahkan yang lebih inheren ada pada fasilitas hukum yang sistemik untuk melakukan upaya digital forensik.

Kata Kunci: Digital Forensik, Penyidikan, Cybercrime.

ABSTRACT

Law enforcement agencies in various countries have begun prioritizing the development of specialized digital forensics units in response to increasingly widespread cyber threats. In Indonesia, the police are also increasing the capacity

of digital forensics laboratories, amidst the rise in data theft, ransomware attacks, online gambling, the child pornography industry, and other cybercrimes. Therefore, digital forensics is no longer considered an optional component but rather an essential requirement in the criminal justice system of the digital era.

The aim of this research is to determine and analyze (1) the form of legal policy in qualifying cybercrime in criminal law norms, (2) the legal procedures for digital forensic efforts in the investigation stage of cybercrime crimes, (3) the legal problems that occur in the function of digital forensics in the process of investigating cybercrime crimes.

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

The research results and discussion can be concluded as follows: (1) The Information and Electronic Transactions Law clarifies the scope of cybercrime by specifying the types of crimes specifically related to activities in the digital space. Articles 27 to 37 of the Information and Electronic Transactions Law specifically regulate crimes related to illegal content, unauthorized access, wiretapping, and attacks on the integrity of other systems. (2) According to Article 187 b of the Criminal Procedure Code, the results of digital forensic examinations in the form of a forensic laboratory report and a forensic expert report must be prepared in accordance with the provisions of laws and regulations or laws. This indicates that the results of digital forensic testing produce a letter from an official regarding a matter within the government that is his responsibility and is intended to prove a matter or condition. (3) The high standard of proof in the Indonesian criminal justice system is sometimes difficult to meet in cybercrime cases, given the easily manipulated nature of digital evidence, even more inherent in the systemic legal facilities for conducting digital forensic efforts.

Keywords: Digital Forensics, Investigation, Cybercrime.

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Hukum yang diciptakan oleh manusia mempunyai tujuan untuk menciptakan keadaan yang teratur, aman dan tertib. Demikian juga hukum pidana yang merupakan salah satu hukum yang dibuat oleh manusia.[1] Hukum ada karena keadaan dimana seseorang ingin merasakan perlindungan hukum dan berhak atas lingkungan hidup yang nyaman dan damai. Ciri dari negara hukum adalah adanya perlindungan terhadap suatu tindakan pidana.

Hukum yang menetapkan apa yang harus dilakukan dan apa yang tidak boleh dilakukan ataupun dilarang. Sasaran hukum yang hendak dituju bukan hanya orang yang nyata berbuat melawan hukum, melainkan juga perbuatan hukum yang kemungkinan akan terjadi, dan kepada alat perlengkapan negara untuk bertindak menurut hukum. Sistem bekerjanya hukum yang demikian itu menerapkan salah satu bentuk penegakan hukum yang berlaku di Indonesia.

Manusia merupakan individu yang sering disebut makhluk sosial. Sebagai individu, manusia mempunyai unsur jasmani dan rohani, unsur fisik dan psikis, serta unsur jiwa dan raga. Sebagai makhluk sosial, manusia saling berinteraksi antara satu dengan yang lainnya dalam kehidupan sehari-hari, hasil dari interaksi antar manusia

[1]Supriyono. Criminology Study of Crime of Fencing the Stolen Goods. *Jurnal Daulat Hukum*, 3 (1) March 2020, hlm 185

tidak selalu baik, tak jarang terjadi penyimpangan-penyimpangan dalam bertingkah laku di kehidupan sehari-hari.[2] Penyimpangan yang terjadi menimbulkan kegaduhan dan ketidaknyamanan dalam masyarakat. Penyimpangan yang dilakukan oleh individu tersebut dapat berupa pelanggaran terhadap norma ataupun tindak kejahatan.

Dalam hukum pidana, sesuatu yang dikatakan sebagai kejahatan apabila tindakan jahat tersebut dirumuskan dalam suatu delik atau tindak pidana dan bagi pelanggarnya dapat dijatuhi pidana. Hal ini sejalan dengan pendapat S.R. Sianturi yang menyebutkan bahwa tindak pidana merupakan suatu tindakan pada tempat, waktu, dan keadaan tertentu, yang dilarang dan diancam dengan pidana oleh undang-undang serta bersifat melawan hukum serta mengandung unsur kesalahan yang dilakukan oleh seseorang yang mampu bertanggung jawab.[3]

Proses penegakkan hukum pidana di Indonesia diatur dalam hukum acara pidana. Hukum acara pidana adalah peraturan yang ditetapkan negara untuk menentukan penyelesaian perkara pidana apabila terdapat orang yang diduga telah melakukan suatu perbuatan tindak pidana. Ini menunjukkan bahwa secara umum tugas hukum acara pidana adalah untuk melaksanakan ketentuan-ketentuan yang ditetapkan dalam hukum pidana. Hukum acara pidana juga merupakan peraturan yang

[2] R. Soeroso, *Pengantar Ilmu Hukum*, Sinar Grafika, Jakarta, 2013, hlm. 297

[3] S. R. Sianturi. *Asas-asas Hukum Pidana di Indonesia dan Penerapan*, Cet. 3. Jakarta: Storia Grafika, 2002, hlm.208.

menetapkan terkait wewenang penegak hukum untuk mengambil tindakan atau proses yang diperlukan untuk menyelesaikan perkara pidana.[4]

Penyelesaian perkara pidana dilakukan melalui beberapa tahapan dimulai dari tahap penyelidikan, tahap penyidikan, tahap penuntutan, tahap persidangan, serta tahap putusan hakim. Dalam ruang lingkup peradilan pidana, awal mula agar 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.[5] Apabila pada proses penyelidikan diyakini bahwa terdapat suatu tindak pidana maka tahapan selanjutnya yang dilakukan adalah tahap penyidikan yang dilakukan oleh penyidik. Proses Penyelidikan dan Penyidikan secara rinci diatur dalam Bab XIV mengenai Penyidikan yaitu Pasal 102-136 KUHAP.[6]

Menurut Pasal 1 angka 2 KUHAP penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangka. Berdasarkan pasal di atas yang diberi kewenangan untuk melakukan penyidikan disebut dengan penyidik. Berdasarkan

---

[4] Ramelan, *Hukum Acara Pidana Teori dan Implementasinya*, Sumber Ilmu Jaya, Jakarta, 2016, hlm 4.

[5] Mutia Hafina Putri, dkk. Proses Penyidikan dalam Sistem Peradilan Pidana Investigation Process in the Criminal Justice System, *Rewang Rencang : Jurnal Hukum Lex Generalis*. 4 (7) 2023, hlm 8

[6] Abdul Hadi, *Fungsi Dan Peran Sidik Jari Dalam Proses Pelaksanaan Penyidikan Ditinjau Dari KUHAP*, Fakultas Hukum Universitas Pancasila, Jakarta, 2004, hlm 29

ketentuan umum Pasal 1 angka 1 KUHAP penyidik adalah pejabat polisi negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh Undang-Undang untuk melakukan penyidikan.

Pada Penyidikan tindak pidana, penyidik mengumpulkan bukti-bukti guna memperkuat dugaan bahwa seseorang yang di duga melakukan tindak pidana benar melakukan suatu tindak pidana. Dalam hukum pidana di Indonesia mengenal adanya barang bukti dan juga alat bukti. Barang bukti menurut Andi Hamzah adalah objek materiel yang meliputi suatu perkara pidana, tetapi barang bukti tidak hanya terbatas pada peluru, pisau, senjata api, perhiasan, televisi, dan lain-lain.[7]

Benda-benda yang dijadikan sebagai barang bukti tersebut adalah benda berwujud, meskipun wujud dari barang bukti itu sendiri tidak ditentukan secara langsung dalam undang-undang. Namun selama ia memiliki relevansi dengan perkara pidana suatu benda dapat dijadikan barang bukti. Alat bukti menurut Andi Hamzah[8] diartikan sebagai segala sesuatu yang berhubungan dengan suatu perbuatan dan dapat digunakan sebagai bahan pembuktian. Pasal 184 ayat 1 KUHAP telah mengatur unsur alat bukti yang sah berdasarkan undang-undang, yaitu (a) Keterangan Saksi; (b) Keterangan Ahli; (c) Surat; (d) Petunjuk; (e) Keterangan Terdakwa.

Selain alat bukti sebagaimana yang terdapat pada KUHAP, Indonesia juga mengakui alat bukti lain seperti pada Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan

[7] Andi Hamzah, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta, 2008, hlm.120
[8] *Ibid*

Transaksi Elektronik Pasal 5 ayat (1) bahwa "Informasi Elektronik dan/ atau Dokumen Elektronik dan/ atau hasil cetaknya merupakan alat bukti hukum yang sah" serta Pasal 5 ayat (2) bahwa "Informasi Elektronik dan/ atau Dokumen Elektronik dan/ atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia".[9]

Seiring dengan perkembangan masyarakat di dunia teknologi informasi dengan hadirnya internet dalam kehidupan manusia. Transformasi signifikan dalam pola interaksi manusia terjadi berkat kemajuan ilmu pengetahuan dan teknologi di bidang teknologi komunikasi. Hal ini memungkinkan komunikasi tanpa batasan geografis dan waktu, membuka jalan menuju era baru dengan perubahan struktur sosial dan nilai-nilai masyarakat, dari yang lokal dan spesifik menjadi global dan universal, serta mempengaruhi nilai-nilai, norma, moral, dan etika.[10]

Era teknologi informasi dimulai seiring dengan munculnya inovasi komputer. Awalnya, komputer hadir dalam bentuk mainframe computer pada dekade 1950-an hingga akhir 1970-an. Produsen utama seperti IBM dan *The Seven Dwarfs* memainkan peran kunci dalam perkembangan *mainframe computer*. [11] Kemajuan teknologi informasi dan komunikasi membawa perubahan signifikan dalam interaksi

[9] Pasal 5 ayat (1) dan ayat (2) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[10] Synthiana Rachmie, Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website, *Jurnal Litigasi*, 21 (1) April 2020, hlm 105

[11] A. Tatumpe, Analisis Yuridis Digital Forensik dalam Pembuktian Tindak Pidana di Indonesia. *Scientia De Lex*, 7 (1) 2019

sosial dan peradaban manusia secara global. Proliferasi perangkat elektronik seperti ponsel pintar, otomatisasi layanan publik, surat kabar digital, dan perangkat lunak memudahkan komunikasi dan tugas-tugas sehari-hari, mengintegrasikan teknologi dalam berbagai aspek kehidupan manusia termasuk transaksi keuangan.[12]

Dinamika perkembangan teknologi ini terdapat pro dan kontra, karena terdapat banyak sekali dampak positif dan negatif yang terjadi dalam lingkungan masyarakat saat ini. Dari sisi positifnya teknologi sangat membantu dan memberikan manfaat bagi kehidupan manusia zaman sekarang namun dari sisi negatif yaitu mempermudah manusia dalam melakukan segala tindak kejahatan dari yang biasa maupun luar biasa.

Penggunaan teknologi informasi memunculkan sistem hukum baru yang dikenal sebagai hukum siber. Istilah ini merujuk pada bidang hukum terkait penggunaan teknologi informasi, mencakup aktivitas melalui jaringan komputer dan internet. Kejahatan komputer atau kejahatan siber atau dalam istilah *cybercrime* merupakan pelanggaran hukum pidana yang memengaruhi berbagai kalangan, menuntut respons aktif dari lembaga Kepolisian untuk menangani kasus-kasus yang melibatkan wilayah yang sangat luas dan tak terbatas.[13]

Pada awalnya, tindak pidana hanya diatur oleh Kitab Undang-Undang Hukum Pidana (KUHP). Pemerintah sebagai penjamin kepastian hukum dapat memanfaatkan teknologi canggih berdasarkan masalah hukum tersebut. Salah satu buktinya adalah

[12] Budiman, dkk. Akses dan Penggunaan Teknologi Informasi dan Komunikasi pada Rumah Tangga dan Individu, *Jurnal Penelitian Komunikasi dan Pembangunan*, 15 (1) Juni 2024, hlm 2

[13] A.A. Agus dan Riskawati, Penanganan Kasus Cybercrime di Kota Makassar (Studi pada Kantor Kepolisian Resort Kota Besar Makassar), *Jurnal Supremasi*, 11 (1) 2016

kebijakan yang ditetapkan dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.[14] Perkembangan teknologi memberikan konsekuensi sepadan, tergantung pada cara penggunaannya. Keuntungan termasuk kemudahan dalam aktivitas individu atau kelompok, namun dampak negatif muncul ketika teknologi disalahgunakan untuk kejahatan dunia maya.[15] Peningkatan sistem keamanan menjadi penting dalam menghadapi lonjakan kasus *cybercrime*, memerlukan upaya aktif dalam mengidentifikasi dan mengatasi modus baru dari para pelaku kejahatan dunia maya.

Selain mengalami perkembangan dari segi bukti, dalam menangani suatu perkara pidana penanganan kasus tindak pidana terutama dalam proses penyidikan juga harus mengalami kemajuan dan perkembangan seiring dengan perkembangan ilmu pengetahuan dan teknologi modern. Diantaranya dapat dilihat dari bagaimana penyidik yang memiliki kompetensi yang sesuai menggunakan ilmu penunjang lainnya untuk mempercepat proses penyelesaian kasus pidana. Terutama dalam menangani kasus yang dalam penanganannya berkaitan dengan teknologi informasi yang terdapat berbagai bukti elektronik pada kasus cybercrime.[16]

Berhubungan dengan tindak pidana cybercrime sangat membutuhkan banyak bukti elektronik agar dapat menjelaskan suatu perkara pidana. Dalam proses

[14] Sry Wahyuni, Yoserwan, Pertanggungjawaban Pidana terhadap Pencemaran Nama Baik melalui Media Sosial, *Unes Law Review*, 6 (1) 2023, hlm 260

[15] M. Riskiyadi, Investigasi Forensik Terhadap Bukti Digital dalam Mengungkap Cybercrime, *Cybersecurity dan Forensik Digital*, 3 (2) 2020, hlm 14

[16] Synthiana Rachmie, *Op.Cit*, 21 (1) April 2020, hlm 106

penanganan tindak pidana yang didalamnya menggunakan teknologi informasi, menurut Christopher seorang ahli digital forensik, menyatakan bahwa bukti asli tidak dapat dianalisis dalam dunia digital dan elektronik karena bukti harus tetap terjaga keasliannya.[17] Namun diantara beberapa ciri dari suatu bukti elektronik salah satunya adalah dapat secara mudah digandakan dan persis dengan yang asli, sehingga perlu didalami kembali apakah data tersebut hasil dari penggandaan atau data yang asli.[18]

Bukti Informasi elektronik dan/atau dokumen elektronik yang mudah diubah dan dimanipulasi oleh pelaku tindak pidana untuk menghilangkan jejak tindakannya juga membuat aparat penegak hukum mengalami kesulitan dalam memastikan keaslian/keotentikan informasi dan/atau dokumen elektronik yang akan digunakan sebagai bukti dalam pembuktian di pengadilan. Oleh karena itu, agar bukti elektronik dianggap sah dan otentik maka diperlukan suatu cabang disiplin ilmu yaitu ilmu forensik digital.

Dalam penanganan kasus *cybercrime*, diperlukan penerapan forensik. Forensik adalah proses untuk menyelidiki dan memverifikasi fakta terkait kejadian kriminal dan aspek hukum yang terkait. Analisis forensik memiliki peran kunci, terutama jika bukti akan dibawa ke persidangan. Forensik digital, bagian dari bidang forensik, mencakup identifikasi dan investigasi materi atau data dari perangkat digital.

Forensik digital, juga disebut digital forensik merupakan salah satu sarana untuk membantu penyidik dalam kewenangannya melakukan penyelidikan dan

[17] *Ibid*, hlm 120
[18] *Ibid*, hlm 107

penyidikan yang diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo Kitab Undang-undang Hukum Acara Pidana (KUHAP). Digital forensik, adalah ilmu pengetahuan dan keahlian yang digunakan untuk mengidentifikasi, mengumpulkan, menganalisa, dan menguji bukti elektronik dalam kasus yang membutuhkan identifikasi dan penanganan bukti elektronik.

Jejak digital adalah fokus dari upaya penyelidikan dalam digital forensik, memperkuat atau melemahkan bukti fisik dalam suatu kasus. Istilah ini awalnya terkait dengan forensik komputer, namun kini mencakup analisis dari semua perangkat penyimpan data digital. Praktik forensik digital telah berkembang seiring popularitas komputasi pribadi dan era internet.[19]

Fungsional bukti digital dalam beberapa kasus *cybercrime* memang sangat kompleks. Penggunaan bukti digital juga masih sering memunculkan perdebatan. Uji forensik digital yang harus ada sebagai pendukung bukti digital tersebut juga masih kurang mendapatkan kepastian hukum. Pembuktian menggunakan bukti elektronik dalam perkara pidana khusus yang dalam undang-undang secara khusus mengatur bukti elektronik sebagai salah satu alat bukti yang sah memang lebih menjamin kepastian hukum dari penggunaan bukti elektronik. Namun, terkait dengan hasil uji forensik digital yang dihadirkan ke dalam persidangan sebagai alat bukti masih menjadi pertanyaan besar. Perdebatan lain yang sering kali muncul terkait dengan proses

[19] N. Aisyah, dkk. Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime Di Indonesia Secara Systematic Review. *Jurnal Esensi Infokom*, 6(1) 2022, hlm 22.

pengujian bukti elektronik, proses pemeliharaan bukti elektronik dan juga sering diperdebatkan kemampuan seorang ahli forensik digital dalam melakukan pengujian bukti elektronik karena serangkaian proses ini belum ada pengaturan secara lebih rinci. Tidak adanya pengaturan mengenai proses pengujian bukti elektronik menyebabkan pengujian yang dilakukan juga dapat dicurigai terjadi manipulasi pada bukti elektronik tersebut akan merugikan berbagai pihak, hal ini sangat terkait dengan integritas. Belum adanya pengaturan secara khusus mengenai proses pengujian bukti elektronik juga menjadi salah satu problematika pokok dari eksistensi hasil uji forensik digital dalam pembuktian.

Dalam konteks penegakan hukum modern, kehadiran digital forensik menjadi sangat penting untuk menjamin validitas alat bukti di ruang sidang. Tidak hanya sekadar perangkat teknis, digital forensik kini menjelma menjadi komponen strategis dalam penyidikan berbagai tindak pidana *cybercrime*. Berdasarkan data dari Interpol Global Crime Trend Summary Report tahun 2024, kasus *cybercrime* meningkat lebih dari 60% dalam 5 tahun terakhir[20], yang menunjukkan urgensi penerapan metode forensik digital yang akurat.

Lembaga penegak hukum di berbagai negara mulai memprioritaskan pengembangan unit khusus digital forensik sebagai bentuk respons terhadap ancaman dunia maya yang kian masif. Di Indonesia, peningkatan kapasitas laboratorium forensik digital melalui Lembaga Kepolisian juga tengah dilakukan, seiring dengan

[20] https://www.interpol.int/How-we-work/Criminal-intelligence-analysis/Our-analysis-reports, Diakses Pada Tanggal 23 Juli 2025

maraknya kasus pencurian data, serangan ransomware, perjudian online, industri pornografi anak dan kejahatan siber lainnya. Dengan demikian, digital forensik tidak lagi dianggap sebagai opsi tambahan, melainkan menjadi kebutuhan esensial dalam sistem peradilan pidana era digital.

Berdasarkan latar belakang tersebut, penulis mengadakan penelitian dengan memilih judul "*Fungsional Digital Forensik dalam Tahap Penyidikan Tindak Pidana Cybercrime*".

B. Rumusan Masalah

Berdasarkan latar belakang telah diuraikan sebagaimana tersebut di atas, maka permasalahan yang dianalisis dalam penelitian tesis ini adalah :

1. Apa bentuk politik hukum dalam mengkualifikasikan *cybercrime* dalam norma hukum pidana?
2. Bagaimana prosedur hukum upaya digital forensik dalam tahap penyidikan tindak pidana *cybercrime*?
3. Apa problematika hukum yang terjadi dalam fungsional digital forensik pada proses penyidikan tindak pidana *cybercrime*?

C. Tujuan Penelitian

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

1. Untuk mengetahui dan menganalisis bentuk politik hukum dalam mengkualifikasikan cybercrime dalam norma hukum pidana;
2. Untuk mengetahui dan menganalisis prosedur hukum upaya digital forensik dalam tahap penyidikan tindak pidana cybercrime;
3. Untuk mengetahui dan menganalisis problematika hukum yang terjadi dalam fungsional digital forensik pada proses penyidikan tindak pidana cybercrime.

D. Manfaat Penelitian

Manfaat dari penelitian ini diharapkan dapat memberikan sumbangsih bagi para pihak, antara lain:

1. Manfaat Teoritis

   Hasil penelitian ini diharapkan dapat berguna untuk kalangan praktisi dan kalangan akademisi dalam mengembangkan ilmu pengetahuan hukum pidana, yang ternyata sekarang paradigma yang berkembang bukan semata-mata hanya implementasi sebuah produk hukum saja tetapi ada bentuk formulatif dalam fungsional digital forensik dalam tahap penyidikan tindak pidana cybercrime.

2. Manfaat Praktis

   Adapun manfaat praktis dari penelitian ini, yakni dapat memberikan konsep pemikiran tentang fungsional digital forensik dalam tahap penyidikan tindak pidana cybercrime dan perlu untuk penjabaran secara ilmiah hukum.

E. Kerangka Konseptual

a. Digital Forensik

Digital Forensik merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital. Sebagai ilmu yang masih baru, masih dibutuhkan pemahaman dan kemampuan untuk menguasai ilmu ini. Penguasaan ilmu ini tidak hanya ditujukan kepada kemampuan teknis semata tetapi juga terkait dengan bidang lain, seperti bidang hukum. Penanganan kasus-kasus yang terkait dengan penggunaan teknologi informasi sering membutuhkan forensik. Forensik merupakan kegiatan untuk melakukan investigasi dan menetapkan fakta yang berhubungan dengan kejadian kriminal dan permasalahan hukum lainnya. Digital Forensik dapat dibagi lebih jauh menjadi forensik yang terkait dengan komputer (*host, server*), jaringan (*network*), aplikasi (termasuk database), dan perangkat (*digital devices*). Masing-masing memiliki pendalaman tersendiri.[21]

b. 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

[21] Budi Rahardjo, Sekilas Mengenai Forensik Digital, *Jurnal Sosioteknologi*, 12 (29) Agustus 2013, hlm 385

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. Penyidikan meliputi kegiatan penggeledahan dan penyitaan, demikian halnya penyidikan yang dilakukan terhadap pelaku. Penyitaan ini erat hubungannya dengan kewenangan Polri sebagai penyidik sering membutuhkan penyitaan meskipun sifatnya sementara, terutama bila adanya dugaan telah terjadi suatu perbuatan pidana.[22]

c. Tindak Pidana

Istilah tindak pidana dipakai sebagai terjemah dari istilah *strafbaar feit* atau *delict*. *Strafbaar feit* terdiri dari tiga kata, yakni *straf*, *baar*, dan *feit*, secara *literlijk*, kata "*straf*" artinya pidana, "*baar*" artinya dapat atau boleh dan "*feit*" adalah perbuatan. Dalam kaitannya dengan istilah *strafbaar feit* secara utuh, ternyata *straf* diterjemahkan juga dengankata hukum. Dan sudah lazim hukum itu adalah terjemahan dari kata *recht*, seolah-olah arti *straf* sama dengan *recht*. Untuk kata "*baar*", ada dua istilah yang digunakan yakni boleh dan dapat. Sedangkan kata "*feit*" digunakan empat istilah yakni, tindak, peristiwa, pelanggaran, dan perbuatan.[23]

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

[23] Adami Chazawi, *Pelajaran Hukum Pidana Bagian I,* Jakarta: Rajawali Pers, 2011, hlm.69.

d. Cybercrime

Dalam dua dokumen Kongres PBB mengenai *The Prevention of Crime and the Treatment of Offenders di Havana*, Cuba pada tahun 1990 dan di Wina, Austria pada tahun 2000, ada dua istilah yang dikenal (1) *Cybercrime* dalam arti sempit disebut computer crime, yaitu prilaku illegal atau melanggar secara langsung menyerang sistem keamanan suatu computer atau data yang diproses oleh komputer; (2) *Cybercrime* dalam arti luas disebut computer related crime, yaitu prilaku ilegal atau melanggar yang berkaitan dengan sistem komputer atau jaringan. Dari beberapa pengertian diatas, secara ringkas dapat dikatakan bahwa *cybercrime* dapat didefinisikan adalah suatu tindakan kriminal yang melanggar hukum dengan menggunakan teknologi komputer sebagai alat kejahatannya. *Cybercrime* ini terjadi karena ada kemajuan di bidang teknologi komputer atau dunia IT khususnya media internet.[24]

F. Kerangka Teori

1. Teori *Locard's Exchange*

Edmond Locard yang terkenal dengan *Locard's Exchange*-nya lahir pada tanggal 13 Desember 1877 di Saint-Chamond, Perancis. Sedikit mengulas tentang masa kecil Edmond Locard, dijelaskan bahwa masa kecil Locard telah mengalami pelecehan seksual oleh orang tuanya sendiri. Kejadian

[24] Eliasta Ketaren, Cybercrime, Cybespace, dan Cyberlaw. *Jurnal Times*, V (2) 2016, hlm 36

yang seperti itu tentunya tidak mudah dijalani oleh Locard, namun dia bertekad untuk membantu mengurangi kekerasan yang terjadi pada manusia disekelilingnya. Locard bekerja keras untuk memecahkan kasus-kasus kekerasan dan bahkan pembunuhan untuk membantu para korban, dan dengan kerja kerasnya itulah dia mendapat julukan "*Helper*" atau "penolong"[25] seperti karakter fiksi Sherlock Holmes.

Locard mempelajari ilmu kedokteran di Lyon dan mendapat gelar Doktor dari bidang kedokteran pada tahun 1902. Locard mulai tertarik untuk menggabungkan ilmu pengetahuan dan kedokteran kedalam masalah hukum. Pada tahun 1910, Departemen Kepolisian Lyon mendirikan laboratorium Penyelidikan Kejahatan pertama, Locard diizinkan untuk mengidentifikasi kumpulan barang bukti yang dibawa dari TKP. Locard benar-benar memberikan kontribusi yang sangat besar dalam bidang forensik, hingga saat ini prinsip Locard Exchange dipakai dalam bidang forensik dari berbagai jenis bidang keilmuan. Dalam semasa hidupnya, Locard banyak mempublikasi karyanya dalam bentuk tulisan dalam bahasa Perancis, Inggris, Jerman dan Spanyol. Karya-karya tersebut masih menjadi rujukan atau prinsip oleh seseorang yang menekuni bidang forensik, maka terciptalah sebuah istilah "*Locard's Exchange Principle*".[26]

[25] Kirk Paul L, Crime Investigation, Physical Evidence and the Police Laboratory, *New York: Interscience Publishers*, 21 (4) December 1953

[26] *Ibid*

Prinsip yang paling terkenal adalah prinsip pertukaran data, Locard menyebutkan bahwa "*every contact leaves a trace*" yang artinya setiap kontak akan meninggalkan jejak. Prinsip dasar Locard inilah yang menjadi acuan bahwa setiap sesuatu yang bersentuhan pasti akan meninggalkan suatu jejak sekecil apapun jejak tersebut dan jejak-jejak itulah yang akan dikumpulkan, kemudian dianalisis sehingga menjadi sebuah petunjuk yang akan mengerucut kepada siapa yang memiliki jejak tersebut.

Locard dalam pubilkasinya "*La Police et ies methhodes Scientifiques*" pada tahun 1934 mengatakan "*Any action of an individual, and obviously, the violent actions of a crime, cannot occur without leaving a trace*"[27] kurang lebih artinya "setiap tindakan individu, dan jelas, aksi kejahatan kekerasan, tidak bisa terjadi tanpa meninggalkan jejak.", dengan kata lain selalu akan ada bukti fisik yang akan ditinggalkan dalam sebuah tindak kekerasan atau kejahatan, meski sudah diupayakan untuk menghapus jejak – jejak tersebut, karena sejatinya bekas/jejak tidak akan hilang seluruhnya.

Seperti yang dikutip dari Teori Locard yang dijelaskan oleh Paul L. Kirk (1953) dalam bukunya yang berjudul "*Crime Investigation: Physical evidence and the police laboratory*" yang menyatakan bahwa "*Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his*

[27] Edmond Locard, *La Police et les Méthodes Scientifiques*, Éditions Rieder, 1934, hlm 11

hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value".[28]

Artinya "kemanapun dia melangkah, apapun yang dia sentuh, apapun yang dia tinggalkan, tanpa disadari, akan menjadi saksi bisu untuknya. Tidak hanya sidik jari atau jejak kakinya, tapi rambutnya, serat pakaian dari bajunya, kaca yang dipecahkan, jejak alat yang tertinggal, cat yang digores, darah atau sperma yang dia simpan atau dia kumpulkan, dan sebagainya, menjadi saksi bisa terhadapnya, ini adalah bukti yang tidak akan pernah lupa, tidak akan keliru disaat kejadian, tidak akan hilang karena tidak ada saksi mata. Ini adalah bukti yang nyata, bukti fisik tidak akan salah, dia tidak dapat memalsukan dirinya sendiri, dia tidak akan sepenuhnya hilang, hanya manusia yang gagal menemukannya, pelajari dan pahamilah itu, dapat mengurangi nilainya". Pendek artian, bahwa bukti fisik tidak akan pernah hilang, jika penyidik menyatakan bahwa tidak ditemukan bukti dari pelaku, maka yang gagal menemukan bukti adalah penyidik itu sendiri.

[28] Kirk Paul L, *Op.Cit*, 21 (4) December 1953

Teori-teori yang dinyatakan oleh Edmond Locard sangat fenomenal pada saat itu dan teorinya banyak mengungkap kasus kejahatan sehingga Locard disebut-sebut sebagai pelopor ilmu forensik dan kriminologi.

Kasus pertama yang ditangani oleh Locard dan berhasil dipecahkan adalah beredarnya uang logam palsu di sekitar wilayah tempat tinggalnya, pihak kepolisian mengetahui identitas para pelaku, namun mereka kesulitan dalam menangkap basah si pelaku untuk dijadikan bukti yang akurat. Akhirnya, Polisi menangkap tiga tersangka, namun para tersangka menolak untuk mengakui bahwa mereka adalah pembuat uang logam palsu. Locard mendengar kabar tersebut, kemudian ia meminta pakaian para tersangka untuk diperiksa. Pada saat itu tidak ada yang mengerti apa yang akan dilakukan Locard pada pakaian itu. Locard sangat bersemangat untuk melakukan pekerjaan sebagai konsultan detektif karena dia ingin membuktikan bahwa dia mempunyai teori yang benar sehingga teorinya dapat diakui suatu saat nanti.

Dengan kaca pembesar dan pinset, Locard memeriksa celana salah satu tersangka, dalam saku, dia melihat debu yang tak biasa, kemudian dengan hati-hati, Locard memindah debu tersebut keselembar kertas putih. Dibawah kaca pembesar, debu itu menunjukkan bahwa benda tersebut merupakan jejak dari logam. Dengan menerapkan tes kimia untuk beberapa butir debu sebagai lanjutan dari observasinya, Locard menemukan timah (*tin*), logam keputih-putihan (*antimony*), timah (*lead*). Apa yang ditemukan oleh Locard dalam observasinya cocok dengan komponen dari uang logam palsu. Bukti yang sama

juga ditemukan pada pakaian dari dua tersangka lainnya. Jadi, Locard telah berhasil membuktikan teorinya dalam mengungkap kasus uang palsu dan berhasil menunjukkan bahwa tersangka tersebut adalah pelaku dalam pembuatan mata uang logam palsu.

"*Every contact leaves a trace*", pernyataan Locard yang sangat fenomenal dan menjadi dasar investigasi telah diterapkan disegala bidang investigasi di berbagai disiplin ilmu.[29]

2. Teori Pembuktian

Dalam bidang pembuktian dikenal beberapa sistem atau teori pembuktian (*bewijstheorie*). Pertama adalah *positief wettelijk bewijstheorie* atau disebut sistem pembuktian berdasrkan undang-undang secara positif. Dikatakan secara positif, karena pembuktian sangat terikat pada undang-undang. Artinya, jika telah terbukti suatu perbuatan sesuai dengan alat-alat bukti yang disebut oleh undang-undang, maka keyakinan hakim tidak diperlukan sama sekali.[30]

Sistem pembuktian ini digunakan dalam hukum acara perdata, kebenaran yang dicari adalah kebenaran formal. Kebenaran yang dicari hanya berdasarkan alat bukti yang ada dalam undang-undang semata dan hakim dalam memeriksa perkara hanya sebatas alat-alat bukti yang diajukan oleh para pihak.

[29] Edmond Locard, *Op.Cit*, 1934
[30] Andi Hamzah, *Op.Cit*, 2008, hlm 251.

Wirjono Projodikoro dalam bukunya berpendapat bahwa sistem pembuktian ini sama sekali tidak mengandung suatu kepercayaan kepada kesan-kesan perseorangn dari hakim. Bisa dikatakan bahwa hakim hanya sebagai corong dari undang-undang atau hanya sebagai perlengkapan saja.[31]

Kedua adalah sistem pembuktian *conviction intime* atau sistem pembuktian keyakinan semata. Dalam sistem ini, untuk menjatuhkan putusan, dasar pembuktinnya hanya semata-mata diserahkan kepada keyakinan hakim. Hakim tidak terikat pada alat bukti, namun hanya berdasarkan keyakinan yang timbul dari hati nurani dan sifat bijaksana seorang hakim. Andi Hamzah berpendapat, bahwa sistem ini memberi kebebasan kepada hakim terlalu besar, sehingga sulit diawasi dan terdakwa atau penasihat hukum juga akan dirugikan karena sulit untuk melakukan pembelaan.[32]

Ketiga adalah system pembuktian *conviction raisonee*. Sistem pembuktian ini artinya, dasar pembuktian menurut keyakinan hakim dalam batas-batas tertentu atas alasan yang logis. Dalam sistem pembuktiaan ini hakim diberi kebebeasan untuk memakai alat-alat bukti disertai dengan alasan logis. Dalam konteks hukum Indonesia, *conviction raisonee* digunakan dalam persidangan tindak pidana ringan, termasuk perkara lalu lintas dan persidangn

[31] Wirjono Projodikoro, *Hukum Acara Pidana Indonesia*, Sumur Bandung, Bandung, 1981, hlm 92

[32] Andi Hamzah, *Op.Cit*., 2008, h 252

perkara pidana dalam acara cepat yang tidak membutuhkan jaksa penuntut umum untuk menghadirkan terdakwa.

Keempat adalah sistem pembuktian berdasarkan undangundang secara negatif atau sering disebut dengan *negatief wettelijk*. Sistem pembuktian ini sangat dikenal dalam sistem peradilan pidana Indonesia. Negatief wettelijk mendasarkan pembuktian pada keyakinan hakim yang timbul dari alat bukti dalam undang-undang secara negatif. Dalam hukum Indonesia sistem pembuktian *negatief wettelijk* ini tercermin dalm ketentuan Pasal 183 KUHAP, yang berbunyi :

> Hakim Tidak boleh menjatuhkan pidana kepada seseorang, kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukanya.

Membuat suatu putusan didasarkan Pasal 183 KUHAP, seorang hakim harus memperoleh keyakinan tentang suatu tindak pidana yang dilakukan oleh terdakwa berdasarkan alat bukti yang sah dalam Pasal 184 KUHAP. Penerapan dua alat bukti yang sah itu dapat dengan sekurangkurangnya seorang saksi ditambah dengan seorang ahli atau surat maupun petunjuk, dengan ketentuan ketentuan alat bukti tersebut saling menguatkan, atau bisa juga dengan keterangan dua orang saksi yang saling bersesuaian, maupun penggabungan antara keterangn seorang saksi dengan keterangan terdakwa, asal keterangan saksi dengan keterngn terdakwa jelas saling bersesuaian. Tentang adanya

keterngan saksi, ada asas yang berkaitan yang menyatakan, satu saksi bukan merupakan saksi (*unus testis nullus testis*).

G. Metode Penelitian

Dalam penelitian ini penulis menggunakan metode penelitian sebagai berikut:

1. Metode Pendekatan

Dalam penelitian yang dilaksanakan, penulisan memperrgunakan pendekatan Yuridis Normatif, yaitu penelitian yang menggunkan metode pendekatan terhadap masalah dengan melihat norma atau Undang-Undang yang berlaku sebagai ketentuan positif, berikut ini teori yang relevan dengan karya tulis ini dengan mengaitkan implementasinya terhadap fakta yang terdapat di lapangan.

2. Spesifikasi Penelitian

Spesifikasi penelitian yang dilakukan menggunakan metode pendekatan deskriptif analitis, yaitu memaparkan dan menganalisis data secara sistematis dengan maksud untuk memberikan data yang seteliti mungkin tentang manusia, keadaan dan gejala-gejala lainnya. Deskriptif mengandung arti, bahwa penulis ingin menggambarkan dan memberikan data yang seteliti mungkin, sistematis dan menyeluruh. Analitis mengandung makna, mengelompokkan, menggabungkan dan membandingkan aspek yang berkaitan dengan masalah secara teori dan praktek.

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 Acara Pidana;
    c. Undang-undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia;
    d. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
    e. Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 6 Tahun 2019 tentang Penyidikan Tindak Pidana.
2) Bahan hukum sekunder yaitu terdiri dari:
    a. Buku-buku;
    b. Hasil penelitian ahli hukum;
    c. Tesis, Skripsi, Disertasi.
3) Bahan hukum tersier yang terdiri dari:
    a. Kamus Hukum;
    b. Kamus besar bahasa Indonesia;.

4. Metode Pengumpulan Data

Untuk mendapatkan data dalam penelitian ini, digunakan metode pengumpulan data sekunder 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 Penyajian Data

Data yang diperoleh dari penelitian kemudian disusun secara teratur selanjutnya dilakukan proses *editing*, untuk memeriksa atau meneliti data yang diperoleh untuk menjamin apakah sudah dapat dipertanggung jawabkan sesuai dengan kenyataan dan dalam *editing* dilakukan pembetulan data yang keliru serta melengkapi data yang kurang kemudian data tersebut dianalisa disajikan dalam bentuk uraian.

6. 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, Kegunaan Penelitian, Kerangka Konseptual, Kerangka Teori, Metode Penelitian, Sistematika Penulisan.

BAB II, Tinjauan Pustaka terdiri dari: Tinjauan Umum Penyidikan, Tinjauan Umum Tindak Pidana, Tinjauan Umum Cybercrime, Tinjauan Umum Digital Forensik, Pembuktian Pidana dalam Perspektif Hukum Islam.

BAB III Hasil Penelitian Dan Pembahasan, terdiri dari: (1) bentuk politik hukum dalam mengkualifikasikan *cybercrime* dalam norma hukum pidana, (2) prosedur hukum upaya digital forensik dalam tahap penyidikan tindak pidana *cybercrime*, dan (3) problematika hukum yang terjadi dalam fungsional digital forensik pada proses penyidikan tindak pidana *cybercrime*.

BAB IV Penutup, terdiri dari: Kesimpulan, Saran.

BAB II

TINJAUAN PUSTAKA

A. Tinjauan Umum Penyidikan

Tahap penyidikan merupakan salah satu bagian penting dalam rangkaian tahap-tahap yang harus dilalui suatu kasus menuju pengungkapan terbukti atau tidaknya dugaan telah terjadinya suatu tindak pidana. Oleh sebab itu keberadaan tahap penyidikan tidak bisa dilepaskan dari adanya ketentuan perundangan yang mengatur mengenai tindak pidanananya.[33]

Penyidikan menurut Kitab Undang-Undang Hukum Acara Pidana yang tercantung dalan Pasal 1 angka 2 diartikan:

> "Serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam Kitab Undang-Undang Hukum Acara Pidana untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terangnya suatu tindak pidana yang terjadi dan guna menemukan tersangkanya".

Penyidikan merupakan rangkaian tindakan penyidik untuk mencari dan mengumpulkan bukti agar dapat ditemukan tersangka. Sedangkan menurut K.wantjik Saleh yang dikutip dalam jurnal hukum Sahuri Lasmadi, penyidikan sendiri diartikan yaitu usaha dan tindakan untuk mencari dan menemukan kebenaran tentang apakah betul terjadi suatu tindak pidana, siapa yang melakukan perbuatan itu, bagaimana sifat perbuatan itu serta siapakah yang terlibat dengan perbuatan itu.[34]

---

[33] Hibnu Nugroho, *Integralisasi Penyidikan Tindak Pidana Korupsi di Indonesia*, Media Aksara Prima, Jakarta, 2012, hlm. 67.

[34] Sahuri Lasmadi, Tumpang Tindih Kewenangan Penyidikan Pada Tindak Pidana Korupsi Pada Perspektif Sistem Peradilan Pidana, *Jurnal Ilmu Hukum*, 2 (3) Juli 2010, hlm. 10.

Penyidik sendiri menurut Pasal 45 angka (1) Undang-Undang Nomor 30 Tahun 2002 adalah:

"Penyidik pada Komisi Pemberantasan Korupsi yang diangkat dan diberhentikan oleh Komisi Pemberantasan Korupsi dan Penyidik melaksanakan fungsi penyidikan tindak pidana korupsi".

Dalam penyidikan sendiri ada yang disebut penyidik yaitu orang yang melakukan penyidikan yang terdiri dari pejabat yang dijelaskan pada Pasal 1 butir (1) Kitab Undang-Undang Hukum Pidana. Pejabat penyidik sendiri terdiri dari Penyidik Polri dan Penyidik Pegawai Negeri Sipil.[35]

Tahap penyidikan terhadap suatu perkara biasanya dilakukan setelah penyidik mengetahui adanya suatu peristiwa yang diduga merupakan suatu tindak pidana. Disamping itu, penyidikan juga akan dimulai apabila penyidik menerima laporan ataupun pengaduan tentang dugaan telah terjadinya suatu tindak pidana.

Sehubungan dengan hal tersebut, Yahya Harahap memberikan penjelasan mengenai penyidik dan penyidikan yaitu:

"Sebagaimana yang telah dijelaskan pada pembahasan ketentuan umum Pasal I Butir 1 dan 2, Merumuskan pengertian penyidikan yang menyatakan,penyidik adalah pejabat Polri atau pejabat pegawai negeri tertentu yang diberi wewenang oleh undang-undang. Sadangkan penyidik sesuai dengan cara yang diatur dalam undang-undang untuk mencari dan mengumpulkan bukti, dan dengan bukti itu membuat atau menjadi terang suatu tindak pidana yang terjadi serta sekaligus menemukan tersangkanya atau pelaku tindak pidananya".[36]

Sedangkan Andi Hamzah, definisi dari Pasal 1 butir 2 yaitu :

---

[35] M. Yahya Harahap, *Pembahasan Permasalahan Dan Penerapan KUHAP, Penyidikan dan Penuntutan*, Cet VII, Sinar Grafika, Jakarta, 2009, hlm. 112.

[36] *Ibid*., hlm. 15.

Penyidikan dalam acara pidana hanya dapat dilakukan berdasarkan undang-undang, hal ini dapat disimpulkan dari kata-kata menurut cara yang diatur dalam undang-undang ini.[37]

Dalam bahasa Belanda ini sama dengan opsporing. Menurut de Pinto yang dikutip dalam jurnal Bambang Tri Bawono menyebutkan bahwa 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.[38]

Dari pengertian diatas dapat disimpulkan bahwa penyidikan merupakan suatu proses atau langkah awal yang merupakan suatu proses penyelesaian suatu tindakpidana yang perlu diselidik dan diusut secara tuntas di dalam sistem peradilan pidana, dari pengertian tersebut, maka bagian-bagian dari hukum acara pidana yang menyangkut tentang Penyidikan adalah ketentuan tentang alat- alat bukti, ketentuan tentang terjadinya delik, pemeriksaan di tempat kejadian, pemanggilan tersangka atau terdakwa, penahan sementara, penggeledahan, pemeriksaan dan introgasi, berita acara, penyitaan, penyampingan perkara, pelimpahan perkara kepada penuntut umum dan pengembalian kepada penyidik untuk disempurnakan.

Pemeriksaan yang dilakukan oleh penyidik difokuskan sepanjang hal yang menyangkut persoalan hukum. Titik pangkal pemeriksaan dihadapan penyidik ialah tersangka. Dari dialah diperoleh keterangan mengenai peristiwa pidana yang sedang

[37] Andi Hamzah, *Op.Cit*, 2008, hlm. 119

[38] Bambang Tri Bawono, Tinjauan Yuridis Hak-Hak Tersangka dalam Pemeriksaan Pendahuluan, *Jurnal Hukum,* XXVI (2), Agustus 2011, hlm. 5555

diperiksa. Akan tetapi, ekalipun tersangka yang menjadi titik tolak pemeriksaan, terhadapnya harus diberlakukan asas akusatur atau biasa diartikan juga dengan menempatkan posisi tersangka sebagai orang yang tidak bersalah.

Tersangka harus ditempatkan pada kedudukan menusia yang memiliki harkat martabat. Dia harus dinilai sebagai subjek, bukan sebagai objek. Yang diperiksa bukan manusia tersangka. Perbuatan tindak pidana yang dilakukannyalah yang menjadi objek pemeriksaan. Pemeriksaan tersebut ditujukan ke arah kesalahan tindak pidana yang dilakukan oleh tersangka. Tersangka harus dianggap tak bersalah, sesuai dengan prinsip hukum "praduga tak bersalah" (*presumption of innocent*) sampai diperoleh putusan pengadilan yang telah berkekuatan hukum tetap.[39]

Pada pemeriksaan tindak pidana, tidak selamanya hanya tersangka saja yang harus diperiksa. Adakalanya diperlukan pemeriksaan saksi atau ahli. Demi untuk terang dan jelasnya peristiwa pidana yang disangkakan. Namun, kepada tersangka harus ditegakkan perlindungan harkat martabat dan hak-hak asasi, kepada saksi dan ahli, harus juga diperlakukan dengan cara yang berperikemanusiaan dan beradab. Penyidik Polri tidak secara serta-merta dapat melakukan kegiatan penyidikan dengan semaunya, melainkan ada juga batasan-batasan yang harus diikuti oleh penyidik tersebut agar tidak melanggar hak asasi manusia mengingat kekuasaan penyidik dalam melakukan rangkaian tindakan tersebut terlampau besar.

[39] M Yahya Harahap, *Op.Cit.* 2009, hlm. 134

Batasan-batasan kegiatan penyidik tersebut telah diatur dalam ketentuan Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 8 Tahun 2009 tentang Implementasi Prinsip dan Standar Hak Asasi Manusia Dalam Penyelenggaraan Tugas Kepolisan Republik Indonesia. Di dalam Pasal 13 ayat (1) Peraturan tersebut disebutkan, dalam melaksanakan kegiatan penyidikan, setiap petugas POLRI dilarang:

a. Melakukan intimidasi, ancaman, siksaan fisik, psikis ataupun seksual untuk mendapatkan informasi, keterangan atau pengakuan;
b. Menyuruh atau menghasut orang lain untuk melakukan tindakan kekerasan di luar proses hukum atau secara sewenang-wenang;
c. Memberitakan rahasia seseorang yang berperkara;
d. Memanipulasi atau berbohong dalam membuat atau menyampaikan laporan hasil penyelidikan;
e. Merekayasa laporan sehingga mengaburkan investigasi atau memutarbalikkan kebenaran;
f. Melakukan tindakan yang bertujuan untuk meminta imbalan dari pihak yang berperkara.[40]

Mengenai batasan-batasan tentang tindakan pemeriksaan yang dilakukan Penyidik dalam rangka proses penyidikan, juga terdapat batasan-batasan yang dituangkan di dalam peraturan a quo tersebut. Batasan-batasan juga tersebut terdapat

[40] Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 8 Tahun 2009 tentang Implementasi Prinsip Dan Standar Hak Asasi Manusia Dalam Penyelenggaraan Tugas Kepolisan Republik Indonesia

di dalam Pasal 27 Ayat (2), yang menyebutkan: Dalam melakukan pemeriksaan terhadap saksi, tersangka atau terperiksa, petugas dilarang:

a. Memeriksa saksi, tersangka atau terperiksa sebelum didampingi penasihat hukumnya, kecuali atas persetujuan yang diperiksa;
b. Menunda-nunda waktu pemeriksaan tanpa alasan yang sah, sehingga merugikan pihak terperiksa;
c. Tidak menanyakan keadaan kesehatan dan kesiapan yang diperiksa pada awal pemeriksaan;
d. Tidak menjelaskan status keperluan terperiksa dan tujuan pemeriksaan;
e. Mengajukan pertanyaan yang sulit dipahami terperiksa, atau dengan cara membentak-bentak, menakuti atau mengancam terperiksa;
f. Mengajukan pertanyaan-pertanyaan yang tidak relevan dengan tujuan pemeriksaan;
g. Melecehkan, merendahkan martabat dan/atau tidak menghargai hak terperiksa;
h. Melakukan kekerasan atau ancaman kekerasan yang bersifat fisik atau psikis dengan maksud untuk mendapatkan keterangan, informasi atau pengakuan;
i. Memaksa saksi, tersangka/terperiksa untuk memberikan informasi mengenai hal-hal yang berkaitan dengan rahasia jabatannya;
j. Membujuk, mempengaruhi atau memperdaya pihak yang diperiksa untuk melakukan tindakan atau tidak melakukan tindakan yang dapat merugikan hak-hak yang diperiksa;

k. Melakukan pemeriksaan pada malam hari tanpa didampingi oleh penasehat hukum dan tanpa alasan yang sah;
l. Tidak memberikan kesempatan kepada terperiksa untuk istirahat, melaksanakan ibadah, makan, dan keperluan pribadi lainnya tanpa alasan yang sah;
m. Memanipulasi hasil pemeriksaan dengan tidak mencatat sebagian keterangan atau mengubah keterangan yang diberikan terperiksa yang menyimpang dari tujuan pemeriksaan;
n. Menolak saksi atau tersangka untuk mengajukan saksi yang meringankan untuk diperiksa;
o. Menghalang-halangi penasehat hukum untuk memberi bantuan hukum kepada saksi/tersangka yang diperiksa;
p. Melakukan pemeriksaan ditempat yang melanggar ketentuan hukum;
q. Tidak membacakan kembali hasil pemeriksaan kepada yang diperiksa dengan bahasa yang dimengerti, sebelum pemeriksaan diakhiri; dan
r. Melalaikan kewajiban tanda tangan pemeriksa, terperiksa dan/atau orang yang menyelesaikan jalannya pemeriksaan.[41]

Dengan adanya prinsip Hak Asasi Manusia yang diakui sebagai hak dasar alami manusia. Maka penyidik dalam menjalankan proses penyidikan dapat bersikap secara manusiawi dan penyidik harus bertindak berdasarkan norma hukum, norma agama,

[41] *Ibid*

kesopanan, kesusilaan yang merupakan hak mendasar bagi setiap warga negara. Sehingga dapat tercapainya proses penyidikan yang berdasarkan Hak Asasi Manusia.

B. Tinjauan Umum Tindak Pidana

Istilah tindak pidana dalam KUHP, dikenal dengan istilah *strafbaarfeit* dan dalam kepustakaan tentang hukum pidana sering mempergunakan istilah delik, sedangkan pembuat undang-undang merumuskan suatu undang-undang mempergunakan istilah peristiwa pidana atau perbuatan pidana atau tindak pidana.[42]

Menurut Moeljatno, dimaksud perbuatan pidana adalah perbuatan yang dilarang oleh suatu aturan hukum, larangan mana disertai ancaman (sanksi) yang berupa pidana tertentu, bagi siapa yang melanggar larangan tersebut. Dapat juga dikatakan bahwa perbuatan pidana adalah perbuatan yang oleh suatu aturan hukum dilarang dan diancam pidana. Asal saja dari pada itu diingat bahwa larangan itu ditujukan kepada perbuatan (yaitu keadaan atau kejadian yang ditimbulkan oleh kelakuan orang) sedangkan ancaman pidananya ditujukan kepada orang yang menimbulkan kejadian itu.[43]

Selanjutnya tindak pidana merupakan suatu istilah yang mengandung suatu pengertian dasar dalam ilmu hukum, sebagai istilah yang dibentuk dengan kesadaran dalam memberikan ciri tertentu pada peristiwa hukum pidana.Tindak pidana mempunyai pengertian yang abstrak dari peristiwa-peristiwa yang kongkrit dalam

[42] Andi Hamzah, *Op.Cit*, 2008, hlm. 72
[43] Moeljanto, *Asas-Asas Hukum Pidana*, Bina Aksara, Jakarta, 1984, hlm 5

lapangan hukum pidana, sehingga tindak pidana haruslah diberikan arti yang bersifat ilmiah dan ditentukan dengan jelas untuk dapat memisahkan dengan istilah yang dipakai sehari-hari dalam kehidupan masyarakat.

Hukum Pidana Belanda menggunakan istilah *strafbaarfeit*. Hukum Pidana negara Anglo Saxon memakai istilah *Offense atauacriminal act* untuk maksud yang sama. Oleh karena KUHP Indonesia bersumber pada WvS Belanda, maka istilah aslinya pun sama yaitu strafbaarfeit. Istilah *Strafbaarfeit* terdiri dari tiga unsur yakni *straf, baar*, dan *feit*. *Straf* berarti hukuman (pidana), baar berarti dapat (boleh), serta feit yang berarti peristiwa (perbuatan). Tindak Pidana berarti suatu perbuatan yang pelakunya dapat dikenai hukuman pidana.[44]

Tindak pidana merupakan salah satu istilah untuk menggambarkan suatu perbuatan yang dapat dipidana, dalam Bahasa belanda disebut sebagai *straftbaarfeit*. Istilah lain yang pernah digunakan untuk menggambarkan perbuatan yang dapat dipidana adalah:

1. Peristiwa pidana;
2. Perbuatan pidana;
3. Pelanggaran pidana;
4. Perbuatan yang dapat dihukum.[45]

[44] Wirjono Prodjodikoro, *Asas-asas Hukum Pidana di Indonesia*, Refika Aditama, Bandung, 2009, hlm. 59.

[45] Masruchin Rubai, *Asas-Asas Hukum Pidana*, UM press dan FH UB, Malang, 2001, hlm 21.

Tindak pidana merupakan pengertian dasar dalam hukum pidana. Tindak pidana merupakan suatu pengertian yuridis, lain halnya dengan istilah perbuatan jahat atau kejahatan. Secara yuridis formal, tindak kejahatan merupakan bentuk tingkah laku yang melanggar undang-undang pidana. Oleh sebab itu setiap perbuatan yang dilarang oleh undang-undang harus dihindari dan barang siapa melanggarnya maka akan dikenakan pidana. Jadi larangan-larangan dan kewajibankewajiban tertentu yang harus ditaati oleh setiap warga Negara wajib dicantumkan dalam undang-undang maupun peraturan-peraturan pemerintah, baik di tingkat pusat maupun daerah.[46]

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

1) *Straf* diartikan sebagai pidana dan hukum;
2) *Baar* diartikan sebagai dapat dan boleh;
3) *Feit* diartikan sebagai tindak, peristiwa, pelnggaran dan perbuatan.

Biasanya tindak pidana disinonimkan dengan delik, yang berasal dari bahasa Latin, yakni *delictum*. Dalam bahasa Jerman disebut *delict*, dan dalam bahasa Belanda disebut *delict*. Dalam Kamus Besar Bahasa Indonesia menggunakan istilah delik yaitu perbuatan yang dapat dikenakan hukuman karena merupakan pelanggaran terhadap tindak pidana.[47]

Adapun istilah yang digunakan oleh para ahli yaitu:

[46] P.A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, PT. Citra Adityta Bakti, Bandung, 1996, hlm. 7

[47] Teguh Prasetyo, *Hukum Pidana*, Rajawali Pers, Jakarta, 2011, hlm 47

Vos menggunakan istilah *strafbaarfeit* yaitu suatu kelakuan manusia yang diancam pidana oleh peraturan undang-undang, jadi suatu kelakuan yang pada umumnya dilarang dengan ancaman pidana.[48] Menurut Simons, *strafbaarfeit* atau tindak pidana adalah kelakuan yang diancam dengan pidana yang bersifat melawan hukum yang berhubungan dengan kesalahan orang yang mampu bertanggung jawab.[49] Selanjutnya menurut Bambang Poernomo, tindak pidana adalah suatu perbuatan yang oleh suatu aturan hukum pidana dilarang dan diancam dengan pidana bagi siapa yang melanggar larangan tersebut.[50]

Pompe membedakan pengertian *strafbaarfeit* yaitu:

a. Definisi menurut teori, memberikan pengertian *strafbaarfeit* adalah suatu pelanggaran terhadap norma, yang dilakukan karena kesalahan si pelanggar dan diancam dengan pidana untuk mempertahankan tata hukum dan menyelamatkan kesejahteraan umum;
b. definisi hukum positif, merumuskan pengertian *strafbaarfeit* adalah suatu kejadian (*feit*) yang oleh peraturan undang-undang dirumuskan sebagai perbuatan yang dapat dihukum.

Sedangkan menurut S.R. Sianturi, pengertian tindak pidana adalah suatu tindakan pada tempat, waktu dan keadaan tertentu yang dilarang atau diharuskan dan diancam dengan pidana oleh undang-undang, bersifat melawan hukum serta dengan

---

[48] Bambang Poernomo, *Op.Cit*,1996, hlm. 91

[49] M. Nurul Irfan, *Korupsi Dalam Hukum Pidana Islam*, Sinar Grafika Offset, Jakarta, 2011, hlm.23

[50] Bambang Poernomo, *Op.Cit*, 1996, hlm.130

kesalahan, dilakukan oleh seseorang yang mampu bertanggung jawab. Maka selanjutnya unsurunsur tindak pidananya adalah terdiri dari: subjek, kesalahan, bersifat melawan hukum, tindakan yang dilarang dan diancam dengan pidana oleh undang-undang serta waktu dan tempat serta keadaan tertentu.

Sedangkan Utrecht menggunakan istilah "peristiwa pidana" beliau menerjemahkan istilah feit secara harfiah menjadi "peristiwa". Namun Moeljatno menolak istilah peristiwa pidana karena katanya peristiwa itu adalah pengertian yang konkret yang hanya menunjuk Kepada suatu kejadian yang tertentu saja, misalnya matinya orang. Hukum Pidana tidak melarang matinya orang, tetapi melarang adanya orang mati karena perbuatan orang lain.

Van Hamel menyatakan bahwa *strafbaarfeit* adalah kelakuan orang yang dirumuskan dalam undang-undang, bersifat melawan hukum, patut dipidana dan dilakukan dengan kesalahan. Sedangkan Simons berpendapat mengenai delik dalam arti *strafbaarfeit* adalah suatu tindakan melanggar hukum yang dilakukan dengan sengaja ataupun tidak sengaja oleh seseorang yang tindakannya tersebut dapat dipertanggungjawabkan dan oleh undang-undang telah dinyatakan sebagai suatu perbuatanyang dapat dihukum. Jonkers dan Utrecht memandang rumusan Simons merupakan rumusan yang lengkap, yang meliputi:

a. Diancam dengan pidana oleh hukum;
b. Bertentangan dengan hukum;
c. Dilakukan oleh orang yang bersalah;
d. Orang itu dipandang bertanggungjawab atas perbuatannya.

Rumusan para ahli hukum tersebut merumuskan delik (*straafbaarfeit*) itu secara bulat, tidak memisahkan antara perbuatan dan akibatnya disatu pihak dan pertanggungjawabannya di lain pihak, A.Z. Abidin menyebut cara perumusan delik seperti ini sebagai aliran monistis tentang delik. Ahli hukum yang lain, memisahkan antara perbuatan dan akibatnya di satu pihak dan pertanggungjawaban di lain pihak sebagai aliran dualistis. Memang di Inggris dipisahkan antara perbuatan yang dilarang oleh Undang-Undang dan diancam pidana (*actus reus*) di satu pihak dan pertanggungjawaban (*mens rea*) dilain pihak.

Berdasakan rumusan yang ada maka delik (*strafbaarfeit*) memuat beberapa unsur yakni:

a. Suatu perbuatan manusia;
b. Perbuatan itu dilarang dan diancam dengan hukuman oleh undang-undang;
c. Perbuatan itu dilakukan oleh seseorang yang dapat dipertanggung jawaban.

Tindak pidana merupakan istilah yang mengandung suatu pengertian dasar dalam ilmu hukum, sebagai istilah yang dibentuk dengan kesadaran dalam memberikan ciri tertentu pada peristiwa hukum pidana, tindak pidana mempunyai pengertian yang abstrak dari peristiwa-peristiwa yang kongkrit dalam lapangan hukum pidana, sehingga tindak pidana haruslah diberikan arti yang bersifat ilmiah dan ditentukan dengan jelas untuk dapat memisahkan dengan istilah yang dipakai sehari-hari dalam kehidupan masyarakat.

Pengertian tindak pidana, banyak dikemukakan oleh para sarjana hukum, diantaranya:

a. S.R.Sianturi, perumusan tindak pidana sebagai berikut: Tindak Pidana adalah sebagai suatu tindakan pada tempat, waktu dan keadaan tertentu yang dilarang atau diharuskan dan diancam dengan pidana oleh undang-undang yang bersifat melawan hukum, serta dengan kesalahan yang dilakukan oleh seseorang (yang mampu bertanggungjawab).
b. R.Tresna, peristiwa pidana adalah: "Sesuatu perbuatan atau rangkaian perbuatan manusia, yang bertentangan dengan undang-undang atau peraturan-peraturan lainnya, terhadap perbuatan mana yang diadakan Tindakan penghukuman".[51]

Menurut Wirjono Prodjodikoro dalam buku Azas-azas Hukum pidana di Indonesia, memberikan suatu pengertian mengenai tindak pidana adalah Pelanggaran norma-norma dalam tiga bidang hukum lain, yaitu Hukum Perdata, Hukum Ketatanegaraan, dan Hukum Tata Usaha Pemerintah, yang oleh pembentuk undang-undang ditanggapi dengan suatu hukum pidana, maka sifat-sifat yang ada dalam suatu tindak pidana adalah sifat melanggar hukum, karena tidak ada suatu tindak pidana tanpa sifat melanggar hukum.

Tindak pidana juga diartikan sebagai suatu dasar yang pokok dalam menjatuhkan pidana orang yang telah melakukan perbuatan pidana atas dasar pertanggung jawaban sesorang atas perbuatan yang telah dilakukannya, tapi sebelum itu mengenai dilarang dan diancamannya suatu perbuatan yaitu mengenai perbuatan

[51] E.Y Kanter dan S.R Sianturi, *Asas-Asas Hukum Pidana di Indonesia dan Penerapannya*, AlumniAHM-PTHM, Jakarta, 1986, hlm. 208-209

pidananya sendiri, yaitu berdasarkan asas legalitas (*principle of legality*) asas yang menentukan bahwa tidak ada perbuatan yang dapat dilarang dan diancam dengan pidana jika tidak ditentukan terlebih dahulu dalam perundang-undangan. Tindak pidana merupakan bagian dasar dari pada suatu kesalahan yang dilakukan terhadap seseorang dalam melakukan suatu kejahatan.

Tindak pidana dapat dibedakan atas tindak pidana/delik *Comissionis*, delik *Ommissionem* dan delik *Comissionis* per *Ommissionem Commissa* antara lain:

a. Delik *Comissionis*

   Delik *Commissionis* adalah delik yang berupa pelanggaran terhadap larangan, yaitu berbuat sesuatu yang dilarang misalnya melakukan pencurian, penipuan, pembunuhan dan sebagainya.

b. Delik *Ommissionem*

   Delik *Omissionis* adalah delik yang berupa pelanggaran terhadap perintah, yaitu tidak berbuat sesuatu yang diperintah misalnya tidak menghadap sebagai saksi dimuka persidangan Pengadilan sebagaimana ditentukan dalam Pasal 522 KUHP.

c. Delik *Comissionis* per *Ommissionem Commissa*

   Pengertian dari delik ini tersebut adalah delik yang berupa pelanggaran terhadap larangan, akan tetapi dapat dilakukan dengan cara tidak berbuat, misalnya: seorang ibu yang membunuh bayinya dengan tidak menyusui (Pasal 338 dan 340 KUHP).

Terkait dengan masalah pengertian tindak pidana, Moeljatno mengemukaka tiga hal yang perlu diperhatikan, yaitu:

a. Perbuatan pidana adalah perbuatan oleh suatu aturan hukum dilarang dan diacam pidana;
b. Larangan ditujukan kepada perbuatan yaitu suatu keadaan atau kejadian yang ditimbulkan oleh perbuatan orang, sedangkan ancaman pidana ditujukan kepada orang yang menimbulkan kejadian itu;
c. Antara larangan dan ancaman pidana ada hubungan yang erat, kejadian tidak dapat dilarang jika yang menimbulkan bukan orang, dan orang tidak dapat diancam dengan pidana jika tidak karena kejadian yang ditimbulkannya.[52]

Menurut Roeslan Saleh, dipidana atau tidaknya seseorang yang melakukan perbuatan tergantung apakah pada saat melakukan perbuatan ada kesalahan atau tidak, apakah seseorang yang melakukan perbuatan pidana itu memang punya kesalahan maka tentu ia dapat dikenakan sanksi pidana, akan tetapi bila ia telah melakukan perbuatan pidana yang terlarang dan tercela tetapi tidak mempunyai kesalahan ia tentu tidak dipidana.[53]

C. Tinjauan Umum Cybercrime

[52] Moeljatno, *Fungsi dan Tujuan Hukum Pidana Indonesia*, Bina Aksara, Jakarta, 1985, hlm. 34

[53] Roeslan Saleh, *Perbuatan Pidana dan Pertanggungjawaban Pidana dan Pengertian Dasar dalam Hukum Pidana*, Aksara Baru, Jakarta, 1983, hlm 75

Cybercrime atau kejahatan berbasis komputer, adalah kejahatan yang melibatkan komputer dan jaringan (*network*).[54] Komputer mungkin telah digunakan dalam pelaksanaan kejahatan, atau mungkin itu sasarannya.[55] *Cybercrimes* dapat didefinisikan sebagai: "Pelanggaran yang dilakukan terhadap perorangan atau sekelompok individu dengan motif kriminal untuk secara sengaja menyakiti reputasi korban atau menyebabkan kerugian fisik atau mental atau kerugian kepada korban baik secara langsung maupun tidak langsung, menggunakan jaringan telekomunikasi modern seperti Internet (jaringan termasuk namun tidak terbatas pada ruang Chat, email, notice boards dan kelompok) dan telepon genggam.[56] *Cybercrime* dapat mengancam seseorang, keamanan negara atau kesehatan finansial.[57]

Isu seputar jenis kejahatan ini telah menjadi sangat populer, terutama seputar hacking, pelanggaran hak cipta, penyadapan yang tidak beralasan dan pornografi. Ada pula masalah privasi pada saat informasi rahasia dicegat atau diungkapkan, secara sah atau tidak. Debarati Halder dan K. Jaishankar lebih jauh mendefinisikan *cybercrime* dari perspektif gender dan mendefinisikan "*cybercrime against women*" sebagai "Kejahatan yang ditargetkan pada wanita dengan motif untuk secara sengaja menyakiti korban secara psikologis dan fisik, menggunakan jaringan telekomunikasi modern

[54] R. Moore, *Cyber Crime: Investigating High-Technology Computer Crime*, Cleveland, Mississippi: Anderson Publishing, 2005

[55] Warren G. Kruse, Jay G. Heiser. *Computer Forensics: Incident Response Essentials*. Addison-Wesley. 2002, hlm 392

[56] Debarati Halder & K. Jaishankar, *Cybercrime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, Pennsylvania USA: IGI, 2011

[57] Steve Morgan, Cyber Crime Costs Projected To Reach $2 Trillion by 2019. *Forbes*. Retrieved September 22, 2016

seperti internet dan telepon genggam". Secara sengaja, baik pemerintah dan swasta terlibat dalam *cybercrimes*, termasuk spionase, pencurian keuangan dan kejahatan lintas batas (*cross-border*) lainnya. Kegiatan yang melintasi batas negara dan melibatkan kepentingan setidaknya satu negara ter-kadang disebut sebagai *cyberwarfare*.

Istilah *cybercrime* saat ini merujuk pada suatu aktivitas kejahatan yang berhubungan dengan dunia maya (*cyberspace*) dan komputer yang berbasis pada kecanggihan perkembangan teknologi internet sebagai media utama untuk melangsungkan kejahatan.[58] Perlu kita ketahui pelaku cybercrime adalah mereka yang memiliki keahlian tinggi dalam ilmu computer, pelaku cybercrime umumnya menguasai algoritma dan pemrograman computer unutk membuat script/kode malware, mereka dapat menganalisa cara kerja system computer dan jaringan, dan mampu menemukan celah pasa system yang kemudian akan menggunakan kelemahan tersebut untuk dapat masuk sehingga tindakan kejahatan seperti pencurian data dapat berhasil dilakukan.

Sifat kejahatan di dunia maya yang non-violence, atau tidak menimbulkan kekacauan yang mudah terlihat. Jika kejahatan konvensional sering kali menimbulkan kekacauan maka kejahatan di internet bersifat sebaliknya. Oleh karena itu, ketakutan atas kejahatan tersebut tidak mudah timbul meskipun bias saja kerusakan yang diakibatkan oleh kejahatan cyber dapat lebih dahsyat dari pada kejahatan-kejahatan

[58] Dikdik, Elisatris, *Cyber Law Aspek Hukum Teknologi Informasi*, Bandung, Refika Aditama, 2009, hlm.8.

lain. Jika pelaku kejahatan konvensional mudah diidentifikasi dan memiliki tipe tertentu maka pelaku cybercrime bersifat lebih universal meski memiliki ciri khusus yaitu kejahatan dilakukan oleh orang-orang yang menguasai penggunaan internet beserta aplikasinya. Pelaku kejahatan tersebut tidak terbatas pada usia dan stereotip tertentu.[59]

Dalam hal ini, keunikan kejahatan ini adalah penggunaan teknologi informasi dalam modus operandi. Itulah sebabnya mengapa modus operandi dalam dunia cyber tersebut sulit dimengerti oleh orang-orang yang tidak menguasai pengetahuan tentang komputer, tekhnik pemrogramannya dan seluk beluk dunia cyber. Kerugian yang ditimbulkan dari kejahatan ini dapat bersifat material maupun non-material. Cybercrime berpotensi menimbulkan kerugian pada banyak bidang seperti politik, ekonomi, sosial budaya yang lebih besar dampaknya dibandingkan dengan kejahatan berintensitas tinggi lainnya.

Beberapa klasifikasi *cybercrime*, dalam beberapa literature dan praktiknya dikelompokan dalam beberapa bentuk, antara lain:

1) Penipuan dan kejahatan finansial

   Penipuan dengan menggunakan komputer adalah salah representasi fakta yang tidak jujur yang dimaksudkan untuk membiarkan orang lain melakukan sesuatu yang menyebabkan kerugian. Bentuk kecurangan dapat difasilitasi dengan menggunakan sistem komputer, termasuk penipuan bank,

[59] Sahat Maruli T. Situmeang, *Cyberlaw*. Penerbit Cakra: Bandung, Cet-1 , 2020, hlm 24-25

carding, pencurian identitas, pemerasan dan pencurian informasi rahasia. Berbagai penipuan internet banyak berbasis *phishing* dan *social engineering* yang menjadi sasaran biasanya konsumen dan pelaku bisnis.[60]

2) *Unauthorized Access*

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.[61]

3) *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 mengganggu ketertiban umum, contohnya adalah penyebaran pornografi.

4) Penyebaran virus secara sengaja,

Penyebaran virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang yang sistem emailnya terkena virus tida menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.

5) *Data Forgery*

[60] Alcianno G. Gani, Cybercrime (Kejahatan Berbasis Computer), *JSI: Jurnal Sistem Informasi*, 5 (1) 2018, hlm 18

[61] Dikdik, Elisatris, *Op.Cit*, 2009, hlm 9

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.

6) *Cyber Espionage*, *Sabotage*, and *Extortion*, *Cyber Espionage*

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. *Sabotage and Extortion* merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

7) *Cyberwarfare*

Departemen Pertahanan Amerika Serikat (*Department of Defense* / DoD) mencatat bahwa dunia maya telah menjadi perhatian tingkat nasional melalui beberapa peristiwa terkini mengenai signifikansi geo-strategis. Di antaranya termasuk serangan terhadap infrastruktur Estonia di tahun 2007, yang diduga oleh hacker Rusia. "Pada bulan Agustus 2008, Rusia kembali melakukan serangan *cyber*, kali ini dalam kampanye kinetik dan non kinetik yang terkoordinasi dan disinkronkan melawan negara Georgia. Khawatir bahwa serangan semacam itu dapat menjadi norma perang antar negara di masa depan,

dampak dari konsep operasi dunia maya akan disesuaikan oleh para komandan militer di masa depan.[62]

8) *Cyberextortion*

Cyberextortion terjadi saat sebuah situs web, server e-mail atau sistem komputer dikenai atau diancam dengan penolakan berulang (*Denial of Service* / DoS) terhadap layanan atau serangan lainnya oleh hacker jahat. Para hacker ini menuntut uang sebagai imbalan dengan janji akan menghentikan serangannya dan atau menawarkan "perlindungan". Menurut Biro Investigasi Federal, saat ini semakin banyak serangan yang dilakukan para pelaku *cyberextortion* pada situs web perusahaan dan jaringan, melumpuhkan kemampuan / kinerja mereka untuk beroperasi dan menuntut pembayaran untuk memulihkan layanan mereka.[63]

9) Pelecehan

Dalam konten ini mungkin menyinggung dengan cara yang tidak spesifik, pelecehan mengarahkan kata-kata kotor, penghinaan atau komentar pada individu tertentu yang memusatkan perhatian pada jenis kelamin, ras, agama, kebangsaan atau orientasi seksual, atau biasa di sebut mengandung unsur SARA. Hal ini sering terjadi di *chat room*, melalui *newsgroup* dan

[62] Alcianno G. Gani, *Op.Cit*, 5 (1) 2018, hlm 20
[63] *Ibid*, hlm 19

dengan mengirim email kebencian ke pihak yang berkepentingan. Pelecehan di internet juga termasuk balas dendam.[64]

10) *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.

11) Perdagangan narkoba

Pasar gelap digunakan untuk membeli dan menjual obat-obatan terlarang secara online. Beberapa pedagang narkoba menggunakan alat pesan terenkripsi untuk berkomunikasi dengan pemasok narkoba. Situs web gelap *Silk Road* adalah pasar online utama untuk obat-obatan sebelum dimatikan oleh penegak hukum (kemudian dibuka kembali di bawah manajemen baru, dan kemudian ditutup oleh penegak hukum lagi). Setelah *Silk Road 2.0* turun, *Silk Road 3 Reloaded* muncul. Namun sebenarnya itu hanya pasar yang lebih lama yang bernama *Diabolus Market*, yang menggunakan nama tersebut untuk lebih banyak menarik keuntungan dari kesuksesan merek sebelumnya.[65]

12) *Hacking* dan *Cracker*

[64] *Ibid*, hlm 21
[65] *Ibid*, hlm 22

Istilah *hacker* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut *cracker*. Boleh dibilang *cracker* ini sebenarnya adalah *hacker* yang 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.[66]

13) *Hijacking*

Hijacking merupakan kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah *Software Piracy* (pembajakan perangkat lunak).

14) *Cyberterrorism*

Seorang *cyberterrorist* adalah seseorang yang mengintimidasi atau menggalang pemerintah atau organisasi untuk memajukan tujuan politik atau sosialnya dengan meluncurkan serangan berbasis komputer terhadap komputer, jaringan atau informasi yang tersimpan di dalamnya. *Cyberterrorism* secara

[66] Sahat Maruli T. Situmeang, *Op.Cit* , 2020, hlm 27

umum dapat didefinisikan sebagai tindakan terorisme yang dilakukan melalui penggunaan dunia maya atau sumber daya komputer. Suatu tindakan *cybercrime* termasuk *cyberterorism* jika mengancam pemerintah atau warga negara, termasuk *cracking* ke situs pemerintah atau militer.[67] Sebagai contoh, sebuah propaganda sederhana di Internet akan terjadi serangan bom saat liburan tahun baru bisa dianggap sebagai *cyberterrorism*. Ada juga kegiatan hacking yang diarahkan pada individu atau keluarga yang diselenggarakan oleh kelompok-kelompok di dalam jaringan, cenderung menimbulkan ketakutan di kalangan orang-orang, mengumpulkan informasi yang relevan untuk menghancurkan kehidupan masyarakat, perampokan, pemerasan, dll.[68]

D. Tinjauan Umum Digital Forensik

Digital berasal dari kata *Digitus*, dalam bahasa Yunani berarti jari jemari. Apabila kita hitung jari jemari orang dewasa, maka berjumlah sepuluh (10). Nilai sepuluh tersebut terdiri dari 2 radix, yaitu 1 dan 0, oleh karena itu Digital merupakan penggambaran dari suatu keadaan bilangan yang terdiri dari angka 0 dan 1 atau *off* dan *on* (bilangan biner). Forensik (berasal dari bahasa Latin *forensis* yang berarti "dari luar", dan serumpun dengan kata forum yang berarti "tempat umum") adalah bidang

[67] *Ibid*, hlm 28
[68] Alcianno G. Gani, *Op.Cit*, 5 (1) 2018, hlm 19

ilmu pengetahuan yang digunakan untuk membantu proses penegakan keadilan melalui proses penerapan ilmu atau sains.[69]

Sulianta mengatakan forensik memilki arti "membawa ke pengadilan". Istilah Forensik adalah suatu proses ilmiah dari ilmu pengetahuan dalam mengumpulkan, menganalisa, dan menghadirkan bukti-bukti dalam persidangan terkait adanya suatu kasus hukum.[70] Dalam proses penanganan tindak pidana kejahatan yang didalamnya menggunakan teknologi informasi tentunya akan membutuhkan proses investigasi forensik. Forensik merupakan suatu kegiatan kajian ilmiah yang dilakukan oleh ahli sesuai dengan kompetensinya bertujuan untuk melakukan identifikasi dan menentukan fakta-fakta yang berhubungan dengan perkara pidana dan bukti-bukti penunjang terjadinya perkara pidana dimaksud.

Analisis forensik merupakan suatu upaya penyidik dalam kewenangannya untuk memintakannya kepada ahli forensik melakukan kajian ilmiah sebagai salah satu langkah penting guna membuat terang suatu perkara pidana dalam kejahatan komputer menggunakan ilmu digital forensik yang dimiliki oleh ahli forensik tersebut. Salah satu bagian dari ilmu forensik adalah forensik digital yang cakupannya adalah penemuan atas hasil investigasi data yang telah ditemukan dalam perangkat digital seperti komputer, handphone dan lainnya. Berbeda dari forensik pada umumnya, digital forensik atau komputer forensik adalah kegiatan ilmiah dalam melakukan

[69] Imam Riadi & Bashor Fauzan Muthohirin, *Forensik Email*, Diandra Kreatif; Yogyakarta, Cetakan 2, 2022, hlm 2

[70] Sulianta Feri. *Komputer Forensik*. Jakarta: Elex Media Komputindo, 2008.

pengumpulan serta analisa data dari berbagai sumber daya komputer atau perangkat digital lainnya yang mencakup pada sistem komputer, jaringan komputer, jalur komunikasi dalam bentuk fisik maupun non fisik, serta berbagai media penyimpanan data yang dianggap layak untuk diajukan dalam persidangan sebagai alat bukti penunjang proses penyelesaian perkara pidana. Hal tersebut memperlihatan dua bidang keilmuan yakni ilmu komputer serta ilmu hukum disatukan dalam penerapannya oleh bidang ilmu digital forensik.[71]

Digital forensik adalah penggunaan ilmu dan metode untuk menemukan, mengumpulkan, mengamankan, menganalisis, menginterpretasi dan mempresentasikan barang bukti digital yang terkait dengan kasus yang terjadi untuk kepentingan rekonstruksi kejadian serta keabsahan proses peradilan.[72] Digital forensik adalah proses mengidentifikasi, memelihara, menganalisis, dan menyajikan bukti digital dengan cara yang dapat diterima secara hukum dan dalam proses hukum apa pun (yaitu, pengadilan hukum).

Menurut Altheide & Carvey[73] digital forensik merupakan penggunaan metode yang telah terbukti memperoleh pemeliharaan, pengumpulan, validasi, analisis identifikasi, interpretasi, dokumentasi, dan penyajian bukti digital yang berasal dari sumber digital untuk tujuan memfasilitasi atau melanjutkan rekonstruksi peristiwa

---

[71]

[72] Ankit Agarwal, et.all., Systematic Digital Forensic Investigation Model, *International Journal of Computer Science and Security (IJCSS)*, 5 (1) 2011, hlm 118-131

[73] Cory Altheide & Harlan Carvey, *Digital Forensics with Open Source Tools*, Syngress, 1st Edition, 2011

yang ditemukan sebagai tindak kriminal, atau membantu mengantisipasi tindakan operasi yang terencana. Forensik digital diasosiasikan dalam banyak pikiran orang terutama dengan penyelidikan kesalahan. Namun, itu juga telah muncul dalam beberapa tahun terakhir sebagai sumber alat dan pendekatan yang menjanjikan untuk memfasilitasi pelestarian dan kurasi digital, khususnya untuk melindungi dan menyelidiki bukti kejahatan yang telah terjadi.

Digital forensik merupakan salah satu sarana untuk membantu penyidik dalam kewenangannya melakukan penyelidikan dan penyidikan yang diatur dalam UU ITE serta Kitab Undang-undang Hukum Acara Pidana (KUHAP). Untuk dapat melakukan penerapan ilmu digital forensik dalam proses penyidikan perlu pemahaman yang lebih dalam mengenai ilmu teknologi selain daripada ilmu hukum yang biasa diterapkan dalam proses pengadilan pidana. Penerapan ilmu digital forensik dibagi menjadi 4 (empat) yaitu:

1) Forensik Komputer yaitu penyidikan yang dilakukan terkait dengan data dan/atau aplikasi yang berada pada komputer tersebut yang didalamnya tercatat dalam berbagai berkas log;
2) Forensik Jaringan/Internet yaitu penyidikan yang dilakukan kepada data yang diperoleh berdasarkan pengamatan di jaringan;
3) Forensik Aplikasi yaitu penyidikan yang dilakukan dengan penggunaan aplikasi tertentu. Aplikasi tersebut memiliki fungsi audit karena aplikasi tersebut terdapat fitur untuk meninggalkan jejak suatu perangkat;

4) Forensik Perangkat yaitu penyidikan dengan tujuan untuk mendapatkan serta mengumpulkan data dan jejak kegiatan- kegiatan tertentu dalam suatu perangkat digital.[74]

Untuk terciptanya penerapan ilmu digital forensik yang komprehensif diperlukan 3 (tiga) komponen terangkai yang harus dipenuhi untuk penerapa ilmu yang berkualitas. Ketiga komponen tersebut yaitu:

1) Manusia (*People*), faktor kualitas manusia yang berpengaruh dalam proses penerapan ilmu digital forensik. Kualitas yang dibutuhkan tidak hanya mampu menggunakan computer namun diperlukan keahlian ilmu pengetahuan khusus dan pengalaman untuk dapat melakukan proses analisa menggunakan ilmu digital forensik;
2) Peralatan (*Equipment*), perlunya beberapa perangkat/alat untuk menunjang proses identifikasi menggunakan digital forensik untuk mendapatkan petunjuk guna menerangkan suatu perkara;
3) Aturan (*Protocol*), dalam komponen aturan diperlukan pemahaman secara mendalam dari sisi ilmu hukum dan pengetahuan lain seperti pengetahuan teknologi informasi untuk menunjang penerapan ilmu dapat menjadi berkualitas dan dengan aturan pula dibutuhkan untuk proses menggali,

[74] Budi Raharjo. *Op.Cit,* 12 (29) 2013, hlm 384

mendapatkan, menganalisis, dan akhirnya menyajikan dalam bentuk laporan yang akurat.[75]

E. Pembuktian Pidana dalam Perspektif Hukum Islam

Pembuktian menurut istilah Bahasa Arab berasal dari kata "*bayyinah*" yang artinya suatu yang menjelaskan. Ibnul Qayyim al- Jauziyah dalam kitabnya *al-Thuruq* al-Hukmiyah mengartikan "*bayyinah*" sebagai segala sesuatu atau apa saja yang dapat mengungkapkan dan menjelaskan kebenaran sesuatu.[76] Pembuktian secara etimologi berasal dari "bukti" yang berarti sesuatu peristiwa. Sedangkan secara terminologis, pembuktian berarti usaha menunjukkan benar atau salahnya seseorang terdakwa dalam sidang pengadilan.[77]

Menurut Subhi Mahmasani, yang dimaksud dengan membuktikan adalah mengajukan alasan dan memberikan dalil sampai pada batas yang meyakinkan. Yang dimaksud meyakinkan adalah apa yang menjadi ketetapan atau keputusan atas dasar penelitian dalil-dalil itu.[78]

Para ulama berbeda pendapat mengenai jenis-jenis alat bukti yang dapat digunakan dalam tindak pidana. Pertama, menurut jumhur ulama, untuk pembuktian

---

[75] Ruci, Meiyanti, and Ismaniah. Perkembangan Digital Forensik. *Jurnal Kajian Ilmiah UBJ*, 15 (2) September 2015, hlm 3

[76] Ibnul Qayyim al-Jauziyah, *al-Thuruq al-Hukmiyah*, Beirut: Dar al-Ma'rifah, 1408 H/ 1988 M, hlm 112.

[77] Sulaikin Lubis, dkk, *Hukum Acara Perdata Peradilan Agama*, Jakarta: Kencana, 2006, hlm 135.

[78] Subhi Mahmasoni, *Falsafah al-Tasyri' Fi al-Islam*, Beirut: al-Kasysyaf, 1419 H/ 1949 M, hlm 220.

jarimah qishash dan *diyat* dapat digunakan tiga cara (alat) pembuktian, yaitu; pengakuan, persaksian, dan *al-qasamah* (sumpah). Kedua, menurut sebagian *fuqaha'* seperti *Ibnul Qayyim* dari mazab Hanbali, untuk pembuktian *qishash* dan *diyat* digunakan empat cara pembuktian, yaitu; pengakuan, persaksian*, al-qasamah*, dan *qarinah* (indikasi).[79]

Ketiga alat bukti tersebut (pengakuan, persaksian, *al- qasamah*, dan *qarinah*) merupakan alat bukti yang banyak digunakan dalam *jarimah-jarimah hudud*. Perbedaan pendapat antara para ulama hanya terdapat dalam alat bukti qarinah, meskipun alat bukti yang paling kuat sebenarnya hanya ada dua, yaitu pengakuan dan persaksian. *Qasamah* sendiri juga termasuk alat bukti yang di perselisihkan, walaupun ulama-ulama dan kalangan mazab empat telah menyepakati.[80]

Pembuktian merupakan hal yang sangat penting dalam suatu kasus atau perkara, karena pembuktian bertujuan untuk mendapatkan kebenaran suatu peristiwa atau kasus yang diajukan kepada hakim. Islam sangat berhati-hati dalam menentukan apakah seseorang tersebut benar-benar telah melakukan perbuatan yang melanggar.

Beban untuk membuktikan kebenaran dakwaan atau gugatan dalam hukum acara Islam, diletakkan diatas pundak pendakwa atau penguggat, diantara kaidah kulli (umum), bukti itu adalah untuk menetapkan sesuatu yang berlawanan dengan lahir,sedangkan sumpah dilakukan untuk mempertahankan hukum asal (kenyataan).

[79] Abdul Qadir 'Audah, *al-Tasyri' al-Jinaiy al-Islami*, Beirut: Dar al-Kitab al-Arabi, juz 2, 1408 H/ 1988 M, hlm 303

[80] Ahmad Wardi Muslich, *Hukum Pidana Islam*, Jakarta: Sinar Grafika, 2005. hlm. 227.

Rasulullah Saw menjelaskan masalah pembebanan pembuktian yang populer dalam perspektif hukumIslam adalah: ”Pembuktian dibebankan pada penggugat dan sumpah kepada tergugat”. Pembuktian dibebankan pada penguggat (*affirmanti incoumbil probato*), bahwa mendapatkan hukum yang sesuai *petitum* gugatannya, seorang penggugat harus mengemukakan bukti-bukti yang membenarkan dalil-dalil gugatannya.

Kesaksian dalam Islam dikenal dengan istilah al-syahadah menurut bahasa memiliki arti sebagai berikut; (1) pernyataan atau pemberian yang pasti. (2) Ucapan yang keluar dari pengetahuan yang diperoleh dengan penyaksian langsung. (3) Mengetahui sesuatu secara pasti, mengalami, dan melihatnya. Menurut syara’ kesaksian adalah pemberitahuan yang pasti yaitu; ucapan yang keluar dan diperolehdari pengetahuan yang diperoleh dengan penyaksian langsung.

Kesaksian dapat diterima sebagai alat bukti apabila memenuhi syarat sebagai berikut; (1) Kesaksian dilakukan didalam sidang pengadilan, jika dilakukan diluar sidang pengadilan, meski itu dihadapan hakim ,tidak dianggap sebagai kesakasian. (2]) Kesaksian diucapkan dengan lafadz kesaksian, seperti saya bersaksi. (3) Jumlah dan syarat orang yang menjadi saksi sesuai dengan syarat dan ketentuan *syari’at*.

Saksi merupakan alat bukti untuk *jarimah qadzaf*, syarat-syarat saksi dalam jarimah ini sama dengan jarimah zina, yaitu; baligh, dapat dipercaya- adil, dan tidak ada penghalang menjadi saksi. Antara *bayyinah* (alat bukti) dan *syadanah* (kesaksian) seolah-olah para ulama menyamakannya. *Ibnul Qayyim* memaknakan bayyinah dengan dengan segala yang dapat menjelaskan perkara. Sedangkan syahadah adalah

mengemukakan keterangan untuk menetapkan hak atas diri orang lain. Dengan kesaksian yang cukup syarat, nyatalah kebenaran bagi hakim dan wajiblah dia memutuskan perkara sesuai dengan kesaksian itu.[81]

Wahbah al-Zuhaili mengemukakan pengertian persaksian adalah suatu pemberitahuan (pernyataan) yang benar untuk membuktikan suatu kebenaran deengan lafadz-lafadz syahadat di depan pengadilan. Sedang menurut syara' kesaksian adalah pemberitaan yang pasti yaitu ucapan yang keluar yang diperoleh dengan penyaksian langsung atau dari pengetahuan yang diperoleh dari orang lain karena beritanya telah tersebar. Memberi kesaksian asal hukumnya fardhu kifayah, artinya jika 2 orang telah memberikan kesaksian maka semua orang telah gugur kewajibannya, dan jika semua orang menolak tidak ada yang mau menjadi saksi maka berdosa semuanya, kerena maksud kesaksian itu adalah untuk memelihara hak. Pengakuan saksi sebagai alat pembuktian untuk suatu *jarimah* merupakan cara yang lazim dan umum. Karena persaksian perupakan cara pembuktian yang sangat penting dalam mengungkap suatu *jarimah*.

[81] Ibnul Qayyim al-Jauziyah, *Op.Cit*, 1408 H/ 1988 M, hlm 114.

BAB III

HASIL PENELITIAN DAN PEMBAHASAN

A. Bentuk Politik Hukum dalam Mengkualifikasikan Cybercrime dalam Norma Hukum Pidana

Soerjono Soekanto dalam tulisannya yang berjudul Ilmu Politik dan hukum berpendapat bahwa Hukum dan politik mempunyai hubungan timbal balik. Ketika hukum berada pada tingkatan tertinggi diatas politik. Hal ini menyebabkan hukum positif mencakup semua standar yang menyebabkan kesepakatan dalam masyarakat tercapai dengan suatu proses konstitusional.[82] Soerjono Soekanto juga mengatakan bahwa dalam menafsirkan hukum, penguasa memisahkan dirinya dan perjuangan untuk menemukan kekuasaan dan tidak dikotori oleh pengaruh politik. Sebaliknya, pelaku-pelaku politik dapat menerima otonomi dan institusi-institusi hukum ketika pelaku-pelaku politik tersebut meyakini bahwa peraturan-peraturan yang harus ditaati didasarkan pada kebijaksanaan yang juga mereka anut sejak zaman dahulu. Pendapat lain mengatakan, hukum sangat dipengaruhi oleh politik, karena hukum sendiri adalah bentuk dari keputusan-keputusan politik yang dibuat oleh penguasa.[83]

[82] Soerjono Soekanto, Ilmu Politik & Hukum, *Jurnal Hukum & Pembangunan*, 18, (3) 2017, hlm 1.

[83] *Ibid*

Hukum bekerja dalam sebuah situasi politik tertentu ditandai dengan adanya relasi antara hukum dan politik hukum itu sendiri, artinya hukum adalah suatu perwujudan dari nilai-nilai yang berkembang, nilainilai berkembang tersebut adalah nilai tentang keadilan. Sehingga idealnya hukum dibuat dengan mempertimbangkan kepentingan yang dapat mewujudkan nilai-nilai keadilan tersebut. Yang mana peraturan-peraturan hukum memiliki ciri-ciri yaitu mengandung perintah dan larangan, menuntut kepatuhan dan adanya sanksi, maka hukum yang berjalan akan menciptakan ketertiban dan keadilan di masyarakat.[84]

Secara etimologis politik hukum adalah interpretasi bahasa Indonesia dari istilah hukum Belanda *rechtspolitiek*, yang merupakan susunan kata *Recht* (pengaturan) dan *Politiek* (kebijakan). Menurut Kamus Besar Bahasa Indonesia (KBBI) kebijakan adalah rangkaian gagasan dan aturan yang menjadi landasan rencana dalam melakukan suatu tugas, prakarsa, dan pendekatan dalam bertindak logis dalam bertindak.[85]

Jadi secara singkat politik hukum berarti merupakan kebijakan hukum. Setelah membaca buku dari Prof. Mahfud MD yang berjudul Politik Hukum di Indoensia diketahui bahwa Politik hukum adalah *legal policy* atau sesuatu garis kebijakan resmi tentang hukum yang akan diberlakukan pada hukum baru ataupun akan adanya suatu penggantian hukum pada hukum lama, tujuannya adalah untuk mencapai tujuan suatu

[84] Merdi Hajiji, Relasi Hukum Dan Politik Dalam Sistem Hukum Indonesia, *Jurnal Rechtsvinding Media Pembinaan Hukum Nasional*, 2 (3), 2013, hlm 362.

[85] Hikmahanto Juwana, Politik Hukum UU Bidang Ekonomi Di Indonesia, *Jurnal Hukum*, 01 (1) 2005

negara,[86] seperti diuraikan dalam bukunyanya tersebut, Prof. Mahfud MD memperjelas bahwa hukum tidak terlepas dari pengaruh politik saat perumusannya bahkan kedudukan politik lebih dominan didalamnya sehingga sulit menemukan bentuk hukum yang netral dari pengaruh politik. Lalu, sebuah politik hukum mempunyai peran sebagai aktivitas pemilihan sarana dalam mencapai suatu tujuan dalam suatu tatanan hukum maupun sosial tertentu di dalam suatu masyarakat hal ini merupakan pendapat dari menurut Satjipto Rahardjo.[87]

Prof. Mahfud MD berpendapat adanya kesatuan dan pengaturan perundang-undangan yang terdiri dari berbagai komponen yang saling ketergantungan satu sama lainnya dalam sistem hukum di Indonesia, yang dibangun untuk mencapai tujuan negara dan berpedoman pada dasar serta cita hukum nasional yang terkandung di dalam Undang-Undang Dasar NRI Tahun 1945.[88] Penjabaran lainnya tentang Politik hukum yakni Politik Hukum adalah alat atau sarana dan langkah yang dapat digunakan oleh pemerintah untuk menciptakan sistem hukum nasional yang dikehendaki dan dengan sistem hukum nasional itu akan diwujudkan cita-cita bangsa Indonesia.[89]

Secara kesimpulan bahwa politik hukum merupakan kebijakan dasar dalam penyelenggaraan negara terkhusus pada bidang hukum dalam konteks hukum positif sebagai hukum yang akan berjalan, yang sedang berjalan dan yang telah berlaku. Hal

[86] Moh. Mahfud MD, *Politik Hukum Di Indonesia*, Jakarta: Raja Grafindo Persada, 2009
[87] Satjipto Rahardjo, *Ilmu Hukum*, Bandung: Aditya Bakti, 1991
[88] Moh. Mahfud MD, *Membangun Politik Hukum Menegakkan Konstitusi*. Jakarta: Rajawali Press, 2012
[89] C.F.G. Sunaryati Hartono, *Politik Hukum Menuju Satu Sistem Hukum Nasional*, Bandung: Alumni, 1991

tersebut berasal dari nilai-nilai yang tumbuh dan hidup di masyarakat dengan tujuan untuk mencapai tujuan negara yang tercantum pada Pembukaan Undang-Undang Dasar Negara Kesatuan Republik Indonesia 1945 (UUD NRI 1945) pada alinea 4, yakni: (I) melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia; (2) memajukan kesejahteraan umum; (3) mencerdaskan kehidupan bangsa; dan (4) ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial. Lalu, peran politik hukum dalam pembentukan hukum dapat kita pahami antara hukum dan politik manakah diantara keduanya yang memiliki posisi lebih dominan, kekuasaan hukum atau kekuasaan politik? Untuk jawaban dari pertanyaan tersebut adalah bergantung pada persepsi dan sudut pandang masyarakat, ingin melihat dari berbagai sudut apakah itu yang kita maksudkan sebagai hukum, dan apa yang kita maksudkan dengan politik. Jika kita berpandangan nondogmatik, dan memandang hukum bukan sekedar peraturan yang dibuat oleh kekuasaan politik, maka tentu saja persoalan lebih lanjut tentang hubungan kekuasaan hukum dan kekuasaan politik masih bisa berkepanjangan. Akan tetapi, saat kita menganut pandangan positif, pandangan ini akan memandang hukum hanya sebagai produk kekuasaan politik. *Law is a command of the Lawgiver*[90](hukum adalah perintah dari penguasa), dalam arti perintah dari mereka yang memiliki kekuasaan tertinggi atau yang memegang kedaulatan.

[90] Merdi Hajiji, *Op.Cit*, 2 (3), 2013

Seperti yang kita ketahui bahwa globalisasi menyebabkan suatu perubahan sosial, perubahan itu menyangkut perubahan yang terjadi di masyarakat, seperti perubahan nilai sosial, pola-pola perilaku, susunan organisasi, susunan lapisan-lapisan lembaga kemasyarakatan, kekuasaan dan wewenang serta interaksi sosial.[91] Perubahan sosial menurut Juliana Lumintang merupakan perubahan-perubahan pada lembaga kemasyarakatan di dalam suatu masyarakat, yang tentu saja akan mempengaruhi sistem sosialnya, yang di dalamnya terkandung suatu nilai-nilai, sikap-sikap dan pola-pola perikelakuan diantara berbagai macam kelompok masyarakat.

Perubahan Sosial pada masa ini merupakan perubahan sosial yang disebabkan perkembangan kemajuan teknologi yakni mordernisasi yang mengarah kepada kehidupan modern. Karena modernisasi yang disebabkan oleh globalisasi tidak dipungkiri akan terjadi juga perubahan dalam suatu bentuk tindak kejahatan. Misalnya, awal mula kejahatan hanya berbentuk penyerangan fisik, perampasan barang secara langsung. Seiring dengan perubahan sosial maka akan terjadi juga perkembangan cara berfikir masyarakat yang membentuk suatu pola pertumbuhan kejahatan, yakni biasa kita kenal dengan kejahatan siber (*cybercrime*).

Secara terminologi, *cybercrime* atau kejahatan berbasis komputer, adalah kejahatan yang melibatkan komputer dan jaringan (*network*).[92] Komputer mungkin telah digunakan dalam pelaksanaan kejahatan, atau mungkin itu sasarannya.[93]

---

[91] Juliana Lumintang, Pengaruh Perubahan Sosial Terhadap Kemajuan Pembangunan Masyrakat di Desa Tara-Tara I, *Acta Diurna Komunikasi*, 4 (2) 2015, hlm 1–4.

[92] R. Moore, *Op.Cit*, 2005

[93] Warren G. Kruse, Jay G. Heiser. *Op.Cit*. 2002, hlm 392

Cybercrimes dapat didefinisikan sebagai: "Pelanggaran yang dilakukan terhadap perorangan atau sekelompok individu dengan motif kriminal untuk secara sengaja menyakiti reputasi korban atau menyebabkan kerugian fisik atau mental atau kerugian kepada korban baik secara langsung maupun tidak langsung, menggunakan jaringan telekomunikasi modern seperti Internet (jaringan termasuk namun tidak terbatas pada ruang Chat, email, notice boards dan kelompok) dan telepon genggam.[94] *Cybercrime* dapat mengancam seseorang, keamanan negara atau kesehatan finansial.[95]

Perkembangan yang kian pesat mengenai teknologi informasi komunikasi berbasis komputer telah berkembang sangat pesat di tengah masyarakat pada saat ini. Masyarakat pun kemudian menjadi dimudahkan dengan perkembangan teknologi tersebut.[96] Salah satu kemudahan teknologi yang dirasakan masyarakat adalah dengan adanya internet. Pada dewasa ini, informasi merupakan suatu media yang sangat menentukan bagi perkembangan ekonomi suatu negara baik negara berkembang maupun negara yang sudah maju.[97] Informasi mengenai individu selalu dikelola oleh pemerintah dan swasta, tetapi munculnya era komputer menciptakan ancaman yang lebih besar bagi privasi individu tersebut, serta kemungkinan individu menderita kerugian sebagai akibat dari ketidaktelitian atau pembocoran informasi akan jauh lebih besar.

---

[94] Debarati Halder & K. Jaishankar, *Op.Cit*: IGI, 2011

[95] Steve Morgan, *Op.Cit*. Retrieved September 22, 2016

[96] Nani Widya Sari, Kejahatan Cyber dalam Perkembangan Teknologi Informasi berbasis Komputer, *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan*, 5 (2) 2018, hlm 578

[97] Shinta Dewi, *Perlindungan Privasi Atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional*, Widya Padjajaran, Bandung, 2009, hlm. 53.

Penggunaan internet dalam berbagai bidang kehidupan tidak saja membuat segala sesuatunya menjadi lebih mudah, namun juga memunculkan sejumlah permasalahan termasuk dalam bidang hukum. Dari hasil survei terbaru yang dipaparkan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mengumumkan jumlah pengguna internet Indonesia tahun 2024 mencapai 221.563.479 jiwa dari total populasi 278.696.200 jiwa penduduk Indonesia tahun 2023. Dari hasil survei penetrasi internet Indonesia 2024 yang dirilis APJII, maka tingkat penetrasi internet Indonesia menyentuh angka 79,5%. Dibandingkan dengan periode sebelumnya, maka ada peningkatan 1,4%. Terhitung sejak 2018, penetrasi internet Indonesia mencapai 64,8%. Kemudian secara berurutan, 73,7% di 2020, 77,01% di 2022, dan 78,19% di 2023.[98]

Tidak dapat dihindari hal-hal demikian seperti yang sudah dijeleskan diatas, menimbulkan beberapa kasus cybercrime di Indonesia, seperti penipuan, hacking, penyadapan data orang lain, spaming email, manipulasi data dengan program komputer untuk mengakses data milik orang lain dan kejahatan yang berimplikatif pada ruang lingkup jenis *cybercrime*.

Dalam hal ini, keunikan kejahatan ini adalah penggunaan teknologi informasi dalam modus operandi. Itulah sebabnya mengapa modus operandi dalam dunia *cyber* tersebut sulit dimengerti oleh orang-orang yang tidak menguasai pengetahuan tentang komputer, tekhnik pemrogramannya dan seluk beluk dunia *cyber*. Kerugian yang

[98] https://apjii.or.id/berita/d/*apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang*, Diakses Pada Tanggal 19 Agustus 2025

ditimbulkan dari kejahatan ini dapat bersifat material maupun non-material. *Cybercrime* berpotensi menimbulkan kerugian pada banyak bidang seperti politik, ekonomi, sosial budaya yang lebih besar dampaknya dibandingkan dengan kejahatan berintensitas tinggi lainnya. Beberapa klasifikasi *cybercrime*, dalam beberapa literature dan praktiknya dikelompokan dalam beberapa bentuk, antara lain:

No	Jenis Kejahatan	Modus Operandi
1	Penipuan dan kejahatan finansial	Penipuan dengan menggunakan komputer adalah salah representasi fakta yang tidak jujur yang dimaksudkan untuk membiarkan orang lain melakukan sesuatu yang menyebabkan kerugian. Bentuk kecurangan dapat difasilitasi dengan menggunakan sistem komputer, termasuk penipuan bank, *carding*, pencurian identitas, pemerasan dan pencurian informasi rahasia. Berbagai penipuan internet banyak berbasis *phishing* dan *social engineering* yang menjadi sasaran biasanya konsumen dan pelaku bisnis.[99]
2	*Unauthorized Access*	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.[100]
3	*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 mengganggu ketertiban umum, contohnya adalah penyebaran pornografi.
4	Penyebaran virus secara sengaja	Penyebaran virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang

[99] Alcianno G. Gani, *Op.Cit*, 5 (1) 2018, hlm 18
[100] Dikdik, Elisatris, *Op.Cit*, 2009, hlm 9

		yang sistem emailnya terkena virus tida menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.
5	*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*.
6	*Cyber Espionage, Sabotage, and Extortion, Cyber Espionage*	Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. *Sabotage and Extortion* merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.
7	*Cyberwarfare*	Departemen Pertahanan Amerika Serikat (*Department of Defense* / DoD) mencatat bahwa dunia maya telah menjadi perhatian tingkat nasional melalui beberapa peristiwa terkini mengenai signifikansi geo-strategis. Di antaranya termasuk serangan terhadap infrastruktur Estonia di tahun 2007, yang diduga oleh hacker Rusia. "Pada bulan Agustus 2008, Rusia kembali melakukan serangan *cyber*, kali ini dalam kampanye kinetik dan non kinetik yang terkoordinasi dan disinkronkan melawan negara Georgia. Khawatir bahwa serangan semacam itu dapat menjadi norma perang antar negara di masa depan, dampak dari konsep operasi dunia maya akan disesuaikan oleh para komandan militer di masa depan.[101]
8	*Cyberextortion*	*Cyberextortion* terjadi saat sebuah situs web, *server e-mail* atau sistem komputer dikenai atau

[101] Alcianno G. Gani, *Op.Cit*, 5 (1) 2018, hlm 20

		diancam dengan penolakan berulang (*Denial of Service* / DoS) terhadap layanan atau serangan lainnya oleh *hacker* jahat. Para *hacker* ini menuntut uang sebagai imbalan dengan janji akan menghentikan serangannya dan atau menawarkan "perlindungan". Menurut Biro Investigasi Federal, saat ini semakin banyak serangan yang dilakukan para pelaku *cyberextortion* pada situs web perusahaan dan jaringan, melumpuhkan kemampuan / kinerja mereka untuk beroperasi dan menuntut pembayaran untuk memulihkan layanan mereka.[102]
9	Pelecehan	Dalam konten ini mungkin menyinggung dengan cara yang tidak spesifik, pelecehan mengarahkan kata-kata kotor, penghinaan atau komentar pada individu tertentu yang memusatkan perhatian pada jenis kelamin, ras, agama, kebangsaan atau orientasi seksual, atau biasa di sebut mengandung unsur SARA. Hal ini sering terjadi di *chat room*, melalui *newsgroup* dan dengan mengirim email kebencian ke pihak yang berkepentingan. Pelecehan di internet juga termasuk balas dendam.[103]
10	*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.
11	Perdagangan narkoba	Pasar gelap digunakan untuk membeli dan menjual obat-obatan terlarang secara online.

[102] *Ibid*, hlm 19
[103] *Ibid*, hlm 21

		Beberapa pedagang narkoba menggunakan alat pesan terenkripsi untuk berkomunikasi dengan pemasok narkoba. Situs web gelap *Silk Road* adalah pasar online utama untuk obat-obatan sebelum dimatikan oleh penegak hukum (kemudian dibuka kembali di bawah manajemen baru, dan kemudian ditutup oleh penegak hukum lagi). Setelah *Silk Road 2.0* turun, *Silk Road 3 Reloaded* muncul. Namun sebenarnya itu hanya pasar yang lebih lama yang bernama *Diabolus Market*, yang menggunakan nama tersebut untuk lebih banyak menarik keuntungan dari kesuksesan merek sebelumnya.[104]
12	*Hacking* dan *Cracker*	Istilah *hacker* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut *cracker*. Boleh dibilang *cracker* ini sebenarnya adalah *hacker* yang 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.[105]
13	*Hijacking*	*Hijacking* merupakan kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah *Software Piracy* (pembajakan perangkat lunak).

[104] *Ibid*, hlm 22
[105] Sahat Maruli T. Situmeang, *Op.Cit* , 2020, hlm 27

14	*Cyberterrorism*	Seorang *cyberterrorist* adalah seseorang yang mengintimidasi atau menggalang pemerintah atau organisasi untuk memajukan tujuan politik atau sosialnya dengan meluncurkan serangan berbasis komputer terhadap komputer, jaringan atau informasi yang tersimpan di dalamnya. *Cyberterrorism* secara umum dapat didefinisikan sebagai tindakan terorisme yang dilakukan melalui penggunaan dunia maya atau sumber daya komputer. Suatu tindakan *cybercrime* termasuk *cyberterorism* jika mengancam pemerintah atau warga negara, termasuk *cracking* ke situs pemerintah atau militer.[106] Sebagai contoh, sebuah propaganda sederhana di Internet akan terjadi serangan bom saat liburan tahun baru bisa dianggap sebagai *cyberterrorism*. Ada juga kegiatan hacking yang diarahkan pada individu atau keluarga yang diselenggarakan oleh kelompok-kelompok di dalam jaringan, cenderung menimbulkan ketakutan di kalangan orang-orang, mengumpulkan informasi yang relevan untuk menghancurkan kehidupan masyarakat, perampokan, pemerasan, dll.[107]
15	Perjudian Online	Judi online merupakan salah satu bentuk kejahatan siber (*cybercrime*) yang memanfaatkan teknologi informasi dan komunikasi, khususnya internet, sebagai media untuk melakukan tindak pidana perjudian. Perjudian yang sebelumnya hanya dikenal secara konvensional kini bertransformasi ke ranah digital dengan memanfaatkan internet sebagai media utama. Aktivitas ini tidak hanya melanggar norma sosial dan moral, tetapi juga menimbulkan persoalan

[106] *Ibid*, hlm 28
[107] Alcianno G. Gani, *Op.Cit*, 5 (1) 2018, hlm 19

		hukum yang kompleks karena sifatnya yang lintas batas dan sulit dilacak.[108]

Kejahatan Dunia Maya (*Cybercrime*) adalah salah satu produk dari globalisasi kejahatan, dimana kejahatan dilakukan tanpa terbatas pada ruang dan waktu. Muladi dan Diah Sulistyani R.S menjelaskan bahwa akselarasi transportasi, komunikasi dan informasi modern melahirkan globalisasi teknologi yang berpengaruh terhadap globalisasi kejahatan (*globalization of crime*). Lebih lanjut dikatakan, kebijakan hukum pidana (*criminal policy*) yang dapat dilakukan dalam menanggulangi hal tersebut adalah dengan *warmaking criminology or harm creating on crime* yang bersifat bermusuhan (*adversarialism*) sebagai pendekatan represif dan dikombinasikan dengan pendekatan preventif mutualisme atau kebersamaan atas dasar *peacemaking criminology*.[109]

Dalam menanggulangi cybercrime maka diperlukan upaya komprehensif baik melalui hukum pidana maupun melalui saluran hukum pidana. Kebijakan pencegahan cybercrime dengan hukum pidana mencakup bidang kebijakan penal yang merupakan bagian dari kebijakan kriminal. Dari sudut pandang kebijakan pidana, upaya pencegahan kejahatan (termasuk penanggulangan cybercrime) tidak dapat dilakukan

[108] Seri Mughni Sulubara, et.all. Judi Online Sebagai Cybercrime Serta Tantangan Penegakan Hukum Pidana di Era Digital: Antara Regulasi, Pembuktian, dan Ancaman Cybercrime, *Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora*, 4 (2) April 2025, hlm 540

[109] Indra Utama Tanjung, et.al. Politik Hukum Terhadap Penanggulangan Kejahatan Dunia Maya, *Judge: Jurnal Hukum*, 3 (1) Februari 2022, hlm 2-3

hanya secara parsial dengan hukum pidana (hukum pidana) namun hal tersebut juga harus dilakukan dengan pendekatan sistematik.[110]

Pada hakikatnya politik atau kebijakan hukum pidana adalah bagaimana hukum pidana dapat dirumuskan secara memadai, memberikan pedoman bagi pembentuk undang-undang, dan melaksanakan hukum pidana. Kebijakan legislatif sangat menentukan dalam tahap-tahap berikutnya karena pada saat akan dibuat peraturan perundang-undangan pidana sudah ditentukan tujuan yang ingin dicapai.

Dalam menanggulangi kejahatan siber (cybercrime) maka diperlukan adanya hukum *Cyber* atau *Cyber Law* adalah aspek hukum yang istilahnya berasal dari *Cyberspace Law* yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet elektronik yang dimulai pada saat mulai online dan memasuki dunia cyber atau maya.

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. Seiring dengan meningkatnya akses internet, muncul berbagai bentuk kejahatan siber seperti pencurian data, peretasan sistem, dan

[110] James Popham, Mary McCluskey and Michael Ouellet, Exploring Police-Reported Cybercrime In Canada Variation And Correlates, *Policing: An International Journal*, 43 (1) 2020, hlm 35

penyebaran malware. Kondisi ini menuntut peran aktif politik hukum dalam membentuk kerangka regulasi yang adaptif dan efektif.[111]

Kebijakan kriminalisasi atau rumusan hukum pidana di Indonesia yaitu sumber hukum pidana materiil pada Kitab Undang-undang Hukum Pidana (KUHP), yaitu norma pidana dalam KUHP sebagian besar masih konvensional dan belum berkaitan langsung dengan perkembangan cybercrime. Selain itu juga terdapat berbagai kelemahan dan keterbatasan dalam menghadapi perkembangan teknologi dan kejahatan teknologi tinggi yang sangat bervariasi. Misalnya, KUHP kesulitan menangani pemalsuan kartu kredit dan transfer dana elektronik karena tidak ada aturan khusus mengenai hal tersebut. Ketentuan yang ada hanya menyangkut: a) sumpah/pernyataan palsu (Pasal 242); b) menghindari mata uang dan uang kertas (Pasal 244-252); c) pemalsuan stempel dan tanda (Pasal 253-262); dan (d) pemalsuan surat (Pasal 263-276).[112]

Oleh karenanya muncul aturan hukum tentang kejahatan Cyber yang di latarbelakangi oleh alasan perkembangan zaman dan perubahan sosial di masyarakat yang memacu Indonesia untuk memiliki Cyber Law mengingat hukum-hukum tradisional sudah tidak dapat dan tidak mampu mengantisipasi perkembangan dunia Cyber atau dunia maya yang semakin pesat. Cyber law di Indonesia sudah diatur dalam

[111] N. R. Putra, et.al. Politik Hukum Teknologi Blockchain Indonesia Menuju Kerangka Hukum yang Implementasi Inovasi dan Adaptasi. *Hukum Dinamika Ekselensia*, 6 (4) 2024

[112] Nurianto Rachmad Soepadmo, Impact Analysis of Information and Electronic Transactions Law (Law No. 19 Year 2016) on the Level of Cyber-Crime in Social Media, *International Journal of Innovation, Creativity and Change*, 12, (8) 2020, hlm 490.

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) muncul di Indonesia pada tahun 2008 pada bulan April, Undang-undang ini disahkan oleh DPR dan kemudian dikenal dengan Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE 2008).

Secara prinsipil, delik atau tindak pidana ialah tindakan yang tak diperbolehkan oleh seorang individu maupun kelompok. Terdapat 8 macam delik yang harus diketahui: Delik formil dan materil; Delik kejahatan dan delik pelanggaran; Delik aduan; Delik umum; Delik tunggal dan delik berganda; Delik *dolus* dan delik *culpa*; Delik *commisionis*, delik *ommisionis*, dan delik *commissionis* per *ommissionem commissa*; serta Delik yang berlangsung terus dan delik yang tidak berlangsung terus.[113]

Sedangkan pidana dalam UU ITE dalam Regulasi mengenai pemakaian Teknologi Informasi dan Komunikasi (TIK) sudah ditetapkan secara jelas setelah diberlakukannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, setelah itu mengalami pembaharuan menjadi Undang-Undang Nomor 19 Tahun 2016 (disingkat UU-ITE). Beberapa tahun setelah UU-ITE diberlakukan, isu-isu seputar penggunaan TIK menjadi topik pembicaraan yang utama.

Kondisi ini menjelaskan bahwa berbagai kasus ITE yang tinggi umumnya melibatkan berbagai pasal yang banyak digunakan, contohnya pencemaran nama baik

[113] Andi Hamzah, *Op.Cit*, 2008

dan penyebaran berita palsu (*hoax*). Namun, penting dicatat bahwa kasus-kasus terkait ITE juga bervariasi, tidak hanya terbatas pada pencemaran nama baik atau penyebaran berita palsu. Tindakan yang tak diperbolehkan menurut Undang-Undang ITE didasari Pasal 27 hingga Pasal 37. Namun, secara lebih terinci, larangan konkret diatur hanya dari Pasal 27 hingga Pasal 35 dalam Undang-Undang ITE.[114]

Aturan ini diterapkan kepada semua individu yang melaksanakan tindakan hukum sesuai dengan UU ITE berlaku untuk di dalam maupun luar Indonesia, yang dapat berdampak hukum seluruh dunia, serta membawa pengaruh buruk kepentingan negara. Salah satu tujuan dari pembentukan UU ITE adalah untuk menyokong perkembangan teknologi informasi dengan menyusun kerangka hukum yang tepat, yang mengatur penggunaannya untuk memastikan keamanan dan mencegah penyalahgunaan, sambil tetap mempertimbangkan berbagai nilai agama serta budaya sosial masyarakat Indonesia.

Secara keseluruhan, keberadaan UU ITE memiliki beberapa manfaat potensial jika diterapkan dengan tepat. Terdapat manfaat UU ITE, seperti:

1) Kejelasan hukum dalam transaksi elektronik;
2) Mendorong pertumbuhan ekonomi di Indonesia;
3) Kontribusi dalam pencegahan kejahatan internet;

[114] Nikles Denny Ardiansyah, Bambang Panji Gunawan, dan Djasim Siswono. Penerapan UU ITE dalam Penegakan Hukum Siber di Indonesia Studi Kasus pada Pasal 27 Hingga Pasal 37, *Jurnal Reformasi Hukum : Cogito Ergo Sum*, 7 (2) Juli 2024, hlm 18-19

4) Perlindungan masyarakat serta penggunaan internet sesuai dengan Pasal 28 ayat (2).[115]

Undang-undang No. 19 Tahun 2016 tentang Perubahan Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik memberikan rincian tentang apa yang dinilai tidak sesuai dengan hukum. Melanggar UU ITE dapat mengakibatkan denda hingga hukuman penjara. Tindakan yang dilarang oleh Pasal 27 UU ITE, yaitu:

1) Memperluas Video Asusila;
2) Judi Online;
3) Melakukan Pencemaran Nama Baik;
4) Pemerasan serta Pengancaman.

Sedangkan dalam UU ITE Pasal 28 dijabarkan yaitu (1) Berita Bohong serta (2) Ujaran Kebencian. Materi UU ITE terbagi dua, yaitu: pengaturan transaksi elektronik dan informasi elektronik, serta pengaturan pelanggaran yang tak diperbolehkan dan diancam hukuman pidana (cybercrime). Selain itu, UU ITE adalah pengaturan tindak pidana siber sebagai Undang-Undang pertama di Indonesia.

Pengaturan mengenai perbuatan-perbuatan yang tidak diperbolehkan pada Bab VII, Pasal 27 - Pasal 37 UU ITE. Perbuatan yang tak diijinkan adalah membuat maupun melakukan perubahan informasi hingga data elektronik sedemikian rupa sehingga terlihat sebagai data atau informasi yang benar. Perihal ini berada pada Pasal 35 UU ITE yang menjabarkan bahwa masing-masing individu yang dengan sengaja

[115] *Ibid*, hlm 19

mengubah, menciptakan, mengubah, menghapus, atau penghancuran Informasi Elektronik dan/atau Dokumen Elektronik dengan niat supaya informasi maupun data tersebut dianggap sebagai data yang asli. Pasal 51 ayat (1) UU ITE mengatur sanksi pidana bagi pelanggaran tersebut, yang menyatakan bahwa setiap individu yang memenuhi berbagai ketentuan layaknya penjelasan dalam Pasal 35 dapat dikenai pidana penjara maksimal 12 tahun dan/atau denda paling banyak dua belas miliar rupiah.

Rumusan dalam Pasal 35 UU ITE, tindak pidana tersebut ialah delik formil, yakni suatu tindak pidana dianggap terjadi begitu perbuatan yang dilarang dilakukan, tanpa memerlukan adanya hasil atau dampak dari perbuatan tersebut. Dengan kata lain, individu bisa dianggap melaksanakan tindak pidana hanya dengan memenuhi kategori perbuatan yang diatur pada undang-undang, tanpa perlu membuktikan akibat dari perbuatan tersebut. Adapun Menurut Pasal 1 angka 5 UU ITE, sistem elektronik terdiri dari berbagai alat serta langkah elektronik yang digunakan mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan data elektronik.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diperbarui melalui Undang-Undang Nomor 1 Tahun 2024, menjadi dasar hukum utama dalam mengatur aktivitas di dunia digital. Dengan disahkanya produk hukum yakni Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Undang-Undang ITE) memiliki

substansi beberapa terobosan dan perluasan asas hukum pidana, alat bukti dan sanksi-sanksinya.

Rapat Paripurna DPR pada 5 Desember 2023 telah menyepakati RUU tentang perubahan kedua UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menjadi UU. Terhitung sejak Februari 2023, pemerintah sudah bergerak mempersiapkan materi perubahan kedua UU ITE. Perubahan ini disambut hangat. Apalagi perubahan kedua ini dilakukan dalam rangka menjawab keresahan publik akan ketidakpastian hukum di dalam UU ITE. Perubahan kedua ini menjadi sorotan tatkala materi regulasi ternyata tidak mencabut pasal yang dianggap menimbulkan polemik, termasuk Pasal 27 ayat (3) tentang pencemaran nama baik. Padahal multitafsir akan pasal tersebut selama ini disinyalir sebagai salah satu penyebab ketidakpastian hukum UU ITE. Masih hadirnya pasal tersebut di dalam perubahan kedua UU ITE mengingatkan kita kepada perubahan pertama UU ITE. Penghapusan Pasal 27 ayat (3) kerap disuarakan. Namun, nyatanya pasal tersebut masih dipertahankan. Mengutip pernyataan Menkoimfo saat itu bahwa Pasal 27 ayat (3) UU ITE tidak mungkin untuk dihapuskan karena dapat menghilangkan efek jera.[116]

Disetujuinya RUU perubahan kedua UU ITE menjadi UU diharapkan dapat memberikan angin segar. Perubahan terhadap 14 pasal dan penambahan 5 pasal diyakini akan lebih memberikan kepastian hukum. Ada beberapa pasal dalam UU ITE

[116] Adi Darmawansyah, Andry Dwiarnanto, Irwan Putra Satriyawan, Istiqomah, Tinjauan Yuridis Cybercrime dalam Tindak Pidana Pencemaran Nama Baik meurut Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, *Jurnal Universitas Bung Karno*, 3 (1) Juni 2024, hlm 408

itu akan berlaku bersamaan dengan UU KUHP yang baru berlaku 1 Januari 2026. Namun ada pula beberapa Pasal UU ITE yang akan dicabut saat UU KUHP diterapkan, beberapa norma dalam revisi UU ITE itu merupakan adopsi dari UU KUHP sekaligus memberikan penjabaran detail dari UU ITE sebelumnya.

Menurut KUHP, tindak pidana umumnya mengacu pada suatu perbuatan yang diancam dengan sanksi pidana dan/atau tindakan oleh peraturan perundang-undangan harus bersifat melawan hukum atau bertentangan dengan hukum yang hidup dalam masyarakat. Sanksi yang dimaksud baik berupa denda maupun hukuman penjara. Namun definisi ini belum mencakup kejahatan berbasis teknologi yang lebih kompleks, seperti kejahatan siber. Maka dari itu, definisi dan regulasi untuk cybercrime diatur dalam undang-undang khusus.

Pada KUHP terbaru (UU No. 1 Tahun 2023), beberapa pasal mulai mencakup tindakan ilegal di ranah digital. Hal tersebut diatur pada Bagian Kelima tentang Tindak Pidana terhadap Informatika dan Elektronika (Pasal 332 sampai Pasal 335 KUHP).

1) Pasal 332 tentang akses ilegal ke komputer atau sistem elektronik. Pasal ini menyebutkan bahwa setiap orang yang secara sengaja dan tanpa izin memasuki sistem komputer milik orang lain dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan dengan tujuan untuk memperoleh Informasi Elektronik dan/ atau dokumen elektronik akan dikenakan pidana 6 (enam)

hingga 8 (delapan) tahun penjara atau denda paling banyak pada kategori V (Rp500 juta) hingga kategori VI (Rp2 miliar).[117]

2) Pasal 333 tentang penggunaan tanpa hak terhadap sistem elektronik untuk memperoleh, mengubah, merusak, atau menghilangkan informasi pertahanan nasional atau hubungan internasional yang dapat menyebabkan gangguan atau bahaya terhadap negara atau hubungan dengan subjek hukum internasional, melakukan tindakan yang menyebabkan transmisi dari program, informasi, kode atau perintah Komputer atau sistem elektronik yang dilindungi negara menjadi rusak., yang diancam dengan hukuman hingga 7 (tujuh) tahun penjara dan denda paling banyak kategori VI (Rp2 miliar).[118]
3) Pasal 334 khususnya mengenai keuntungan finansial yang diperoleh secara ilegal dari sistem elektronik yaitu dengan cara memperoleh informasi keuangan dari bank sentral, lembaga perbankan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayararn atau yang mengandung data laporan nasabahnya, serta menyebarkan, memperdagangkan, atau memanfaatkan Kode Akses atau informasi yang serupa dengan hal tersebut yang dapat digunakan menerobos Komputer atau sistem elektronik dengan maksud menyalahgunakan yang akibatnya dapat memengaruhi sistem elektronik bank sentral, lembaga perbankan atau lembaga keuangan, serta perniagaan di dalam dan luar negeri.

[117] Pasal 332 ayat (1), (2) dan (3) Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-undang Hukum Pidana

[118] Pasal 333 huruf a sampai i Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-undang Hukum Pidana

Pelaku yang terbukti melanggar pasal ini dapat dikenai pidana hingga 10 (sepuluh) tahun penjara atau pidana denda paling banyak kategori IV (Rp2 miliar).[119]

4) Pasal 335 akses ilegal informasi rahasia milik pemerintah. Pasal ini menyebutkan bahwa setiap Orang yang tanpa hak menggunakan atau mengakses Komputer atau sistem elektronik dengan cara apa pun, dengan maksud memperoleh, mengubah, merusak, atau menghilangkan informasi milik pemerintah yang karena statusnya harus dirahasiakan atau dilindungi, dipidana dengan pidana penjara paling lama 12 (dua belas) tahun atau pidana denda paling banyak kategori VII (Rp5 miliar).[120]

UU ITE memperjelas cakupan tindak pidana siber dengan menyebutkan jenis-jenis kejahatan yang secara spesifik berkaitan dengan aktivitas di ruang digital. Pasal 27 hingga Pasal 37 UU ITE secara spesifik mengatur tentang kejahatan terkait konten ilegal akses tidak sah, penyadapan, dan serangan terhadap integritas sistem lainnya.

UU ITE menganggap kejahatan siber sebagai pelanggaran serius dengan dampak yang besar. Oleh sebab itu, sanksi yang dikenakan terhadap pelaku cybercrime cukup berat, dengan ancaman pidana hingga sepuluh tahun penjara atau denda maksimal Rp 1 miliar, tergantung pada jenis dan tingkat kejahatannya.

[119] Pasal 334 huruf a sampai d Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-undang Hukum Pidana

[120] Pasal 335 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-undang Hukum Pidana

Beberapa kualifikasi cybercrime secara norma hukum pidana yang diatur dalam Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mencakup:[121]

No	Konstruksi Hukum	Jenis Kejahatan	Substansi Hukum
1	**Pasal 27** Pasal ini mengatur mengenai berbagai tindakan distribusi konten ilegal di ruang digital	Konten yang Melanggar Kesusilaan	Setiap orang dilarang untuk menyebarluaskan,mentransmisikan, atau membuat dapat diaksesnya informasi elektronik yang mengandung muatan yang melanggar kesusilaan secara sengaja dan tanpa hak. Muatan ini mencakup konten yang mengandung unsur pornografi, eksploitasi seksual, atau tindakan tidak senonoh yang dapat merusak moral masyarakat.
		Konten Perjudian	Melarang distribusi atau transmisi informasi elektronik yang mengandung unsur perjudian. Tindakan ini bertujuan untuk mencegah penyebaran aktivitas perjudian yang dapat diakses dengan mudah melalui media digital.
		Pencemaran Nama Baik dan Kehormatan	Pasal 27A yang disisipkan setelah Pasal 27 menjelaskan bahwa tindakan menyerang kehormatan atau nama baik orang lain melalui tuduhan atau informasi palsu juga dianggap pelanggaran. Pelanggaran ini ditujukan pada mereka yang menggunakan media digital untuk

[121] Pasal 27-37 Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

			menyebarkan tuduhan yang dapat merusak reputasi seseorang.
		Pemaksaan dengan Ancaman	Pasal 27 B menambahkan larangan terhadap tindakan distribusi informasi yang digunakan untuk memeras atau mengancam orang lain. Tindakan ini mencakup ancaman untuk meminta barang, uang, atau pengakuan utang dengan menggunakan dokumen elektronik untuk menakut-nakuti korban.
2	**Pasal 28** Pasal ini mengatur penyebaran informasi elektronik yang berpotensi menimbulkan kerugian pada pihak lain, dengan dua fokus utama	Penyebaran Informasi Palsu atau Menyesatkan	Penyebaran Informasi Palsu atau Menyesatkan Melarang distribusi informasi yang berisi berita bohong atau informasi yang dapat menyesatkan masyarakat. Pelanggaran ini bertujuan untuk mencegah kerugian materiil pada konsumen dalam transaksi elektronik yang mengandalkan informasi akurat.
		Penyebaran Kebencian atau Hasutan	Melarang tindakan menyebarkan informasi yang menghasut atau mengajak orang lain untuk melakukan permusuhan atau kebencian terhadap kelompok berdasarkan ras, agama, etnis, dan sebagainya. Pasal ini melindungi masyarakat dari konten digital yang dapat memicu konflik atau diskriminasi.
3	**Pasal 29** Pasal ini mengatur mengenai larangan mengirimkan ancaman kekerasan atau ancaman lainnya secara langsung melalui dokumen elektronik	Ancaman Kekerasan	Setiap orang yang secara sengaja dan tanpa hak mengirimkan informasi yang berisi ancaman kekerasan kepada orang lain dapat dikenakan sanksi. Tujuan utama dari pasal ini adalah untuk melindungi individu dari intimidasi atau teror melalui pesan digital.

4	**Pasal 30** Pasal ini mengatur tentang akses tidak sah (*unauthorized access*) ke dalam sistem elektronik	Akses Tanpa Izin ke Sistem Elektronik	Setiap orang dilarang untuk memasuki atau menyusup ke dalam sistem elektronik milik orang lain tanpa izin yang sah. Tindakan peretasan atau penyusupan ke dalam perangkat atau jaringan digital yang bukan miliknya, untuk mengakses data atau informasi pribadi, adalah bentuk kejahatan siber yang diatur dalam pasal ini.
		Kontrol Ilegal atas Sistem	Selain mendapatkan akses, seseorang yang tanpa izin mencoba mengendalikan atau menguasai sistem elektronik orang lain juga dianggap melanggar hukum. Ini mencakup upaya untuk memanfaatkan sistem pihak lain untuk keuntungan pribadi atau untuk kepentingan jahat.
5	**Pasal 31** Pasal ini mengatur tentang penyadapan atau intersepsi informasi elektronik yang dilakukan secara ilegal	Larangan Penyadapan Komunikasi Digital	Setiap orang yang melakukan intersepsi atau penyadapan informasi elektronik orang lain tanpa izin dinyatakan melanggar hukum. Tindakan ini mencakup pengawasan terhadap komunikasi digital seperti email, pesan instan, atau panggilan suara tanpa persetujuan pihak yang bersangkutan.
		Hak atas Privasi dalam Komunikasi Digital	Pasal ini menguatkan prinsip privasi dengan memastikan bahwa informasi elektronik individu tidak dapat diakses, direkam, atau dipantau oleh pihak lain tanpa alasan hukum yang jelas. Setiap bentuk penyadapan harus dilakukan berdasarkan ketentuan hukum untuk menjaga hak asasi dan kebebasan berkomunikasi.
6	**Pasal 32**	Pengubahan, Penghilangan, atau	Setiap orang yang sengaja dan tanpa hak melakukan tindakan perusakan, pengubahan, penghilangan, atau

	Pasal ini mengatur tentang tindakan perusakan,pengubahan, penghilangan, atau pemindahan informasi elektronik atau dokumen elektronik tanpa izin	Pemindahan Data Elektronik Tanpa Izin	pemindahan data elektronik dianggap melanggar hukum. Ini termasuk segala upaya untuk mengubah isi data tanpa sepengetahuan atau izin pemiliknya, seperti menghapus atau merusak data milik orang lain di sistem elektronik.
		Penguasaan Data secara Melawan Hukum	Tindakan yang berupaya memindahkan data elektronik dari satu sistem ke sistem lain tanpa izin juga diatur dalam pasal ini. Misalnya, memindahkan atau mencuri data dari sistem perusahaan atau individu untuk keuntungan pribadi atau tujuan jahat adalah tindakan ilegal.
7	**Pasal 33** Pasal ini melarang setiap orang yang secara sengaja dan tanpa hak melakukan tindakan yang menyebabkan terganggunya sistem elektronik	Mengganggu Sistem Elektronik	Tindakan ini mencakup setiap usaha yang dapat mengganggu fungsi, aksesibilitas, atau efektivitas sistem elektronik, seperti serangan *Distributed Denial of Service* (DDoS) atau serangan lain yang menargetkan sistem agar tidak berfungsi secara normal.
		Mencegah Akses terhadap Sistem	Pasal ini juga melarang tindakan yang bertujuan untuk memblokir atau mencegah akses ke sistem elektronik oleh pihak yang berhak. Misalnya, melakukan pemblokiran terhadap situs atau jaringan tertentu tanpa izin merupakan tindakan ilegal.
8	**Pasal 34** Pasal ini melarang setiap orang yang dengan sengaja dan tanpa hak memproduksi, menjual, atau	Produksi dan Distribusi Perangkat Lunak Berbahaya (*Malware*)	Melarang pembuatan dan penjualan perangkat lunak yang dirancang untuk merusak, mencuri data, atau mengganggu sistem elektronik. Contoh perangkat lunak ini termasuk virus, trojan, dan *spyware* yang sering digunakan untuk tujuan peretasan atau pencurian data.

	menyebarkan perangkat lunak yang dirancang khusus untuk menyerang atau merusak sistem elektronik	Penggunaan Perangkat untuk Menyerang Sistem	Melarang setiap bentuk distribusi atau pemanfaatan alat yang dapat digunakan untuk menyerang sistem elektronik, termasuk alat yang dapat menembus sistem keamanan tanpa izin.
9	**Pasal 35** Pasal ini melarang setiap orang untuk memalsukan data elektronik atau dokumen elektronik	Pemalsuan Data Elektronik atau Dokumen	Setiap orang yang dengan sengaja dan tanpa hak memalsukan atau mengubah data atau dokumen elektronik untuk keuntungan pribadi atau tujuan tertentu dianggap melanggar hukum. Ini termasuk tindakan memalsukan tanda tangan elektronik atau dokumen resmi secara digital.
		Keamanan Identitas Digital dan Transaksi Elektronik	Pasal ini bertujuan untuk menjaga keaslian dan integritas data serta dokumen elektronik, yang penting dalam transaksi digital atau komunikasi resmi. Pelanggaran terhadap keaslian dokumen dapat mengakibatkan kerugian bagi individu maupun entitas bisnis.
10	**Pasal 36 dan Pasal 37** Pasal 36 dan Pasal 37 mengatur bahwa setiap tindakan yang melanggar pasal-pasal sebelumnya (Pasal 27-35) dan menimbulkan kerugian bagi orang lain dapat dikenakan sanksi.	Akibat Hukum bagi Pelanggaran yang Merugikan Pihak Lain	Setiap tindakan yang terbukti melanggar ketentuan dalam Pasal 27 hingga Pasal 35, dan menyebabkan kerugian materiil atau immateriil bagi orang lain, dapat dikenakan sanksi pidana. Dengan kata lain, jika tindakan tersebut terbukti berdampak pada kerugian korban, maka pelaku dapat dihukum lebih berat.
		Sanksi sebagai Bentuk Perlindungan Hukum	Pasal ini memperkuat perlindungan hukum terhadap korban kejahatan siber dengan memastikan bahwa pelaku yang menyebabkan kerugian pada orang lain melalui tindakan ilegal di dunia digital dapat dituntut dan dihukum.

Bentuk-bentuk kejahatan siber yang tercantum dalam UU ITE ini menunjukkan bahwa undang-undang telah mencakup berbagai aspek tindakan ilegal di ranah digital, baik yang berdampak langsung maupun tidak langsung terhadap individu, masyarakat, atau negara. Setiap pasal dalam UU ITE memberikan landasan hukum yang jelas untuk menindak berbagai aktivitas kriminal di ruang digital yang terus berkembang. [122] Misalnya, ketentuan tentang distribusi konten ilegal, penyebaran kebencian, dan ancaman kekerasan (Pasal 27-29) dirancang untuk menjaga ketertiban sosial serta mencegah penyebaran konten yang dapat memicu konflik atau kerusuhan dalam masyarakat. Pasal-pasal ini menegaskan larangan terhadap penyebaran informasi elektronik yang mengandung muatan kesusilaan, perjudian, fitnah, atau ujaran kebencian yang mengarah pada diskriminasi berbasis ras, agama, etnis, dan karakteristik lainnya.[123]

Selain itu, ketentuan mengenai akses tidak sah (Pasal 30) melindungi sistem elektronik dari peretasan atau penyusupan tanpa izin yang dapat membahayakan keamanan data dan integritas sistem. Pasal 31 juga mengatur larangan penyadapan dan intersepsi informasi elektronik yang bertujuan untuk menjaga hak privasi dalam komunikasi digital dari penyalahgunaan oleh pihak yang tidak bertanggung jawab.[124]

---

[122] A. Y. Pratama, et al., Penegakan Tindak Pidana Cyberstalking dalam Hukum Positif Indonesia. *Legal Standing: Jurnal Ilmu Hukum*, 8 (3) 2024, hlm 703.

[123] Budiyanto, *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia*, Sada Kurnia Pustaka, Serang Banten, 2025, hlm 18

[124] *Ibid*

Pasal-pasal yang mengatur gangguan data (Pasal 32) dan sistem (Pasal 33) berfungsi untuk melindungi integritas data dan operasional dari upaya peretasan yang dapat mengakibatkan kerugian finansial atau operasional pada lembaga yang diserang. Selain itu, UU ITE juga mengantisipasi penyebaran perangkat lunak berbahaya (Pasal 34) yang sering kali digunakan dalam serangan siber untuk mengendalikan atau merusak sistem komputer milik orang lain. Dalam hal ini, UU ITE tidak hanya menindak pelaku yang menggunakan teknologi secara ilegal, tetapi juga mereka yang memproduksi dan mendistribusikan perangkat atau perangkat lunak dengan tujuan kriminal.[125]

Selanjutnya, pasal tentang manipulasi data dan informasi elektronik (Pasal 35) memberikan perlindungan terhadap keaslian data, yang sangat penting dalam transaksi bisnis dan legalitas dokumen digital. Tindakan manipulasi data ini dapat mengakibatkan kerugian besar bagi korban yang datanya diubah atau disalahgunakan. Akhirnya, ketentuan yang mengatur perbuatan yang merugikan pihak lain (Pasal 36-37) menunjukkan bahwa UU ITE melindungi semua pihak yang dirugikan, baik secara materiil maupun immateriil, akibat pelanggaran hukum siber.[126]

Dengan adanya berbagai ketentuan ini, UU ITE berfungsi sebagai instrumen yang komprehensif untuk menindak berbagai bentuk kejahatan siber di Indonesia dan memastikan keamanan digital bagi masyarakat luas.[127] Selain itu, dalam UU ITE

[125] *Ibid*
[126] *Ibid*
[127] *Ibid*, hlm 19

norma pidana berupa sanksi hukum pidana dalam lingkup cybercrime diatur pada Pasal 45, 45A serta 45B dengan variasi sanksi pidana penjara dan pidana denda sesuai bobot perbuatan delik pidana nya yang berupa:

1. Sanksi pidana Pasal 45

    1) Ayat (1) “Setiap Orang yang dengan sengaja dan tanpa hak menyiarkan, mempertunjukkan, mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan untuk diketahui umum sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rpl.000.000.000,00 (satu miliar rupiah)”;
    2) Ayat (3) “Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, dan/ atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan perjudian sebagaimana dimaksud dalam Pasal 27 ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 10.000.000.000,00 (sepuluh miliar rupiah)”.
    3) Ayat (4) “Setiap Orang yang dengan sengaja menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal, dengan maksud supaya hal tersebut diketahui umum dalam bentuk Informasi Elektronik dan/ atau Dokumen Elektronik yang dilakukan melalui Sistem Elektronik sebagaimana dimaksud dalam Pasal 27A dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/ atau denda paling banyak Rp400.000.000,00 (empat ratus juta rupiah)”.
    4) Ayat (6) “Dalam hal perbuatan sebagaimana dimaksud pada ayat (4) tidak dapat dibuktikan kebenarannya dan bertentangan dengan apa yang diketahui padahal telah diberi kesempatan untuk membuktikannya, dipidana karena fitnah dengan pidana penjara paling lama 4 (empat) tahun dan/ atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).
    5) Ayat (8) "Setiap Orang yang 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. sebagaimana dimaksud dalam Pasal 278 ayat (1) dipidana dengan

pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)".

6) Ayat (10) "Setiap Orang yang 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, dengan ancaman pencemaran atau dengan ancaman akan membuka rahasia, memaksa orang supaya: (a) memberikan suatu barang yang Sebagian atau seluruhnya milik orang tersebut atau milik orang lain; atau (b) memberi utang, membuat pengakuan utang, atau menghapuskan piutang. Sebagaimana dimaksud dalam Pasal 278 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).[128]

2. Sanksi Pidana Pasal 45A

1) Ayat (1) "Setiap Orang yang 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 Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)".
2) Ayat (2) "Setiap orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang sifatnya menghasut, mengajak, atau orang lain sehingga menimbulkan rasa kebencian atau permusuhan terhadap individu dan/atau kelompok masyarakat tertentu berdasarkan ras, kebangsaan, etnis, warna kulit, agama, kepercayaan, jenis kelamin, disabilitas mental, atau disabilitas fisik sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)".
3) Ayat (3) "Setiap Orang yang dengan sengaja menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik yang diketahuinya memuat pemberitahuan bohong yang menimbulkan kerusuhan di masyarakat sebagaimana dimaksud dalam Pasal 28 ayat (3) dipidana dengan pidana

[128] Pasal 45 Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah)".[129]

3. Sanksi Pidana Pasal 45B

"Setiap Orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik secara langsung kepada korban yang berisi ancaman kekerasan dan/ atau menakut-nakuti sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/ atau denda paling banyak Rp750.000.000,00 (tqjuh ratus lima puluh juta rupiah)".[130]

Kriminalisasi cybercrime di Indonesia khususnya dalam UU-ITE dapat dibagi dalam dua kategori, yaitu perbuatan yang menggunakan komputer sebagai sarana kejahatan, dan perbuatan-perbuatan yang menjadikan komputer sebagai sasaran kejahatan.[131] Kejahatan yang menggunakan komputer sebagai sarana adalah setiap tindakan yang mendayagunakan data komputer, sistem komputer, dan jaringan komputer sebagai alat untuk melakukan kejahatan di ruang maya bukan ruang nyata. Kejahatan yang menjadikan komputer sebagai sasaran adalah setiap perbuatan dengan menggunakan komputer yang diarahkan pada data komputer, sistem komputer, atau jaringan komputer, atau ketiganya secara bersama-sama. Perbuatan tersebut dilakukan di ruang maya bukan ruang nyata, sehingga seluruh aktivitas yang dilarang oleh peraturan perundang-undangan terjadi di ruang maya.

[129] Pasal 45A Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[130] Pasal 45B Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[131] Indra Utama Tanjung, et.al. *Op.Cit*, 3 (1) Februari 2022, hlm 7

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia merupakan langkah signifikan dalam memberikan kerangka hukum yang jelas untuk mengatur interaksi di dunia maya dan menangani kejahatan siber. Meskipun UU ITE telah mengalami beberapa revisi untuk menyesuaikan dengan perkembangan teknologi dan kebutuhan masyarakat, tantangan dalam penerapannya tetap ada, seperti potensi kriminalisasi pengguna internet dan ketidakpastian dalam eksposisi beberapa pasal. UU ITE mengatur berbagai jenis kejahatan siber dengan tujuan melindungi masyarakat dari dampak negatif teknologi informasi. Oleh karena itu, penting untuk terus melakukan evaluasi dan perbaikan terhadap kebijakan ini agar dapat lebih efektif dalam menanggulangi kejahatan siber dan melindungi hak-hak masyarakat di era digital.

B. Prosedur Hukum Upaya Digital Forensik dalam Tahap Penyidikan Tindak Pidana Cybercrime

Perkembangan pesat teknologi komunikasi berbasis internet telah mengubah banyak aspek kehidupan, mulai dari mempermudah komunikasi hingga meningkatkan efisiensi di berbagai bidang. Namun, kemajuan ini juga memunculkan tantangan besar berupa munculnya berbagai jenis kejahatan siber (*cyber crime*) yang menggunakan

internet sebagai media utama.[132] Cybercrime merupakan salah satu bentuk baru dari kejahatan di masa modern sekarang yang mendapatkan perhatian khusus di dunia internasional karena dianggap sangat membahayakan. Cybercrime merupakan kejahatan yang dilakukan secara berkelompok maupun perorangan dengan menggunakan perangkat komputer ataupun alat telekomunikasi apapun yang terhubung pada internet, biasanya dilakukan oleh orang yang ahli dalam penggunaan komputer yang dapat melakukan kejahatan tersebut.[133]

Tindak pidana siber merupakan suatu dampak negatif yang ditimbulkan dari perkembangan dunia digital. Pelaku dari tindak pidana siber merupakan seseorang yang memiliki keahlian dalam mengoperasikan ilmu komputer, dapat menguasai algoritma serta program komputer, memiliki kemampuan dalam menganalisis cara kerja sistem komputer, dan mampu menemukan celah untuk melemahkan sistem komputer sehingga dapat masuk kedalamnya untuk melakukan tindakan jahat.[134]Pelaku kejahatan dalam kelompok tindak pidana tersebut dengan cara yang tidak sah, tanpa izin, dan/atau tanpa sepengetahuan dari pemiliknya memasuki sistem jaringan komputer yang telah dijadikan sebagai target untuk dilakukannya suatu perbuatan pidana.[135]

---

[132] Ira Irmansyah, Kekuatan Digital Forensik dalam Mengungkap Tindak Pidana Cyber Crime (Studi Kasus: Hacker Ilegal Akses Pembayaran Kereta Commuter Indonesia (KCI), *Jispendiora: Jurnal Ilmu Sosial, Pendidikan dan Humaniora,* 3 (3) Desember 2024, hlm 122

[133] Sutarman. *Cyber Crime Modus Operandi dan Penanggulangannya.* Yogyakarta: LaksBang PRESSindo, 2007, hlm 24

[134] Sahat Maruli T. Situmeang, *Op.Cit ,* 2020.

[135] Dikdik dan Elisatris Gultom, *Op.Cit*, 2009.

Fenomena ini terjadi karena internet memungkinkan interaksi virtual tanpa batas geografis dan fisik, sehingga pelaku kejahatan dapat melakukan tindakan ilegal tanpa mudah terdeteksi. Karakteristik dunia maya yang anonim dan terdesentralisasi mempermudah pelaku untuk menghapus jejak digital mereka, sehingga identitas mereka sering kali sulit dilacak oleh penegak hukum.[136] Seringkali penegak hukum di Indonesia mengalami kesulitan saat melakukan penyidikan yang berupaya menjerat pelaku karena masalah pembuktian yang tidak memenuhi ketentuan sistem hukum pidana Indonesia, akan tetapi upaya penangkapan terhadap para pelaku kejahatan cybercrime harus tetap dilaksanakan, upaya perluasan alat bukti menjadi solusi untuk penegakkan hukum tersebut.

Penindakan terhadap pelaku kejahatan berdasarkan sistem peradilan pidana dilakukan melalui proses penyelidikan dan penyidikan terlebih dahulu. Kepolisian merupakan instansi penegak hukum dan memiliki fungsi untuk melakukan pelaksanaan penyelidikan dan penyidikan terhadap suatu peristiwa pidana yang terjadi di Indonesia. Penyidik Polri saat melakukan penegakan hukum terhadap tindak pidana siber memerlukan bantuan atau dukungan dari stakeholder siber lainnya[137], seperti PPNS pada Kementerian Komunikasi dan Digital (Komdigi), Badan Siber dan Sandi Negara (BSSN), Badan Intelijen Negara (BIN) bahkan sampai dapat berkoordinasi dengan

[136] Ira Irmansyah, *Op.Cit,* 3 (3) Desember 2024, hlm 122

[137] Manayra Aisha Putri Indradjaja, dkk. Implementation of Investigations into Cyber Crimes in a Comparative Legal Perspective: Indonesia and the United Kingdom, *Jurnal Ilmiah Penegakan Hukum*, 11 (2) Desember 2024, hlm 164

PPATK (Pusat Pelaporan dan Analisis Transaksi Keuangan) dalam menyelidiki transaksi keuangan digital pada lingkup kejahatan siber.

Secara umum, tahap penyidikan merupakan salah satu bagian penting dalam rangkaian tahap-tahap yang harus dilalui suatu kasus menuju pengungkapan terbukti atau tidaknya dugaan telah terjadinya suatu tindak pidana. Oleh sebab itu keberadaan tahap penyidikan tidak bisa dilepaskan dari adanya ketentuan perundangan yang mengatur mengenai tindak pidanananya.[138]

Penyidikan menurut Kitab Undang-Undang Hukum Acara Pidana yang tercantung dalan Pasal 1 angka 2 diartikan:

"Serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam Kitab Undang-Undang Hukum Acara Pidana untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terangnya suatu tindak pidana yang terjadi dan guna menemukan tersangkanya".

Penyidikan merupakan rangkaian tindakan penyidik untuk mencari dan mengumpulkan bukti agar dapat ditemukan tersangka. Sedangkan menurut K.wantjik Saleh yang dikutip dalam jurnal hukum Sahuri Lasmadi, penyidikan sendiri diartikan yaitu usaha dan tindakan untuk mencari dan menemukan kebenaran tentang apakah betul terjadi suatu tindak pidana, siapa yang melakukan perbuatan itu, bagaimana sifat perbuatan itu serta siapakah yang terlibat dengan perbuatan itu.[139]

Sehubungan dengan hal tersebut, Yahya Harahap memberikan penjelasan mengenai penyidik dan penyidikan yaitu:

---

[138] Hibnu Nugroho, *Op.Cit*, 2012, hlm. 67.
[139] Sahuri Lasmadi, *Op.Cit*, 2 (3) Juli 2010, hlm. 10.

"Sebagaimana yang telah dijelaskan pada pembahasan ketentuan umum Pasal I Butir 1 dan 2, Merumuskan pengertian penyidikan yang menyatakan,penyidik adalah pejabat Polri atau pejabat pegawai negeri tertentu yang diberi wewenang oleh undang-undang. Sadangkan penyidik sesuai dengan cara yang diatur dalam undang-undang untuk mencari dan mengumpulkan bukti, dan dengan bukti itu membuat atau menjadi terang suatu tindak pidana yang terjadi serta sekaligus menemukan tersangkanya atau pelaku tindak pidananya".[140]

Sedangkan Andi Hamzah, definisi dari Pasal 1 butir 2 yaitu :

Penyidikan dalam acara pidana hanya dapat dilakukan berdasarkan undang-undang, hal ini dapat disimpulkan dari kata-kata menurut cara yang diatur dalam undang-undang ini.[141]

Dalam bahasa Belanda ini sama dengan opsporing. Menurut de Pinto yang dikutip dalam jurnal Bambang Tri Bawono menyebutkan bahwa 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.[142]

Dari pengertian diatas dapat disimpulkan bahwa penyidikan merupakan suatu proses atau langkah awal yang merupakan suatu proses penyelesaian suatu tindakpidana yang perlu diselidik dan diusut secara tuntas di dalam sistem peradilan pidana, dari pengertian tersebut, maka bagian-bagian dari hukum acara pidana yang menyangkut tentang Penyidikan adalah ketentuan tentang alat- alat bukti, ketentuan tentang terjadinya delik, pemeriksaan di tempat kejadian, pemanggilan tersangka atau terdakwa, penahan sementara, penggeledahan, pemeriksaan dan introgasi, berita acara,

[140] *Ibid*., hlm. 15.
[141] Andi Hamzah, *Op.Cit*, 2008, hlm. 119
[142] Bambang Tri Bawono, *Op.Cit,* XXVI (2), Agustus 2011, hlm. 5555

penyitaan, penyampingan perkara, pelimpahan perkara kepada penuntut umum dan pengembalian kepada penyidik untuk disempurnakan.

Pemeriksaan yang dilakukan oleh penyidik difokuskan sepanjang hal yang menyangkut persoalan hukum. Titik pangkal pemeriksaan dihadapan penyidik ialah tersangka. Dari dialah diperoleh keterangan mengenai peristiwa pidana yang sedang diperiksa. Akan tetapi, ekalipun tersangka yang menjadi titik tolak pemeriksaan, terhadapnya harus diberlakukan asas akusatur atau biasa diartikan juga dengan menempatkan posisi tersangka sebagai orang yang tidak bersalah.

Tersangka harus ditempatkan pada kedudukan menusia yang memiliki harkat martabat. Dia harus dinilai sebagai subjek, bukan sebagai objek. Yang diperiksa bukan manusia tersangka. Perbuatan tindak pidana yang dilakukannyalah yang menjadi objek pemeriksaan. Pemeriksaan tersebut ditujukan ke arah kesalahan tindak pidana yang dilakukan oleh tersangka. Tersangka harus dianggap tak bersalah, sesuai dengan prinsip hukum "praduga tak bersalah" (*presumption of innocent*) sampai diperoleh putusan pengadilan yang telah berkekuatan hukum tetap.[143] Pada pemeriksaan tindak pidana, tidak selamanya hanya tersangka saja yang harus diperiksa. Adakalanya diperlukan pemeriksaan saksi atau ahli. Demi untuk terang dan jelasnya peristiwa pidana yang disangkakan.

Sistem hukum terkait pembuktian adalah salah satu segmen hukum yang telah ada sejak zaman dahulu. Ini disebabkan oleh naluri manusia dan masyarakat, dalam

[143] M Yahya Harahap, *Op.Cit.* 2009, hlm. 134

segala keprimitifannya, yang pada dasarnya mempunyai naluri keadilan. Naluri ini akan tersentuh jika terdapat keputusan pengadilan yang menghukum orang yang tidak bersalah, membebaskan orang yang bersalah, atau memberikan kemenangan pada pihak yang sebenarnya tidak berhak dalam suatu persengketaan. Pembuktian mengenai apakah terdakwa benar-benar melakukan tindak pidana yang dituduhkan merupakan elemen kunci dalam proses hukum pidana. Di sini, hak asasi manusia berada dalam bahaya. Oleh karena itu, tujuan dari hukum acara pidana adalah untuk mencari kebenaran materiil, berbeda dengan hukum acara perdata yang lebih memfokuskan pada kebenaran formal.[144]

Pembuktian merupakan masalah yang memegang peranan sidang pengadilan melalui pembuktian ditentukan nasib terdakwa. Apabila hasil pembuktian dengan alat-alat bukti yang ditentukan undangundang tidak cukup membuktikan kesalahan yang didakwakan kepada terdakwa, maka terdakwa dibebaskan dari hukuman. Sebaliknya, kalau kesalahan terdakwa dapat dibuktikan dengan alat bukti yang disebut dalam Pasal 184 KUHAP, terdakwa dinyatakan bersalah kepadanya akan dijatuhkan oleh karena itu, hakim harus berhati-hati, cermat, dan matang menilai dan mempertimbangkan nilai pembuktian meneliti sampai dimana batas minimum kekuatan pembuktian atau *Bewijs Kracht* dari setiap alat bukti yang disebut dalam Pasal 184 KUHAP.[145]

---

[144] Amsori, Fakhri Awaluddin, dan Momon Mulyana. Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital, *Journal Humaniora: Jurnal Hukum dan Ilmu Sosial*, 02 (01) Januari 2024, hlm 17

[145] M Qahar Awaka dan Alhadiansyah, Utilization of Digital Forensics in Proving the Crime of Disseminating Indecent Videos Through Facebook Social Media in the Legal Area of West Kalimantan Police, *Jurnal Hukum Sehasen*, 9 (2) Oktober 2023, hlm 459

Pembuktian bersalah tidaknya seseorang terdakwa haruslah melalui pemeriksaan di depan sidang pengadilan. Dalam hal pembuktian ini, hakim perlu memperhatikan kepentingan masyarakat dan kepentingan terdakwa. Kepentingan masyarakat berarti, bahwa seseorang yang telah melanggar ketentuan pidana (KUHP) atau undang-undang pidana lainnya, harus mendapat hukuman yang setimpal yang kesalahannya. Sedangkan kepentingan terdakwa, berarti bahwa terdakwa harus diperlakukan secara adil sedemikian rupa sehingga tidak ada seseorang yang tidak bersalah mendapat hukuman, atau kalau memang ia bersalah jangan sampai mendapat hukuman yang terlalu berat, tetapi hukuman itu harus seimbang dengan kesalahannya.

Begitu pula dalam cara mempergunakan dan menilai kekuatan pembuktian yang melekat pada setiap alat bukti, dilakukan dalam batas-batas yang dibenarkan undang-undang, agar dalam mewujudkan kebenaran yang hendak dijatuhkan, majelis hakim terhindar dari pengorbanan kebenaran yang harus dibenarkan. jangan sampai kebenaran yang diwujudkan dalam putusan berdasar hasil perolehan dan penjabaran yang keluar dari garis yang dibenarkan sistem pembuktian. tidak berbau dan diwarnai oleh perasaan dan pendapat subjektif hakim.[146]

Menghadapi kejahatan siber, salah satu tantangan utama adalah proses pembuktian tindak pidana. Dalam konteks hukum pidana, pembuktian adalah aspek krusial dalam proses peradilan karena berpengaruh pada keputusan terhadap terdakwa. Pembuktian mencakup prosedur yang sah secara hukum untuk membuktikan

[146] *Ibid*

kebenaran tuduhan, serta bukti-bukti yang diakui dan diterima oleh undang-undang. Proses ini berperan penting karena jika pembuktian gagal, terdakwa dapat dibebaskan. Sebaliknya, jika bukti cukup, terdakwa dapat dinyatakan bersalah dan dijatuhi hukuman.[147]

Proses pembuktian biasanya dimulai sejak adanya indikasi peristiwa pidana. Penyelidikan dilakukan untuk mencari tahu apakah suatu peristiwa dapat dikategorikan sebagai tindak pidana. Penyidikan selanjutnya dilakukan untuk mengumpulkan bukti yang relevan, sesuai dengan ketentuan dalam Pasal 1 angka 13 Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian. Dalam kasus kejahatan siber, bukti digital seperti log data, metadata, dan dokumen elektronik sangat vital. Pasal 5 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) secara tegas menyatakan bahwa informasi elektronik beserta hasil cetaknya dapat dijadikan bukti yang sah di pengadilan.

Cyber crime memiliki ciri khas yang membedakannya dari kejahatan konvensional, termasuk dalam hal pelaku, korban, modus operandi, dan tempat kejadian. Oleh karena itu, dibutuhkan pendekatan serta peraturan khusus yang di luar cakupan Kitab Undang-Undang Hukum Pidana (KUHP) untuk menangani masalah ini. Perkembangan teknologi yang cepat mengharuskan sistem hukum untuk lebih fleksibel dan responsif terhadap perubahan yang terjadi di dunia maya. Dalam hal ini, kepolisian

[147] Ira Irmansyah, *Op.Cit,* 3 (3) Desember 2024, hlm 122

sebagai aparat penegak hukum memiliki peran penting, mulai dari penyelidikan awal hingga pengumpulan bukti yang sah untuk diajukan di pengadilan.

Secara yuridis, Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP) telah menetapkan alat bukti yang sah menurut undang-undang, yang terdiri dari (1). Keterangan Saksi, (2). Keterangan Ahli, (3). Surat, (4). Petunjuk, (5). Keterangan Terdakwa. Menurut Yahya Harahap, Pasal 184 ayat (1) KUHAP secara jelas telah menentukan alat bukti yang sah menurut undang-undang. Diluar jenis-jenis alat bukti tersebut, penggunaan bukti tidak dibenarkan untuk membuktikan kesalahan terdakwa. Para pihak yang terlibat dalam sidang, seperti Ketua sidang, penuntut umum, terdakwa, atau penasihat hukum, terikat dan hanya diperbolehkan menggunakan alat-alat bukti yang telah ditentukan oleh Pasal 184 ayat (1) KUHAP. Mereka tidak diperkenankan menggunakan alat bukti lainnya sesuai keinginan mereka di luar jenis alat bukti yang telah ditentukan. Hanya alat-alat bukti yang telah ditetapkan tersebut yang dianggap sah dan memiliki "kekuatan pembuktian". Penggunaan alat bukti di luar jenis yang telah ditetapkan tidak memiliki nilai pembuktian yang sah dan tidak diakui sebagai alat bukti yang mengikat. Namun, hal ini menimbulkan permasalahan dalam penggunaan alat bukti elektronik. Dalam UU ITE sebagai suatu peraturan hukum khusus, terdapat prinsip-prinsip hukum baru yang berbeda dari sistem hukum yang ada dalam KUHP maupun KUHAP. Salah satunya adalah pengakuan alat bukti elektronik sebagai alat bukti yang sah dalam hukum pembuktian di Indonesia. Sejak UU ITE diundangkan, terjadi penambahan jenis alat bukti di persidangan, yaitu informasi elektronik dan/atau dokumen elektronik. Dalam ketentuan umum UU ITE, diketahui

bahwa jenis data elektronik seperti tulisan, foto, suara, dan gambar dianggap sebagai informasi elektronik, sementara jenis informasi elektronik seperti tulisan, foto, suara, dan gambar yang disimpan pada flashdisk yang dapat dibuka melalui perangkat komputer dianggap sebagai dokumen elektronik.

Pasal 1 angka 4 UU ITE, dokumen elektronik merujuk pada data atau informasi yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau bentuk lain yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik. Dokumen elektronik meliputi tulisan, suara, gambar, peta, rancangan, foto, atau bentuk lainnya, serta mencakup huruf, tanda, angka, kode akses, symbol, atau perforasi yang memiliki makna atau arti dan dapat dipahami oleh orang yang mampu memahaminya. Sementara itu, pengertian informasi elektronik berdasarkan Pasal 1 angka 1 Undang-Undang ITE adalah satu atau kumpulan data elektronik, termasuk tulisan, suara, gambar, peta, rancangan, foto, elektronik data *interchange* (EDI), surat elektronik (electronic mail), telegram, telecopy, atau bentuk lainnya, serta mencakup huruf, tanda, angka, kode akses, symbol, atau perforasi yang telah diolah dan memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Dalam konteks Undang-Undang ITE, diatur bahwa informasi elektronik atau dokumen elektronik, beserta hasil cetaknya, merupakan alat bukti yang sah dan merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia. Alat bukti elektronik yang dibuat dalam bentuk informasi elektronik dan dokumen elektronik dianggap sah menurut UU ITE. Hal ini sejalan dengan Pasal 184 Kitab Undang-Undang Hukum Acara Pidana

(KUHAP), yang menyatakan bahwa alat-alat bukti yang sah terdiri dari keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa.[148]

Pembuktian tindak pidana informasi dan transaksi elektronik melalui alat-alat bukti menurut UU ITE terbaru yaitu Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, diatur dalam Pasal 5 yang menentukan:

1) Informasi Elektronik dan/ atau Dokumen Elektronik dan/ atau hasil cetaknya merupakan alat bukti hukum yang sah;
2) Informasi Elektronik dan/ atau Dokumen Elektronik dan/ atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.
3) Informasi Elektronik dan/ atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini.[149]

Berdasarkan ketentuan Pasal 5 UU ITE tersebut di atas dapat diketahui bahwa alat-alat bukti dalam pembuktian tindak pidana informasi dan transaksi elektronik dalam informasi elektronik dan atau dokumen elektronik dan atau hasil cetakannya merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku

[148] M Qahar Awaka dan Alhadiansyah, *Op.Cit*, 9 (2) Oktober 2023, hlm 463
[149] Pasal 5 Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

di Indonesia yakni Undang-undang Nomor 8 Tahun 1981 tentang Kitab Undang-undang Hukum Acara Pidana (KUHAP).

Alat-alat bukti ini sangat diperlukan karna hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang- kurangnya dan alat bukti yang sah, hakim memperoleh keyakinan bahwa suatu tindak pidana benar terjadi dan terdakwalah yang melakukan perbuatan itu. Pembuktian tindak pidana cybercrime harus didasarkan pada alat-alat bukti yang sah sebagaimana diatur dalam Pasal 5 UU ITE dan Pasal 184 KUHAP. Alat-alat bukti tersebut harus benar-benar sesuai dengan fakta artinya tidak rekayasa.[150]

Penyidikan tindak pidana informasi dan transaksi elektronik menurut Pasal 42 UU ITE dilakukan berdasarkan ketentuan dalam hukum acara pidana dan ketentuan dalam UU ITE. Maksudnya, semua aturan yang ada dalam KUHAP tetap berlaku sebagai ketentuan umum (*lex generalis*), kecuali disimpangi oleh UU ITE sebagai ketentuan khusus (*lex specialis*). Dengan kata lain, ketentuan mengenai penyidikan yang tidak diatur dalam UU ITE tetap diberlakukan sesuai dengan ketentuan yang ada di KUHAP. Pengaturan ini juga selaras dengan ketentuan dalam Pasal 284 ayat (2) KUHAP yaitu bahwa terhadap semua perkara diberlakukan ketentuan dalam KUHAP, dengan pengecualian terdapat ketentuan khusus acara pidana pada undang-undang tertentu, sampai ada perubahan dan/atau tidak dinyatakan berlaku lagi.[151]

---

[150] Adi Darmawansyah, Andry Dwiarnanto, Irwan Putra Satriyawan, Istiqomah, *Op.Cit*, 3 (1) Juni 2024, hlm 420

[151] Josua Sitompul, *Cyberspace Cybercrimes Cyberlaw Tinjauan Aspek Hukum Pidana*, Jakarta: Tatanusa. 2012, hlm 309

Secara mekanisme, alat bukti yang diperoleh dari proses penyidikan, penyidikan cybercrime atau tindak pidana informasi dan transaksi elektronik, memiliki perbedaan dengan penyidikan tindak pidana umum atau konvensional. Penyidikan cybercrime tidak bisa dilakukan seperti tindak pidana konvensional karena dalam mengungkap kasus cybercrime perlu yang namanya digital forensik untuk memudahkan penyidik dalam menemukan alat bukti maupun barang bukti, sehingga dapat membuat terang suatu tindak pidana dan juga tersangkanya.[152]

Dalam hal pengakuan adanya barang bukti elektronik, setiap kasus cybercrime atau kejahatan umum yang ditemukan barang bukti digital atau barang bukti elektronik dalam penyidikan harus dimulai dari tahap pengumpulan barang bukti dan menggunakan forensik digital hingga tahapan selanjutnya. Kegunaan digital forensik sejak tahap penyidikan adalah untuk berusaha menemukan kebenaran materiil dalam setiap proses pembuktian suatu tindak pidana, sehingga dapat mewujudkan asas du*e process of law*.[153]

Sebagai kejahatan dunia maya, pemeriksaan bukti yang ditemukan oleh polisi harus dilakukan sesuai dengan tahap yang seharusnya dilakukan, yakni dengan menggunakan teknik digital forensik yang merupakan semua tahapan pengambilan, pemulihan, penyimpanan, pemeriksaan informasi dan dokumen elektronik dengan

[152] Sharofan Mirfandaresky, et.al,. Digital Forensik dalam Penyidikan Tindak Pidana Penipuan Online (Studi Kasus di Wilayah Hukum Kepolisian Resor Ponorogo), *Dinamika*, 28 (10) Januari 2022, hlm 4611

[153] Fachrul Rozi, Sistem Pembuktian Dalam Proses Persidangan Pada Perkara Pidana, Jurn*al Yuridis Unaja*, 1 (2) 2019.

menggunakan metode dan alat yang bertanggung jawab untuk memperoleh bukti yang dapat dihadirkan di persidangan.

Perlunya digital forensik dalam mengungkap cybercrime dikarenakan beberapa hal diantaranya:

1) Kegiatan cybercrime tidak terbatas oleh teritorial negara;
2) Kegiatan cybercrime tidak berwujud;
3) Sulitnya pembuktian karena data elektronik relatif mudah untuk diubah, disadap, dipalsukan dan dikirimkan ke seluruh belahan dunia dalam hitungan detik;
4) Sudah tidak memungkinkan lagi menggunakan hukum konvensional.[154]

Secara terminlogi, menurut Sulianta mengatakan forensik memilki arti "membawa ke pengadilan". Istilah Forensik adalah suatu proses ilmiah dari ilmu pengetahuan dalam mengumpulkan, menganalisa, dan menghadirkan bukti-bukti dalam persidangan terkait adanya suatu kasus hukum.[155] Dalam proses penanganan tindak pidana kejahatan yang didalamnya menggunakan teknologi informasi tentunya akan membutuhkan proses investigasi forensik. Forensik merupakan suatu kegiatan kajian ilmiah yang dilakukan oleh ahli sesuai dengan kompetensinya bertujuan untuk melakukan identifikasi dan menentukan fakta-fakta yang berhubungan dengan perkara pidana dan bukti-bukti penunjang terjadinya perkara pidana dimaksud.

[154] Sharofan Mirfandaresky, et.al,. *Op.Cit*, 28 (10) Januari 2022, hlm 4612
[155] Sulianta Feri. *Op.Cit*, 2008.

Analisis forensik merupakan suatu upaya penyidik dalam kewenangannya untuk memintakannya kepada ahli forensik melakukan kajian ilmiah sebagai salah satu langkah penting guna membuat terang suatu perkara pidana dalam kejahatan komputer menggunakan ilmu digital forensik yang dimiliki oleh ahli forensik tersebut.

Salah satu bagian dari ilmu forensik adalah forensik digital yang cakupannya adalah penemuan atas hasil investigasi data yang telah ditemukan dalam perangkat digital seperti komputer, handphone dan lainnya. Berbeda dari forensik pada umumnya, digital forensik atau komputer forensik adalah kegiatan ilmiah dalam melakukan pengumpulan serta analisa data dari berbagai sumber daya komputer atau perangkat digital lainnya yang mencakup pada sistem komputer, jaringan komputer, jalur komunikasi dalam bentuk fisik maupun non fisik, serta berbagai media penyimpanan data yang dianggap layak untuk diajukan dalam persidangan sebagai alat bukti penunjang proses penyelesaian perkara pidana. Hal tersebut memperlihatan dua bidang keilmuan yakni ilmu komputer serta ilmu hukum disatukan dalam penerapannya oleh bidang ilmu digital forensik.[156]

Berdasarkan pendapat para ahli terkait terminologi digital forensik antara lain:

1) Menurut Muhammad Nuh Al-Azhar sebagai pakar forensik digital Polri menyatakan bahwa digital forensik adalah suatu bidang ilmu pengetahuan sekaligus teknologi komputer yang berorientasi pada kepentingan pembuktian hukum (*Pro Justice*), serta bertujuan untuk membuktikan kejahatan yang

[156] Synthiana Rachmie, *Op.Cit*, *Jurnal Litigasi*, 21 (1) April 2020, hlm 114

berteknologi tinggi atau computer crime secara ilmiah (*scientific*) sehingga bukti digital yang ditemukan dapat digunakan sebagai alat bukti yang sah dalam persidangan;[157]

2) Menurut Yudi Prayudi sebagai ahli digital forensik UII, menyatakan bahwa digital forensik merupakan suatu ilmu sekaligus metode untuk menemukan, mengumpulkan, mengamankan, menganalisis, menginterpretasi dan mempresentasikan barang bukti digital dalam rangka kepentingan proses penegakan hukum pidana dalam persidangan.[158]
3) Menurut Lazaridis, seorang Cyprus sebagai ahli *software engineering* senior bahwa digital forensik adalah ilmu dan metode untuk melakukan penemuan, validasi dan interpretasi bukti digital yang ditemukan pada perangkat elektronik yang digunakan dengan kejahatan komputer.[159]

Secara prinsipil, ilmu digital forensik memiliki 4 (empat) prinsip dasar, yaitu:

Untuk dapat melakukan penerapan ilmu digital forensik dalam proses penyidikan perlu pemahaman yang lebih dalam mengenai ilmu teknologi selain daripada ilmu hukum yang biasa diterapkan dalam proses pengadilan pidana. Penerapan ilmu digital forensik dibagi menjadi 4 (empat) yaitu:

---

[157] Muhammad Nuh Al-Azhar, *Digital Forensic Panduan Praktis Investigasi Komputer*. Jakarta: Salemba Infotek. 2012

[158] Asep Sudirman, Kerangka Kerja Digital Forensic Readiness pada sebuah Organisasi (Studi Kasus: PT Waditra Reka Cipta Bandung), *Cyber Security dan Forensik Digital*, 2 (2) November 2019, hlm 83

[159] Handrizal. Analisis Perbandingan Toolkit Puran File Recovery, Glary Undelete Dan Recuva Data Recovery Untuk Digital Forensik. *J-SAKTI: Jurnal Sains Komputer Dan Informatika*, 1 (1) 2017, hlm 84

1) Forensik Komputer yaitu penyidikan yang dilakukan terkait dengan data dan/atau aplikasi yang berada pada komputer tersebut yang didalamnya tercatat dalam berbagai berkas *log*. Sebagai contoh, aktivitas pengguna yang gagal masuk karena salah memasukkan password akan tercatat sebagai bagian dari upaya untuk melakukan penerobosan akses dengan cara *brute force password cracking*. Selain itu, aktivitas seperti pengguna memasukkan flash disk ke port USB juga tercatat dan dapat menjadi fokus dalam penyidikan komputer forensik.
2) Forensik Jaringan/Internet yaitu penyidikan yang dilakukan kepada data yang diperoleh berdasarkan pengamatan di jaringan. Contohnya, pengamat dapat mengamati lalu lintas data pada server-server yang diakses oleh seorang pengguna yang diduga melakukan penerobosan pada server tersebut. Perangkat khusus digunakan untuk melakukan penyadapan jaringan guna memantau dan mengumpulkan data terkait kejadian ini.
3) Forensik Aplikasi yaitu penyidikan yang dilakukan dengan penggunaan aplikasi tertentu. Aplikasi tersebut memiliki fungsi audit karena aplikasi tersebut terdapat fitur untuk meninggalkan jejak suatu perangkat. Penyidik dapat memanfaatkan catatan jejak tersebut, misalnya pada aplikasi email yang mencatat header email, untuk menelusuri kejadian yang terkait dengan email palsu atau email dengan maksud menyesatkan.
4) Forensik Perangkat (*Mobile Forensic*) yaitu penyidikan dengan tujuan untuk mendapatkan serta mengumpulkan data dan jejak kegiatan-kegiatan tertentu

dalam suatu perangkat digital.[160] Forensik jenis ini berkaitan dengan barang bukti elektronik seperti handphone dan smartphone. Pemeriksaan ini terfokus pada informasi digital yang tersimpan di perangkat tersebut, seperti panggilan masuk, panggilan keluar, SMS, e-mail, foto, dan video. Tujuan dari mobile forensik adalah untuk mengidentifikasi komunikasi antara pelaku kejahatan dan menganalisis data yang berkaitan dengan kejahatan yang terjadi.

5) *Image Forensic* yaitu forensik yang berkaitan dengan jenis barang bukti digital berupa file gambar. Jenis digital forensik ini sering dianalisis untuk mengetahui peralatan kamera digital yang digunakan untuk mengambil gambar tersebut dan juga dapat memeriksa waktu pengambilan gambar. Pemeriksaan ini dapat membantu dalam mengidentifikasi asal dan autentisitas gambar digital yang menjadi bukti dalam suatu kasus.[161]

Untuk terciptanya penerapan ilmu digital forensik yang komprehensif diperlukan 3 (tiga) komponen terangkai yang harus dipenuhi untuk penerapa ilmu yang berkualitas. Ketiga komponen tersebut yaitu:

1) Manusia (*People*), faktor kualitas manusia yang berpengaruh dalam proses penerapan ilmu digital forensik. Kualitas yang dibutuhkan tidak hanya mampu menggunakan computer namun diperlukan keahlian ilmu pengetahuan khusus dan pengalaman untuk dapat melakukan proses analisa menggunakan ilmu digital forensik;

[160] Budi Raharjo. *Op.Cit,* 12 (29) 2013, hlm 384
[161] M Qahar Awaka dan Alhadiansyah, *Op.Cit*, 9 (2) Oktober 2023, hlm 464

2) Peralatan (*Equipment*), perlunya beberapa perangkat/alat untuk menunjang proses identifikasi menggunakan digital forensik untuk mendapatkan petunjuk guna menerangkan suatu perkara;
3) Aturan (*Protocol*), dalam komponen aturan diperlukan pemahaman secara mendalam dari sisi ilmu hukum dan pengetahuan lain seperti pengetahuan teknologi informasi untuk menunjang penerapan ilmu dapat menjadi berkualitas dan dengan aturan pula dibutuhkan untuk proses menggali, mendapatkan, menganalisis, dan akhirnya menyajikan dalam bentuk laporan yang akurat.[162]

Ilmu digital forensik memiliki 4 (empat) prinsip dasar, yaitu (1) Data digital sebagai bukti tidak boleh dilakukan perubahan, karena keasliannya akan mempengaruhi kekuatan pembuktian hukum didalam persidangan; (2) Kompetensi orang ahli dalam melakukan analisa terhadap data digital karena akan berdampak pada tindakan yang dilakukan terhadap barang bukti data digital tersebut; (3) Terdapat standar operasional prosedur (SOP) secara teknis dan praktis mengenai langkah-langkah yang dilakukan terhadap media penyimpanan selama proses pemeriksaan terhadap data digital sebagai dasar perlakuan apabila dilakukan dikemudian hari oleh orang yang berbeda namun hasilnya akan sama dan dijamin keamanannya; (4)

[162] Ruci, Meiyanti, and Ismaniah. *Op.Cit*, 15 (2) September 2015, hlm 3

Tanggung jawab dari setiap orang yang terlibat dalam proses investigasi, pemeriksaan dan analisis dilakukan sesuai dengan ketentuan yang berlaku.[163]

Menurut Kemmish tahap yang akan dilakukan dalam pemeriksaan digital forensik untuk memeriksa barang bukti yang diperoleh dari suatu tindak pidana siber, yakni:

1) Identifikasi Bukti

Identifikasi barang bukti merupakan tahap utama dari forensik digital, dan identifikasi yang dilakukan pada tahap ini umumnya berupa identifikasi terkait dimana barang bukti tersebut berada, dimana barang bukti tersebut disimpan, dan bagaimana penyimpanan barang bukti tersebut harus dilakukan, sehingga data yang disimpan dalam bukti memiliki karakteristik yang sama.[164] Proses penyimpanan harus dilakukan menggunakan perangkat dan metode yang aman, agar bukti tidak mengalami kerusakan atau perubahan yang dapat mempengaruhi keabsahannya di persidangan. Penyimpanan bukti digital juga melibatkan proses membuat salinan cadangan atau *backup* dari data asli, sehingga apabila terjadi kehilangan atau kerusakan pada bukti digital, masih ada salinan yang dapat digunakan untuk keperluan penyidikan lebih lanjut. Selain itu, dalam proses penyimpanan bukti digital, pihak penyidik harus

[163] Ruuhwan, Imam Riadi, and Yudi Prayudi. Analisis Kelayakan Integrated Digital Forensics Investigation Framework untuk Investigasi Smartphone. *Jurnal Buana Informatika*, 7 (4) 2016, hlm 265

[164] Farol Medeline, Elis Rusmiati & Rully Herdita Ramadhani, Forensik Digital dalam Pembuktian Tindak Pidana Ujaran Kebencian di Media Sosial, *PAMPAS: Journal Of Criminal Law*, 3 (3) 2022, hlm 318

menjaga kerahasiaan dan integritasnya dengan ketat, sehingga bukti tersebut tidak dapat diakses atau dimanipulasi oleh pihak yang tidak berwenang. Seluruh langkah dalam proses identifikasi dan penyimpanan bukti digital harus dilakukan dengan cermat dan sesuai dengan standar digital forensik yang berlaku. Hal ini bertujuan untuk memastikan bahwa bukti yang ditemukan dapat diakui sebagai alat bukti yang sah dan dapat digunakan dalam proses persidangan untuk menuntut pelaku kejahatan yang terlibat dalam *cybercrime*.[165]

2) Analisis bukti digital

Pada tahap ini, bukti yang telah diperoleh dieksplorasi kembali dalam skenario terkait investigasi, termasuk memeriksa metadata. Biasanya, file memiliki metadata di mana informasi tentang file ditambahkan, seperti berapa kali file diedit, jumlah sesi pengeditan, nama komputer, berapa kali disimpan, di mana file dicetak, dan tanggal dan waktu itu diubah. "Kemudian, pada tahap ini juga dilakukan proses pemulihan dengan cara memulihkan file dan folder yang terhapus, memulihkan kata sandi, membuat ulang partisi, membuka format drive, membangun kembali halaman web yang dikunjungi, memulihkan email yang terhapus.[166]

3) Presentasi

[165] M Qahar Awaka dan Alhadiansyah, *Op.Cit,* 9 (2) Oktober 2023, hlm 464
[166] Farol Medeline, Elis Rusmiati & Rully Herdita Ramadhani, *Op.Cit*, 3 (3) 2022, hlm 319

Tahap presentasi adalah tahap di mana bukti yang ada divalidasi dan hubungannya dengan kasus yang ada. Pada tahap ini, hasil tes akan ditampilkan pada bukti yang relevan dengan kasus yang sedang diperiksa.[167]

Dalam hukum acara pidana yang berlaku di Indonesia, sistem pembuktian yang dianut adalah sistem pembuktian *negatief wettelijk bewijstheorie*, artinya untuk menjatuhkan hukuman, hakim harus terlebih dahulu memperoleh keyakinan berdasarkan alat bukti yang sah dan diatur dengan undang-undang. Hal ini sejalan dengan Pasal 183 Undang-Undang Nomor 8 Tahun 1981 tentang KUHAP, yang menyatakan bahwa dalam mengambil suatu putusan hakim harus dipidana berdasarkan sekurang-kurangnya 2 (dua) alat bukti yang sah dan atas dasar urusan.

Pembuktian, sebagai inti dari peradilan pidana, merupakan bagian penting dari peradilan pidana. Bukti menyangkut apakah terdakwa yang muncul di persidangan adalah orang yang tepat dan melakukan perbuatan yang dituduhkan. Dengan alat bukti, nasib terdakwa akan ditentukan dan diajukan di persidangan berdasarkan alat bukti yang ditentukan oleh undang-undang. Jika hasil penggunaan alat bukti yang diakui undang-undang sebagai alat bukti tidak cukup untuk membuktikan bahwa terdakwa bersalah atas terdakwa, terdakwa dibebaskan dari hukuman. Namun apabila alat bukti yang diatur dalam Pasal 184 KUHAP dapat membuktikan kesalahan terdakwa, maka terdakwa akan dinyatakan “bersalah” dan terdakwa akan divonis bersalah.

[167] *Ibid*

Hasil penyidikan berupa pemeriksaan forensik digital yang diuraikan di atas pada akhirnya akan membantu hakim dalam mengambil keputusan dengan mengevaluasi dan berdasarkan kesesuaian alat bukti yang diajukan dan memeriksa hubungannya dengan setiap unsur pasal yang didakwakan. Hal ini berkaitan dengan Pasal 183 KUHAP yang menyatakan bahwa keyakinan hakim didasarkan pada alat bukti yang sah. Hasil forensik digital menghasilkan barang bukti juga sejalan dengan tujuan alat bukti itu sendiri, yaitu untuk mencari dan memperoleh kebenaran materiil, bukan sekedar mencari kesalahan.[168]

Sebagai ilmu yang mendasari hukum acara pidana, hasil pemeriksaan forensik digital di ruang sidang biasanya dituangkan dalam surat. Hasil forensik digital forensik berupa surat antara lain BAP laboratorium forensik, BAP ahli, laporan uji forensik digital (misalnya *visum et repertum*). Menurut Pasal 187 b KUHAP, hasil pemeriksaan forensik digital berupa BAP laboratorium forensik dan BAP ahli forensik harus dibuat sesuai dengan ketentuan peraturan perundang-undangan atau undang-undang. Hal ini menunjukan bahwa hasil uji forensik digital menghasilkan surat dari seorang pejabat tentang suatu hal yang terdapat dalam pemerintahan yang menjadi tanggung jawabnya dan dimaksudkan untuk membuktikan suatu hal atau keadaan.[169]

[168] Farol Medeline, Elis Rusmiati & Rully Herdita Ramadhani, *Op.Cit*, 3 (3) 2022, hlm 322

[169] Christloy Totota Karo-Karo & Handar Subhandi Bakhtiar, Analisis Kasus Peretasan Media Sosial melalui Digital Forensik sebagai Upaya Preventif Penyidik Mencegah Kejadian Salah Tangkap (Studi Kasus Peretasan Ravio Patra), *TERANG : Jurnal Kajian Ilmu Sosial, Politik dan Hukum*, 1 (4) 2024, hlm 182

Hasil forensik digital di persidangan pengadilan tidak hanya menghasilkan bukti surat, tetapi juga bukti keterangan ahli. Ahli forensik digital harus memahami dan mengikuti ilmu komputer dan prosedur terkait hukum yang diakui secara nasional dan internasional. Ahli forensik digital juga harus berpengalaman dalam teori yang terkait dengan bukti digital yang ditemukan dan memahami penggunaan perangkat lunak atau aplikasi forensik, sehingga barang bukti digital dapat diuji dengan baik dan akurat.

Berdasarkan Pasal 43 (5) huruf j UU ITE, dalam penyidikan cybercrime pada ranah pelibatan ahli yang mana berketentuan secara yuridis untuk meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik. Artinya ahli forensik digital berarti seseorang dengan keahlian tertentu di bidang teknologi informasi yang bertanggung jawab secara akademis dan praktis tentang pengetahuan itu.[170]

Peran dan fungsi forensik digital dalam hal ini dapat dilihat dari tahap investigasi. Selama fase penyidikan, Kepolisian menggunakan forensik digital untuk menemukan dan mengumpulkan barang bukti yang ada. Peran dan fungsi forensik digital dalam kasus cybercrime juga dapat dilihat dari alat bukti yang tersedia. Pada tahap penyidikan, Kepolisian tetap harus berpegang teguh pada asas *unus testis nullus testis* atau satu saksi bukan saksi yang memiliki maksud yaitu seminimalnya terdapat dua alat bukti. Asas *unus testis nullus testis* ini bisa menjelaskan bahwa jika terdapat suatu penyidikan dan kemudian hanya memiliki satu saksi maka dinyatakan batal demi

[170] Pasal 43 (5) huruf j Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

hukum, hal ini juga disebutkan dalam Pasal 184 KUHAP menjelaskan bahwa pembuktian sekurang-kurangnya dua alat bukti.[171] Alat bukti ini yang disebutkan dalam pasal tersebut untuk membuktikan unsur-unsur bahwa telah terjadinya tindak pidana kejahatan siber.

Sehingga dapat dilihat bagaimana Peran digital forensik dalam menjadi alat bantu pihak Kepolisian pada kedudukannya adalah cukup penting untuk menjadi dasar pertimbangan ilmiah dalam melakukan penetapan tersangka. Pemeriksaan forensik digital terhadap barang bukti terkait tindak pidana cybercrime akan memandu penyidik dari tahap pemeriksaan awal hingga menemukan tersangka pelaku cybercrime. Forensik digital akan berperan dalam menemukan pelaku dan merekonstruksi perilaku. Forensik digital dalam proses forensik akan lebih bertanggung jawab karena merupakan bentuk penerapan teknik ilmiah dan menganalisis bukti yang ada.

Secara tinjauan teoritis terhadap fungsional digital forensik pada tahap penyidikan dalam mengungkap kasus cybercrime berimplikasi pada sebuah prinsip yang paling terkenal adalah prinsip pertukaran data, Locard menyebutkan bahwa "*every contact leaves a trace*" yang artinya setiap kontak akan meninggalkan jejak. Prinsip dasar Locard inilah yang menjadi acuan bahwa setiap sesuatu yang bersentuhan pasti akan meninggalkan suatu jejak sekecil apapun jejak tersebut dan jejak-jejak itulah yang akan dikumpulkan, kemudian dianalisis sehingga menjadi sebuah petunjuk yang

[171] Maulana Daffa Ilhami dan Wiwik Afifah, Mengukir Sifat Unus Testis Terhadap Pembuktian Tindak Pidana Seksual, *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, 3 (2) Mei-Agustus 2023, hlm 1634

akan mengerucut kepada siapa yang memiliki jejak tersebut yang mana hal ini berimplikasi pada upaya penyidikan terhadap kejahatan cybercrime yang tidak mustahil memiliki sebuah jejak dengan diungkapkan dengan bantuan sebuah bidang ilmu yaitu digital forensik.

C. Problematika Hukum yang Terjadi dalam Fungsional Digital Forensik pada Proses Penyidikan Tindak Pidana Cybercrime

Hukum pidana merupakan salah satu sarana yang dimiliki oleh negara dalam menjalankan kewajiban memberikan perlindungan pada hak setiap warga negara untuk mendapatkan rasa aman terutama terhadap ancaman terjadinya kejahatan. Jika dibandingkan dengan hukum yang lainnya, hukum pidana ini memiliki karakteristik yang khas, terletak pada adanya sanksi yang sangat tegas yaitu berupa nestapa.[172] Oleh sebab itu, sistem hokum pidana harus selalu direevaluasi, direkonstruksi, diharmonisasikan dan diaktualisasikan secara cermat dan tepat, melalui pemahaman dan pemikiran yang utuh, agar di satu sisi handal dalam mengantisipasi perkembangan kejahatan.

Hukum pidana saat ini dibutuhkan dalam menyelesaikan kejahatan yang semakin berkembang. Dalam hal ini misalnya tindak pidana cyber crime seiring dengan berkembangnya teknologi. Pelaku tindak pidana cyber crime semakin pintar dalam melakukan aksinya, bahkan menghilangkan barang bukti agar tidak dapat diketahui.

[172] Herlyanty Bawole, Perlindungan Hukum Bagi Korban Dalam Sistem Peradilan Pidana, *Lex Et Societatis*, IX (3) July-September 2021, hlm 20

Hal tersebut dikarenakan barang bukti elektronik sangat mudah untuk diubah, dihapus dan dirusak.

Dunia internet merupakan dunia digital yang terdiri dari dunia komunikasi dengan proses yang jauh lebih "virtual" (maya). Identitas seorang individu sangatlah sulit untuk diketahui di dalam dunia digital ini karena sifatnya lebih global. Disini tidak ada sidik jari yang merupakan ciri khas dari setiap orang. Atau tidak ada darah yang dapat dianalisa. Meski demikian proses kejahatan di dalamnya bukannya tidak berbekas sama sekali. Proses komunikasi dan komputasi digital juga bisa menghasilkan atribut khas, yaitu "benda digital".[173]

Pertukaran atribut khas juga terjadi dalam proses tindak pidana dunia maya ini, meskipun wujudnya adalah berupa benda digital. Contoh benda-benda digital seperti misalnya sebuah file dokumen, log akses, *e-mail header* dan *log*, medan elektromagnet pada piringan *harddisc*, alamat IP, dan masih banyak lagi. Benda-benda ini tidak bisa disentuh, diraba, dibaui, dirasa. Benda ini hanya bisa dilihat, diukur satuannya, dan diproses lebih lanjut juga dengan menggunakan komputer. Tetapi meskipun demikian bukti-bukti ini sangat penting dan cukup kuat untuk dapat membuktikan sebuah kejahatan berupa cybercrime.[174]

Secara sederhana contohnya adalah dalam sebuah *e-commerce web server* yang memiliki sistem logging setiap kali server tersebut diakses. Melalui *log* ini, semua

[173] Sahuri Lasmadi, Pengaturan Alat Bukti dalam Tindak Pidana Dunia Maya, *Jurnal Ilmu Hukum Jambi*, 5 (2) Oktober 2014, hlm 11

[174] *Ibid*

orang yang mengakses server akan terekam dengan jelas keterangannya, biasanya berupa alamat IP, *port-port* komunikasi yang digunakan, aktifitasnya di dalam *server* tersebut, dan banyak lagi. Dari *log* ini Anda dapat mengetahui alamat IP berapa yang melakukan "*carding*".[175] Kemudian dapat dicari ISP dari pemilik alamat IP ini. Setelah menghubungi ISP yang bersangkutan dan menyertakan bukti-bukti aktifitasnya, maka tidak menutup kemungkinan sudah dekat kepada pelaku. Itupun jika pelaku tersebut tidak "berkeliling dunia" dulu memanfaatkan celah-celah komputer orang lain untuk melakukan kejahatannya.

Dunia digital memang sangat luas cakupannya. Sebuah kelompok kerja yang bernama *Standard Working Group on Digital Evidence* (SWGDE) mendefinisikan bukti digital sebagai semua informasi yang memiliki nilai pembuktian yang kuat yang disimpan atau ditransmisikan dalam bentuk sinyal-sinyal listrik digital.[176] Oleh karena itu, data yang sesuai dengan definisi ini biasanya adalah berupa kumpulan logika digital yang membentuk sebuah informasi, termasuk teks dokumen, video, audio, file gambar, alamat-alamat komunikasi digital, dan masih banyak lagi.

Perangkat yang menggunakan format data digital untuk menyimpan informasi memang sangat banyak. Perangkat yang memiliki potensi untuk menyimpan bukti digital selain komputer, jaringan komputer dan jaringan, juga terdapat perangkat lainnya seperti perangkat ponsel, smart card, bahkan *microwave* juga bisa berperan

[175] Mehda Zuraida, Credit Card Fraud (Carding) dan ampaknya Terhadap Perdagangan Luar Negeri Indonesia, *Jurnal Analisis Hubungan Internasional*, 4 (1) Maret 2015, hlm 1636

[176] Scientific Working Group on Digital Evidence, Best Practices for Remote Collection of Digital Evidence from an Endpoint, *SWGDE Documents*. Version 2.0 November 2022, hlm 3

sebagai sumber bukti digital. Berdasarkan pertimbangan inilah maka dibuat tiga kategori besar untuk sumber bukti digital, yaitu:

1) *Open komputer systems*

Perangkat yang masuk dalam kategori jenis ini adalah perangkat komputer. Sistem yang memiliki media penyimpanan, keyboard, monitor, dan perangkat yang biasanya ada di dalam komputer masuk dalam kategori ini. Seperti misalnya laptop, desktop, server, dan perangkat sejenis lainnya. Perangkat yang memiliki sistem media penyimpanan yang semakin besar dari waktu ke waktu ini merupakan sumber yang kaya akan bukti digital. Sebuah file yang sederhana saja pada sistem ini dapat mengandung informasi yang cukup banyak dan berguna bagi proses investigasi. Contohnya detail seperti kapan file tersebut dibuat, siapa pembuatnya, seberapa sering file tersebut diakses, dan informasi lainnya semua merupakan informasi penting.

2) *Communication systems*

Sistem telepon tradisional, komunikasi wireless, internet, jaringan komunikasi data, merupakan salah satu sumber bukti digital yang masuk dalam kategori ini. Sebagai contoh, jaringan internet membawa pesan-pesan dari seluruh dunia melalui e-mail. Kapan waktu pengiriman e-mail ini, siapa yang mengirimnya, melalui mana pengirim mengirim, apa isi dari e-mail tersebut merupakan bukti digital yang sangat penting dalam investigasi.

3) *Embedded computer systems*

Perangkat telepon bergerak (ponsel), *Personal Digital Assistant* (PDA), *smart card*, dan perangkat-perangkat lain yang tidak dapat disebut komputer tapi memiliki sistem komputer dalam bekerjanya dapat digolongkan dalam kategori ini. Hal ini dikarenakan bukti-bukti digital juga dapat tersimpan di sini. Sebagai contoh, sistem navigasi mobil dapat merekam ke mana saja mobil tersebut berjalan. Sensor dan modul diagnosa yang dipasang dapat menyimpan informasi yang dapat digunakan untuk menyelidiki terjadinya kecelakaan, termasuk informasi kecepatan, jauhnya perjalanan, status rem, posisi persneling yang terjadi dalam lima menit terakhir. Semuanya merupakan sumber-sumber bukti digital yang sangat berguna.[177]

Akan tetapi, bukti digital tersebut terbentur dalam hukum pembuktian di Indonesia. Posisi hukum pembuktian seperti biasanya akan berada dalam posisi dilematis sehingga dibutuhkan jalan kompromistis. Di satu pihak hukum harus selalu dapat mengikuti perkembangan zaman dan teknologi, sehingga perlu pengakuan hukum terhadap berbagai perkembangan teknologi digital untuk berfungsi sebagai alat bukti di pengadilan. Akan tetapi, di lain pihak kecenderungan terjadi manipulasi penggunaan alat bukti digital oleh pihak yang tidak bertanggung jawab menyebabkan hukum tidak bebas dalam mengakui alat bukti digital tersebut. Bahkan jika mengikuti

[177] Imam Riadi dan Ade Kurniawan, *Forensik Jaringan dan Cloud*, Diadra Kreatif Penerbit, Sleman, Cetakan Kedua, 2020, hlm 162-169

teori klasik dalam hukum pembuktian yang disebut dengan hukum alat bukti terbaik (*best evidence rule*), maka suatu alat bukti digital sulit diterima dalam pembuktian.[178]

The best evidence rule mengajarkan bahwa suatu pembuktian terhadap isi yang substansial dari suatu dokumen atau rekaman harus dilakukan dengan membawa ke pengadilan dokumen atau rekaman asli tersebut. Kecuali jika dokumen atau rekaman tersebut memang tidak ada, dan ketidakberadaannya bukan terjadi karena kesalahan yang serius dari pihak yang membuktikan. Dengan demikian menurut doktrin ini, fotokopi (bukan asli) dari suatu surat tidak mempunyai kekuatan pembuktian di pengadilan. Demikian juga dengan bukti digital, seperti e-mail, surat dengan mesin faksimile, tanda tangan elektronik, tidak ada aslinya ke pengadilan sehingga hal ini mengakibatkan permasalahan hukum yang serius dalam bidang hukum pembuktian. Pemakaian internet dalam melakukan transaksi elektronik dewasa ini berkembang dengan pesat sehingga sektor hukum pun, termasuk hukum pembuktian, diminta untuk turun tangan sehingga lalu lintas bisnis, *security* dan sektor kegiatan lain melalui internet dapat tercipta ketertiban dan kepastian, di samping tercapai pula unsur keadilan bagi para pihak.[179]

Bukti elektronik baru dapat dinyatakan sah apabila menggunakan sistem elektronik yang sesuai dengan peraturan yang berlaku di Indonesia. Suatu bukti elektronik dapat memiliki kekuataan hukum apabila informasinya dapat dijamin

[178] Munir Fuady, *Teori Hukum Pembuktian (Pidana dan Perdata),* Bandung: Citra Aditya Bakti, 2006, hlm 151.

[179] *Ibid*. hlm 152

keutuhannya, dapat dipertanggungjawabkan, dapat diakses, dan dapat ditampilkan sehingga menerangkan suatu keadaan.[180] Berdasarkan hal-hal tersebut di atas, maka dapat dilihat bahwa tidak ada alasan untuk menolak bukti digital sebagai alat bukti yang sah dalam hukum pembuktian di Indonesia. Selain terjamin kevalidan nya, juga mengingat fungsi dari bukti digital itu sendiri yang dapat membuktikan kebenaran materil dari suatu tindak pidana yang dilakukan. Sehingga dapat terciptalah kepastian hukum bagi masyarakat Indonesia. Oleh karena itu, dengan disahkannya Undang-Undang Informasi dan Transaksi Elektronik maka bukti elektronik ini telah diakui sebagai alat bukti yang sah sehingga dapat digunakan dalam melakukan pembuktian.

Hal ini dapat dilihat dalam pengaturan Pasal 44 yang menentukan bahwa alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut:

1) Alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan;
2) Alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).[181]

Jadi di sini dapat dilihat telah terjadi perluasan alat bukti. Artinya sekarang ini dalam penanganan tindak pidana dunia maya, alat bukti yang digunakan tidak hanya alat bukti yang diatur dalam KUHAP tetapi juga telah diakui alat bukti yang lain yaitu

[180] Adi Darmawansyah, Andry Dwiarnanto, Irwan Putra Satriyawan, Istiqomah, *Op.Cit*, 3 (1) Juni 2024, hlm 422

[181] Pasal 44 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

alat bukti berupa informasi elektronik dan dokumen elektronik. Secara asas legalitas berarti menuntut adanya ketentuan peraturan perundang-undangan ditetapkan terlebih dahulu dengan sah. Setelah itu perbuatan yang dilakukan oleh manusia yang terbukti memenuhi unsur-unsur tindak pidana dapat dijatuhi pidana. Dengan demikian dalam asas ini terseimpul bahwa peraturan perundang-undangan tidak dapat diberlakukan surut/mundur (retroaktif), agar hal ini menjadi jaminan kepastian hukum.[182] UU ITE juga menganut asas legalitas (sebagai asas fundamental dalam hukum pidana), yaitu sebagaimana tampak dalam Pasal 54 ayat (1) bahwa undang-undang ini mulai berlaku pada tanggal diundangkannya. Artinya, ketentuan pidana yang ada dalam UU ITE akan dilaksanakan setelah diberlakukan.

Agar Informasi dan Dokumen Elektronik dapat dijadikan alat bukti hukum yang sah, UU ITE mengatur bahwa adanya syarat formal dan syarat materiil yang harus dipenuhi. Syarat formal diatur dalam Pasal 5 UU ITE, yaitu bahwa Informasi atau Dokumen Elektronik bukanlah dokumen atau surat yang menurut perundang-undangan harus dalam bentuk tertulis. Sedangkan syarat materiil diatur dalam Pasal 6, Pasal 15, dan Pasal 16 UU ITE, yang pada intinya Informasi dan Dokumen Elektronik harus dapat dijamin keautentikannya, keutuhannya, dan ketersediaannya. Untuk menjamin terpenuhinya persyaratan materiil yang dimaksud, dalam banyak hal dibutuhkan digital forensik.[183]

---

[182] Herdino Fajar Gemilang & Handar Subhandi Bakhtiar, Meninjau Ilmu Digital Forensik Terhadap Bukti Elektronik dalam Tindak Pidana Informasi dan Transaksi Elektronik, *Perahu (Penerangan Hukum): Jurnal Ilmu Hukum*, 12 (2) September 2024, hlm 49

[183] T. Arifiyadi & J. Sitompul, *Gadgetmu, Harimaumu*. Lentera Hati. 2015

Dalam melakukan pencarian bukti-bukti digital, seorang ahli forensik tersebut harus memahami dan mengikuti prosedur-prosedur mengenai ilmu komputer dan ilmu hukum yang diakui secara nasional maupun internasional, selain itu ahli forensik juga perlu mendalami teori-teori yang berkaitan dengan bukti digital yang ditemukan baik secara online maupun yang terdapat dalam suatu perangkat, dan ahli forensik harus memahami penggunaan software atau aplikasi forensik untuk mencari bukti-bukti digital tersebut dengan tepat dan akurat. Sehingga ahli forensik harus memiliki ilmu yang berkompeten secara khusus dan memiliki pengalaman dalam hal melakukan investigasi ilmu digital forensik tersebut.

Digital forensik secara keilmuan menjadi elemen penting sebagai *support system* penegakan hukum berupa penyidikan cybercrime guna mencapai alat bukti yang autentik untuk dimunculkan pada proses persidangan. Namun secara yuridis, digital forensik memiliki problematika secara ketentuan yuridis dalam mengakomodir teknis pelaksanaan secara formil dengan sebuah produk hukum yang lebih spesifik.

Implementasi digital forensik dalam penyidikan tindak pidana cyber crime saat ini belum diatur secara spesifik dalam peraturan perundang-undangan. Pengaruhnya adalah proses penyidikan belum memiliki landasan hukum dan pedoman yang jelas untuk menerapkan digital forensik dalam penyidikan kasus-kasus tersebut. Peraturan UU ITE yang ada saat ini hanya mengatur mengenai alat bukti informasi dan transaksi elektronik, bukan mengenai digital forensik secara menyeluruh. Pentingnya pengaturan terkait digital forensik dalam pembuktian berimplikasi pada aspek-aspek yang melekat pada hasil dari proses penyidikan cybercrime berupa:

1) Sebagai pedoman bagi aparat penegak hukum dalam menangani barang bukti dan alat elektronik yang terkait dengan tindak pidana cyber crime. Dengan pengaturan yang jelas, aparat penegak hukum dapat menggunakan digital forensik secara efektif dan tepat dalam proses penyidikan dan pengumpulan bukti.
2) Meningkatkan validitas, realibilitas serta kredibilitas barang bukti dan alat bukti elektronik yang digunakan dalam persidangan. Dengan adanya pengaturan yang sesuai, keabsahan dan integritas bukti digital dapat dipertanggungjawabkan dengan jelas di hadapan pengadilan.
3) Menghindari terjadinya kekosongan yuridis atau kekosongan hukum dalam pengaturan tata cara pembuktian tindak pidana siber (cybercrime). Dengan adanya ketentuan yang mengatur tentang digital forensik, akan tercipta kerangka hukum yang lengkap dan dapat mendukung efektivitas penanganan kasus cyber crime.

Kerangka hukum yang ada saat ini, meskipun telah memberikan landasan untuk penanganan kasus kejahatan siber, masih memerlukan pembaruan untuk mengakomodasi perkembangan teknologi terbaru. UU ITE dan perubahannya belum sepenuhnya mampu mengantisipasi kompleksitas kejahatan siber kontemporer. Interpretasi hukum terhadap bukti digital juga masih menjadi tantangan, terutama dalam menentukan admisibilitas dan bobot pembuktiannya di pengadilan. Standar pembuktian yang tinggi dalam sistem peradilan pidana Indonesia terkadang sulit dipenuhi dalam kasus kejahatan siber, mengingat sifat bukti digital yang mudah

dimanipulasi[184], bahkan yang lebih inheren ada pada fasilitas hukum yang sistemik untuk melakukan upaya digital forensik.

Kendala dalam pengumpulan dan analisis bukti digital menjadi aspek kritis dalam proses pembuktian. Volatilitas bukti digital mengharuskan penyidik untuk bertindak cepat dan tepat dalam mengamankan bukti, namun hal ini sering terkendala oleh prosedur hukum yang memerlukan waktu, seperti proses mendapatkan surat perintah penggeledahan. Menjaga integritas bukti digital melalui chain of custody yang ketat juga menjadi tantangan tersendiri, mengingat kemudahan dalam memanipulasi data digital. Analisis bukti yang kompleks, terutama dalam kasus yang melibatkan volume data yang besar, memerlukan *tools* forensik canggih dan keahlian khusus yang tidak selalu tersedia.[185]

Di balik kontribusi positifnya, UU ITE juga menghadapi sejumlah keterbatasan yang membatasi efektivitas penyidikan tindak pidana siber. UU ITE sering kali dianggap belum cukup adaptif terhadap perkembangan teknologi, seperti penggunaan kecerdasan buatan atau teknologi *blockchain* dalam kejahatan siber, sehingga penyidik sering kali harus berinovasi di luar kerangka hukum yang ada. Secara global, UU ITE mengamanatkan kerja sama dengan penyedia layanan, realisasi di lapangan sering kali terkendala oleh perbedaan yurisdiksi hukum internasional. Sebagai contoh, penyedia platform global yang berbasis di luar negeri tidak selalu mematuhi permintaan data dari

[184] Nurul Aini dan Fauziah Lubis, Tantangan Pembuktian dalam Kasus Kejahatan Siber, *Judge: Jurnal Hukum*, 5 (2) 2024, hlm 58

[185] *Ibid*

aparat penegak hukum Indonesia, terutama jika tidak ada perjanjian bilateral atau multilateral yang relevan. Hal ini memperlambat proses penyidikan dan mengurangi peluang untuk mengungkap pelaku kejahatan.

Kerangka teori penyidikan pidana menekankan pentingnya regulasi hukum yang jelas, adaptif, dan implementatif untuk mendukung proses penyidikan. Dalam konteks ini, UU ITE dikategorikan sebagai regulasi yang memberikan fondasi dasar, namun memerlukan pengembangan untuk mengikuti dinamika kejahatan siber yang terus berkembang. Menurut teori penyidikan, hukum pidana yang efektif harus mencakup aturan substansial (materi tindak pidana) dan aturan prosedural (cara penanganan perkara).[186]

Dalam ruang lingkup UU ITE, meskipun aturan substansial sudah memadai, aturan prosedural masih kurang mendalam, khususnya dalam upaya digital forensik. Hal ini kemudian menyatakan bahwa penyidikan tindak pidana lintas batas membutuhkan kolaborasi internasional yang kuat. Belum adanya standarisasi global dalam prosedur forensik digital dapat menimbulkan masalah dalam admisibilitas bukti di pengadilan.[187] Perbedaan standar dan praktik antar negara atau bahkan antar lembaga penegak hukum dapat mempengaruhi kualitas dan keabsahan bukti yang dikumpulkan. Untuk mengatasi hal ini, diperlukan upaya harmonisasi standar forensik digital di

[186] Eko Nurisman, Risalah Tantangan Penegakan Hukum Tindak Pidana Kekerasan Seksual Pasca Lahirnya Undang-Undang Nomor 12 Tahun 2022*, Jurnal Pembangunan Hukum Indonesia*, 4 (2)Mei 2022, hlm 173.

[187] Victor R Kebande, Nickson M Karie and H.s. Venter. A Generic Digital Forensic Readiness Model for BYOD using Honeypot Technology, *2016 IST-Africa Week Conference*, Durban, South Africa, 2016, hlm 2

tingkat internasional. Organisasi seperti INTERPOL dan UNODC dapat berperan dalam mengembangkan dan mempromosikan best practices dalam forensik digital. Pelatihan dan sertifikasi bagi penyidik forensik digital juga perlu ditingkatkan untuk menjamin kualitas dan profesionalisme dalam penanganan bukti digital.[188]

Dalam hal ini, UU ITE belum sepenuhnya memfasilitasi kerja sama global yang efektif, karena ketergantungannya pada mekanisme tradisional seperti *Mutual Legal Assistance* (MLA), yang cenderung lamban. Sebagai perbandingan, beberapa negara maju telah mengadopsi perjanjian internasional, seperti *Budapest Convention on Cybercrime*[189], yang dapat mempercepat proses investigasi serta menghasilkan hasil yang akurat dan autentik dalam fungsional digital forensik.

Untuk memperkuat efektivitas UU ITE, reformasi hukum yang mengadopsi standar internasional dan pengaturan prosedural yang lebih teknis diperlukan dalam mengakomodir metode digital forensik pada proses penyidikan cybercrime. Dengan demikian, kerangka hukum Indonesia dapat menjadi lebih responsif terhadap tantangan kejahatan siber modern dan mendukung aparat penegak hukum dalam menjalankan tugasnya secara efisien.

Secara tinjauan komparatif, peneliti mencoba melaksanakan analisa perbandingan dengan situasi dan kondisi sistem fungsional digital forensik dalam

[188] Cameron S.D. Brown, Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, Australian National University, *International Journal of Cyber Criminology*, 9 (1) 2015

[189] Chat Le Nguyen dan Golman Wilfred, Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries: 'Law on the Books' vs 'Law in action', *Computer Law & Security Review, Elsevier*, (40) April 2021, hlm.105523.

koridor penegakan hukum di negara lain guna mencapai sebuah konsep hukum ideal untuk mengakomodir digital forensik dalam penyidikan cybercrime di wilayah hukum Indonesia.

1. Inggris

   Kerangka hukum dan kebijakan untuk forensik digital di Inggris mencakup berbagai kebijakan Parlemen, undang-undang, yurisprudensi, dan pedoman profesional. Undang-undang utama meliputi Undang-Undang Kepolisian dan Bukti Pidana tahun 1984, Undang-Undang Prosedur Pidana dan Investigasi tahun 1996, Undang-Undang Perlindungan Data tahun 2018, Undang-Undang Kekuasaan Investigasi tahun 2016, dan Undang-Undang Pengaturan Kekuasaan Investigasi tahun 2000. Undang-undang ini mengatur kewenangan penggeledahan dan penyitaan, aturan pengungkapan, perlindungan privasi, dan kewenangan pengawasan yang relevan dengan investigasi digital. Prinsip-prinsip penting juga telah ditetapkan melalui yurisprudensi, seperti aturan pembuktian mengenai praduga keandalan bukti digital dan otentikasi bukti media sosial. Di sisi kebijakan, Panduan Praktik Berlaku ACPO memberikan prinsip-prinsip umum, sementara prosedur yang lebih rinci dapat ditemukan di sumber-sumber seperti Kode Praktik Regulator Ilmu Forensik. Prinsip-prinsip utama meliputi menjaga integritas data asli, membangun proses lacak balak yang kuat, memastikan kompetensi staf, dan memelihara jejak audit yang terperinci. Badan-badan profesional seperti Regulator Ilmu Forensik dan Kejaksaan Agung juga mengeluarkan panduan

prosedural bagi para praktisi. Kepatuhan terhadap kerangka hukum dan kebijakan yang multifaset ini sangat penting bagi investigasi forensik digital agar dapat menghasilkan bukti yang andal dan dapat diterima sekaligus melindungi hak-hak individu sekaligus melindungi hak-hak individu.[190]

2. Meksiko dan Uni Eropa

Di Meksiko dan Uni Eropa, praktik forensik digital digunakan untuk menyelidiki kejahatan dan mengumpulkan bukti digital. Namun, terdapat beberapa perbedaan dalam cara pelaksanaan forensik digital di masing-masing wilayah. Meksiko dan Uni Eropa memiliki undang-undang yang mengatur pengumpulan dan penggunaan bukti digital dalam investigasi kriminal. Di Meksiko, Kitab Undang-Undang Hukum Acara Pidana dan Undang-Undang Federal tentang Pemeliharaan Bukti menyediakan kerangka hukum untuk forensik digital. Di Uni Eropa, Peraturan e-Bukti digunakan untuk mengakses bukti elektronik lintas batas. Praktik forensik digital di Meksiko dan Uni Eropa mematuhi standar teknis yang diakui secara internasional, seperti yang ditetapkan oleh *the International Organization for Standardization* (ISO) dan *the National Institute of Standards and Technology* (NIST) di Amerika Serikat.

[190] Stephen Mason & Daniel Seng, *Electronic Evidence*, published by the Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 4th ed. 2017. hlm 125-375

Uni Eropa telah membentuk Pusat Kejahatan Siber Eropa (th*e European Cybercrime Centre*/ EC3) untuk memfasilitasi kerja sama antar lembaga penegak hukum. Di Meksiko, Unit Investigasi Kejahatan Siber (UICIB) bekerja sama dengan mitra internasional untuk menyelidiki kejahatan siber.[191]

Tantangan dan kontradiksi dalam forensik digital pada lingkup konstruksi hukum untuk menangani bukti digital ini sangat banyak dan kompleks. Meningkatnya volume dan keragaman bukti digital, kurangnya standardisasi dan personel yang berkualifikasi, tuntutan kerangka hukum yang terus berkembang, serta implikasi etika dan sosialnya, semuanya membutuhkan perhatian dan investasi yang berkelanjutan. Lembaga penegak hukum perlu selalu meningkatkan kemampuan mereka untuk menyelidiki kejahatan siber secara efektif guna melindungi masyarakat dari ancaman digital. Tetap mengikuti perkembangan teknologi sangat penting bagi penyidik forensik digital yang menangani kasus kejahatan siber.

Optimalisasi fungsional digital forensik secara sistematis dan legitimatif bukan tanpa kompromi, hal ini berdasarkan pada sifat urgensitas negara untuk melindungi aset siber pemerintah dan melindungi lalu lintas siber masyarakat dari kejahatan siber yang saat ini semakin berkembang dan berindikasi dapat merusak stabilitas keamanan negara, politik, perekonomian, sosial, bahkan bisa sampai memecah belah keutuhan bangsa dengan kejahatan yang menjurus pada radikalisme, propaganda, terorisme

[191] Naeem Allah Rakha, Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations, *Mexican Law Review,* 16 (2) Juni 2024

dengan memanfaatkan media siber yang sudah menjadi atensi tinggi masyarakat dalam melakukan segala kegiatan di dunia siber.

Secara efektivitas, digital forensik sangat mengakomodir keberhasilan penegakan hukum terhadap cybercrime yang memiliki kesulitan yang sangat kompleks. Digital forensik dapat menjadi sebuah jawaban atas impresi dan dogma oleh circle pelaku cybercrime bahwa kejahatan mereka di media siber tidak akan mudah ditaklukan oleh penegak hukum dalam mendapatkan bukti-bukti kejahatan atas subjek hukum yang melakukan. Artinya dengan digital forensik menjadi representasi teori *Locard's Exchange* bahwa "*every contact leaves a trace*" yang artinya setiap kontak akan meninggalkan jejak. Prinsip dasar Locard inilah yang menjadi acuan bahwa setiap sesuatu yang bersentuhan pasti akan meninggalkan suatu jejak sekecil apapun jejak tersebut dan jejak-jejak itulah yang akan dikumpulkan, kemudian dianalisis sehingga menjadi sebuah petunjuk yang akan mengerucut kepada siapa yang memiliki jejak tersebut.

Secara teori Locard yang mana teori tersebut meskipun tercipta pada era kejahatan konvensional namun teori Locard dapat dimaknai dan terepresentasi pada sebuah kejahatan siber yang sekalipun pelaku sangat lihai secara sarat enkripsi dan bersifat anonimitas sangat sulit untuk ditembus dalam menemukan bukti-bukti serta mengidentifikasi pelaku cybercrime tetap akan ada celah bagi penegak hukum untuk memecahkan kasus tersebut dengan mengurai secercah jejak kejahatan yang pasti ada dan tertinggal.

Seperti yang dikutip dari Teori Locard yang dijelaskan oleh Paul L. Kirk (1953) dalam bukunya yang berjudul "*Crime Investigation: Physical evidence and the police laboratory*" yang menyatakan bahwa "*Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value*".[192]

Artinya "kemanapun dia melangkah, apapun yang dia sentuh, apapun yang dia tinggalkan, tanpa disadari, akan menjadi saksi bisu untuknya. Tidak hanya sidik jari atau jejak kakinya, tapi rambutnya, serat pakaian dari bajunya, kaca yang dipecahkan, jejak alat yang tertinggal, cat yang digores, darah atau sperma yang dia simpan atau dia kumpulkan, dan sebagainya, menjadi saksi bisa terhadapnya, ini adalah bukti yang tidak akan pernah lupa, tidak akan keliru disaat kejadian, tidak akan hilang karena tidak ada saksi mata. Ini adalah bukti yang nyata, bukti fisik tidak akan salah, dia tidak dapat memalsukan dirinya sendiri, dia tidak akan sepenuhnya hilang, hanya manusia yang gagal menemukannya, pelajari dan pahamilah itu, dapat mengurangi nilainya". Pendek

[192] Kirk Paul L, *Op.Cit*, 21 (4) December 1953

artian, bahwa bukti fisik tidak akan pernah hilang, jika penyidik menyatakan bahwa tidak ditemukan bukti dari pelaku, maka yang gagal menemukan bukti adalah penyidik itu sendiri.

BAB IV

PENUTUP

A. Kesimpulan

1. Beberapa kualifikasi cybercrime secara norma hukum pidana yang diatur dalam Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mencakup Pasal 27 tentang tindakan distribusi konten ilegal di ruang digital; Pasal 28 tentang penyebaran informasi elektronik yang berpotensi menimbulkan kerugian pada pihak lain; Pasal 29 tentang larangan mengirimkan ancaman kekerasan atau ancaman lainnya secara langsung melalui dokumen elektronik; Pasal 30 tentang akses tidak sah

(*unauthorized access*) ke dalam sistem elektronik; Pasal 31 tentang penyadapan atau intersepsi informasi elektronik yang dilakukan secara ilegal; Pasal 32 tentang tindakan perusakan, pengubahan, penghilangan, atau pemindahan informasi elektronik atau dokumen elektronik tanpa izin; Pasal 33 tentang melarang setiap orang yang secara sengaja dan tanpa hak melakukan tindakan yang menyebabkan terganggunya sistem elektronik; Pasal 34 tentang melarang setiap orang yang dengan sengaja dan tanpa hak memproduksi, menjual, atau menyebarkan perangkat lunak yang dirancang khusus untuk menyerang atau merusak sistem elektronik; Pasal 35 tentang melarang setiap orang untuk memalsukan data elektronik atau dokumen elektronik; Pasal 36 dan 37 tentang setiap tindakan yang melanggar pasal-pasal sebelumnya (Pasal 27-35) dan menimbulkan kerugian bagi orang lain dapat dikenakan sanksi.

2. Pembuktian tindak pidana informasi dan transaksi elektronik melalui alat-alat bukti menurut UU ITE terbaru yaitu Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang ITE, diatur dalam Pasal 5 yang menentukan Informasi Elektronik dan/ atau Dokumen Elektronik dan/ atau hasil cetaknya merupakan alat bukti hukum yang sah; Informasi Elektronik dan/ atau Dokumen Elektronik dan/ atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia; Informasi Elektronik dan/ atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur

dalam Undang-Undang ini. Pasal 183 KUHAP yang menyatakan bahwa keyakinan hakim didasarkan pada alat bukti yang sah. Hasil forensik digital menghasilkan barang bukti juga sejalan dengan tujuan alat bukti itu sendiri, yaitu untuk mencari dan memperoleh kebenaran materiil, bukan sekedar mencari kesalahan. Hasil forensik digital forensik berupa surat antara lain BAP laboratorium forensik, BAP ahli, laporan uji forensik digital (misalnya *visum et repertum*). Menurut Pasal 187 b KUHAP, hasil pemeriksaan forensik digital berupa BAP laboratorium forensik dan BAP ahli forensik harus dibuat sesuai dengan ketentuan peraturan perundang-undangan atau undang-undang. Hal ini menunjukan bahwa hasil uji forensik digital menghasilkan surat dari seorang pejabat tentang suatu hal yang terdapat dalam pemerintahan yang menjadi tanggung jawabnya dan dimaksudkan untuk membuktikan suatu hal atau keadaan. Berdasarkan Pasal 43 (5) huruf j UU ITE, dalam penyidikan cybercrime pada ranah pelibatan ahli yang mana berketentuan secara yuridis untuk meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik. Artinya ahli forensik digital berarti seseorang dengan keahlian tertentu di bidang teknologi informasi yang bertanggung jawab secara akademis dan praktis tentang pengetahuan itu.

3. Kerangka hukum yang ada saat ini, meskipun telah memberikan landasan untuk penanganan kasus kejahatan siber, masih memerlukan pembaruan untuk mengakomodasi perkembangan teknologi terbaru. UU ITE dan perubahannya

belum sepenuhnya mampu mengantisipasi kompleksitas kejahatan siber kontemporer. Interpretasi hukum terhadap bukti digital juga masih menjadi tantangan, terutama dalam menentukan admisibilitas dan bobot pembuktiannya di pengadilan. Standar pembuktian yang tinggi dalam sistem peradilan pidana Indonesia terkadang sulit dipenuhi dalam kasus kejahatan siber, mengingat sifat bukti digital yang mudah dimanipulasi, bahkan yang lebih inheren ada pada fasilitas hukum yang sistemik untuk melakukan upaya digital forensik.

B. Saran

1. Indonesia perlu melakukan perbaikan dalam regulasi yang ada seperti UU ITE, agar lebih sesuai dengan perkembangan teknologi dan tantangan kejahatan siber yang semakin kompleks;
2. Perlunya kebijakan eskalasi kuantitas jumlah fasilitas laboratorium forensik digital di seluruh daerah di wilayah Indonesia guna optimalisasi standar pembuktian cybercrime;
3. Memperkuat kapasitas sumber daya manusia pada perangkat penegak hukum melalui pelatihan teknis, serta meningkatkan koordinasi antar lembaga penegak hukum, baik di tingkat nasional maupun internasional;
4. Melalui langkah-langkah strategis yang terintegrasi ini, diharapkan proses penyidikan tindak pidana siber di Indonesia dapat berjalan lebih efektif, efisien, dan sesuai dengan standar hukum internasional yang berlaku.

DAFTAR PUSTAKA

A. Buku

Abdul Hadi, *Fungsi Dan Peran Sidik Jari Dalam Proses Pelaksanaan Penyidikan Ditinjau Dari KUHAP*, Fakultas Hukum Universitas Pancasila, Jakarta, 2004

Abdul Qadir 'Audah, *al-Tasyri' al-Jinaiy al-Islami*, Beirut: Dar al-Kitab al-Arabi, juz 2, 1408 H/ 1988 M

Adami Chazawi, *Pelajaran Hukum Pidana Bagian I,* Jakarta: Rajawali Pers, 2011

Ahmad Wardi Muslich, *Hukum Pidana Islam*, Jakarta: Sinar Grafika, 2005

Andi Hamzah, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta, 2008

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

Budiyanto, *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia*, Sada Kurnia Pustaka, Serang Banten, 2025

C.F.G. Sunaryati Hartono, *Politik Hukum Menuju Satu Sistem Hukum Nasional*, Bandung: Alumni, 1991

Cory Altheide & Harlan Carvey, *Digital Forensics with Open Source Tools*, Syngress, 1st Edition, 2011

Debarati Halder & K. Jaishankar, *Cybercrime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, Pennsylvania USA: IGI, 2011

Dikdik, Elisatris, *Cyber Law Aspek Hukum Teknologi Informasi*, Bandung, Refika Aditama, 2009

Edmond Locard, *La Police et les Méthodes Scientifiques*, Éditions Rieder, 1934

E.Y Kanter dan S.R Sianturi, *Asas-Asas Hukum Pidana di Indonesia dan Penerapannya*, AlumniAHM-PTHM, Jakarta, 1986

Hibnu Nugroho, *Integralisasi Penyidikan Tindak Pidana Korupsi di Indonesia*, Media Aksara Prima, Jakarta, 2012

Ibnul Qayyim al-Jauziyah, *al-Thuruq al-Hukmiyah*, Beirut: Dar al-Ma'rifah, 1408 H/ 1988 M

Imam Riadi dan Ade Kurniawan, *Forensik Jaringan dan Cloud*, Diadra Kreatif Penerbit, Sleman, Cetakan Kedua, 2020

Imam Riadi & Bashor Fauzan Muthohirin, *Forensik Email*, Diandra Kreatif; Yogyakarta, Cetakan 2, 2022

Josua Sitompul, *Cyberspace Cybercrimes Cyberlaw Tinjauan Aspek Hukum Pidana*, Jakarta: Tatanusa. 2012

Masruchin Rubai, *Asas-Asas Hukum Pidana*, UM press dan FH UB, Malang, 2001

Moh. Mahfud MD, *Politik Hukum Di Indonesia*, Jakarta: Raja Grafindo Persada, 2009

M. Nurul Irfan, *Korupsi Dalam Hukum Pidana Islam*, Sinar Grafika Offset, Jakarta, 2011

Moeljanto, *Asas-Asas Hukum Pidana*, Bina Aksara, Jakarta, 1984

_____, *Fungsi dan Tujuan Hukum Pidana Indonesia*, Bina Aksara, Jakarta, 1985

Moh. Mahfud MD, *Membangun Politik Hukum Menegakkan Konstitusi*. Jakarta: Rajawali Press, 2012

M. Yahya Harahap, *Pembahasan Permasalahan Dan Penerapan KUHAP, Penyidikan dan Penuntutan*, Cet VII, Sinar Grafika, Jakarta, 2009

Munir Fuady, *Teori Hukum Pembuktian (Pidana dan Perdata),* Bandung: Citra Aditya Bakti, 2006

P.A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, PT. Citra Adityta Bakti, Bandung, 1996

Ramelan, *Hukum Acara Pidana Teori dan Implementasinya*, Sumber Ilmu Jaya, Jakarta, 2016

R. Moore, *Cyber Crime: Investigating High-Technology Computer Crime*, Cleveland, Mississippi: Anderson Publishing, 2005

Roeslan Saleh, *Perbuatan Pidana dan Pertanggungjawaban Pidana dan Pengertian Dasar dalam Hukum Pidana*, Aksara Baru, Jakarta, 1983

R. Soeroso, *Pengantar Ilmu Hukum*, Sinar Grafika, Jakarta, 2013

Sahat Maruli T. Situmeang, *Cyberlaw*. Penerbit Cakra: Bandung, Cet-1 , 2020

Satjipto Rahardjo, *Ilmu Hukum*, Bandung: Aditya Bakti, 1991

Shinta Dewi, *Perlindungan Privasi Atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional*, Widya Padjajaran, Bandung, 2009

S. R. Sianturi. *Asas-asas Hukum Pidana di Indonesia dan Penerapan*, Cet. 3. Jakarta: Storia Grafika, 2002

Stephen Mason & Daniel Seng, *Electronic Evidence*, published by the Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 4th ed. 2017

Subhi Mahmasoni, *Falsafah al-Tasyri' Fi al-Islam*, Beirut: al-Kasysyaf, 1419 H/ 1949 M

Sulaikin Lubis, dkk, *Hukum Acara Perdata Peradilan Agama*, Jakarta: Kencana, 2006

Sulianta Feri. *Komputer Forensik*. Jakarta: Elex Media Komputindo, 2008

Sutarman. *Cyber Crime Modus Operandi dan Penanggulangannya.* Yogyakarta: LaksBang PRESSindo, 2007

T. Arifiyadi & J. Sitompul, *Gadgetmu, Harimaumu*. Lentera Hati. 2015

Teguh Prasetyo, *Hukum Pidana*, Rajawali Pers, Jakarta, 2011

Warren G. Kruse, Jay G. Heiser. *Computer Forensics: Incident Response Essentials*. Addison-Wesley. 2002

Wirjono Projodikoro, *Hukum Acara Pidana Indonesia*, Sumur Bandung, Bandung, 1981

_____, *Asas-asas Hukum Pidana di Indonesia*, Refika Aditama, Bandung, 2009

B. Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Kitab Undang-Undang Hukum Acara Pidana.

Undang-undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-undang Hukum Pidana

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

Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 6 Tahun 2019 tentang Penyidikan Tindak Pidana

C. Jurnal, Media Internet dan Dokumen Ilmiah

A.A. Agus dan Riskawati, Penanganan Kasus Cybercrime di Kota Makassar (Studi pada Kantor Kepolisian Resort Kota Besar Makassar), *Jurnal Supremasi*, 11 (1) 2016

Adi Darmawansyah, Andry Dwiarnanto, Irwan Putra Satriyawan, Istiqomah, Tinjauan Yuridis Cybercrime dalam Tindak Pidana Pencemaran Nama Baik meurut Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan

Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, *Jurnal Universitas Bung Karno*, 3 (1) Juni 2024

Alcianno G. Gani, Cybercrime (Kejahatan Berbasis Computer), *JSI: Jurnal Sistem Informasi*, 5 (1) 2018

Amsori, Fakhri Awaluddin, dan Momon Mulyana. Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital, *Journal Humaniora: Jurnal Hukum dan Ilmu Sosial*, 02 (01) Januari 2024

Ankit Agarwal, et.all., Systematic Digital Forensic Investigation Model, *International Journal of Computer Science and Security (IJCSS)*, 5 (1) 2011

Asep Sudirman, Kerangka Kerja Digital Forensic Readiness pada sebuah Organisasi (Studi Kasus: PT Waditra Reka Cipta Bandung), *Cyber Security dan Forensik Digital*, 2 (2) November 2019

A. Tatumpe, Analisis Yuridis Digital Forensik dalam Pembuktian Tindak Pidana di Indonesia. *Scientia De Lex*, 7 (1) 2019

A. Y. Pratama, et al., Penegakan Tindak Pidana Cyberstalking dalam Hukum Positif Indonesia. *Legal Standing: Jurnal Ilmu Hukum*, 8 (3) 2024

Bambang Tri Bawono, Tinjauan Yuridis Hak-Hak Tersangka dalam Pemeriksaan Pendahuluan, *Jurnal Hukum,* XXVI (2), Agustus 2011

Budiman, dkk. Akses dan Penggunaan Teknologi Informasi dan Komunikasi pada Rumah Tangga dan Individu, *Jurnal Penelitian Komunikasi dan Pembangunan*, 15 (1) Juni 2024

Budi Rahardjo, Sekilas Mengenai Forensik Digital, *Jurnal Sosioteknologi*, 12 (29) Agustus 2013

Cameron S.D. Brown, Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, Australian National University, *International Journal of Cyber Criminology*, 9 (1) 2015

Chat Le Nguyen dan Golman Wilfred, Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries: 'Law on the Books' vs 'Law in action', *Computer Law & Security Review, Elsevier*, (40) April 2021

Christloy Totota Karo-Karo & Handar Subhandi Bakhtiar, Analisis Kasus Peretasan Media Sosial melalui Digital Forensik sebagai Upaya Preventif Penyidik Mencegah Kejadian Salah Tangkap (Studi Kasus Peretasan Ravio Patra), *TERANG : Jurnal Kajian Ilmu Sosial, Politik dan Hukum*, 1 (4) 2024

Eko Nurisman, Risalah Tantangan Penegakan Hukum Tindak Pidana Kekerasan Seksual Pasca Lahirnya Undang-Undang Nomor 12 Tahun 2022*, Jurnal Pembangunan Hukum Indonesia*, 4 (2)Mei 2022

Eliasta Ketaren, Cybercrime, Cybespace, dan Cyberlaw. *Jurnal Times*, V (2) 2016

Fachrul Rozi, Sistem Pembuktian Dalam Proses Persidangan Pada Perkara Pidana, *Jurnal Yuridis Unaja*, 1 (2) 2019

Farol Medeline, Elis Rusmiati & Rully Herdita Ramadhani, Forensik Digital dalam Pembuktian Tindak Pidana Ujaran Kebencian di Media Sosial, *PAMPAS: Journal Of Criminal Law*, 3 (3) 2022

Handrizal. Analisis Perbandingan Toolkit Puran File Recovery, Glary Undelete Dan Recuva Data Recovery Untuk Digital Forensik. *J-SAKTI: Jurnal Sains Komputer Dan Informatika*, 1 (1) 2017

Herdino Fajar Gemilang & Handar Subhandi Bakhtiar, Meninjau Ilmu Digital Forensik Terhadap Bukti Elektronik dalam Tindak Pidana Informasi dan Transaksi Elektronik, *Perahu (Penerangan Hukum): Jurnal Ilmu Hukum*, 12 (2) September 2024

Herlyanty Bawole, Perlindungan Hukum Bagi Korban Dalam Sistem Peradilan Pidana, *Lex Et Societatis*, IX (3) July-September 2021

Hikmahanto Juwana, Politik Hukum UU Bidang Ekonomi Di Indonesia, *Jurnal Hukum*, 01 (1) 2005

https://apjii.or.id/berita/d/*apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang*

https://www.interpol.int/How-we-work/Criminal-intelligence-analysis/Our-analysis-reports

Indra Utama Tanjung, et.al. Politik Hukum Terhadap Penanggulangan Kejahatan Dunia Maya, *Judge: Jurnal Hukum*, 3 (1) Februari 2022

Ira Irmansyah, Kekuatan Digital Forensik dalam Mengungkap Tindak Pidana Cyber Crime (Studi Kasus: Hacker Ilegal Akses Pembayaran Kereta Commuter Indonesia (KCI), *Jispendiora: Jurnal Ilmu Sosial, Pendidikan dan Humaniora,* 3 (3) Desember 2024

James Popham, Mary McCluskey and Michael Ouellet, Exploring Police-Reported Cybercrime In Canada Variation And Correlates, *Policing: An International Journal*, 43 (1) 2020

Juliana Lumintang, Pengaruh Perubahan Sosial Terhadap Kemajuan Pembangunan Masyrakat di Desa Tara-Tara I, *Acta Diurna Komunikasi*, 4 (2) 2015

Kirk Paul L, Crime Investigation, Physical Evidence and the Police Laboratory, *New York: Interscience Publishers*, 21 (4) December 1953

Manayra Aisha Putri Indradjaja, dkk. Implementation of Investigations into Cyber Crimes in a Comparative Legal Perspective: Indonesia and the United Kingdom, *Jurnal Ilmiah Penegakan Hukum*, 11 (2) Desember 2024

Maulana Daffa Ilhami dan Wiwik Afifah, Mengukir Sifat Unus Testis Terhadap Pembuktian Tindak Pidana Seksual, *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, 3 (2) Mei-Agustus 2023

Mehda Zuraida, Credit Card Fraud (Carding) dan ampaknya Terhadap Perdagangan Luar Negeri Indonesia, *Jurnal Analisis Hubungan Internasional*, 4 (1) Maret 2015

Merdi Hajiji, Relasi Hukum Dan Politik Dalam Sistem Hukum Indonesia, *Jurnal Rechtsvinding Media Pembinaan Hukum Nasional*, 2 (3), 2013

M Qahar Awaka dan Alhadiansyah, Utilization of Digital Forensics in Proving the Crime of Disseminating Indecent Videos Through Facebook Social Media in the Legal Area of West Kalimantan Police, *Jurnal Hukum Sehasen*, 9 (2) Oktober 2023

M. Riskiyadi, Investigasi Forensik Terhadap Bukti Digital dalam Mengungkap Cybercrime, *Cybersecurity dan Forensik Digital*, 3 (2) 2020

Mutia Hafina Putri, dkk. Proses Penyidikan dalam Sistem Peradilan Pidana Investigation Process in the Criminal Justice System, *Rewang Rencang : Jurnal Hukum Lex Generalis*. 4 (7) 2023

Naeem Allah Rakha, Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations, *Mexican Law Review,* 16 (2) Juni 2024

N. Aisyah, dkk. Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime Di Indonesia Secara Systematic Review. *Jurnal Esensi Infokom*, 6 (1) 2022

Nani Widya Sari, Kejahatan Cyber dalam Perkembangan Teknologi Informasi berbasis Komputer, *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan*, 5 (2) 2018

Nikles Denny Ardiansyah, Bambang Panji Gunawan, dan Djasim Siswono. Penerapan UU ITE dalam Penegakan Hukum Siber di Indonesia Studi Kasus pada Pasal 27 Hingga Pasal 37, *Jurnal Reformasi Hukum : Cogito Ergo Sum*, 7 (2) Juli 2024

Nurianto Rachmad Soepadmo, Impact Analysis of Information and Electronic Transactions Law (Law No. 19 Year 2016) on the Level of Cyber-Crime in Social Media, *International Journal of Innovation, Creativity and Change*, 12, (8) 2020

Nurul Aini dan Fauziah Lubis, Tantangan Pembuktian dalam Kasus Kejahatan Siber, *Judge: Jurnal Hukum*, 5 (2) 2024

Ruci, Meiyanti, and Ismaniah. Perkembangan Digital Forensik. *Jurnal Kajian Ilmiah UBJ*, 15 (2) September 2015

Ruuhwan, Imam Riadi, and Yudi Prayudi. Analisis Kelayakan Integrated Digital Forensics Investigation Framework untuk Investigasi Smartphone. *Jurnal Buana Informatika*, 7 (4) 2016

Sahuri Lasmadi, Tumpang Tindih Kewenangan Penyidikan Pada Tindak Pidana Korupsi Pada Perspektif Sistem Peradilan Pidana, *Jurnal Ilmu Hukum*, 2 (3) Juli 2010

_____, Pengaturan Alat Bukti dalam Tindak Pidana Dunia Maya, *Jurnal Ilmu Hukum Jambi*, 5 (2) Oktober 2014

Scientific Working Group on Digital Evidence, Best Practices for Remote Collection of Digital Evidence from an Endpoint, *SWGDE Documents*. Version 2.0 November 2022

Sharofan Mirfandaresky, et.al,. Digital Forensik dalam Penyidikan Tindak Pidana Penipuan Online (Studi Kasus di Wilayah Hukum Kepolisian Resor Ponorogo), *Dinamika*, 28 (10) Januari 2022

Seri Mughni Sulubara, et.all. Judi Online Sebagai Cybercrime Serta Tantangan Penegakan Hukum Pidana di Era Digital: Antara Regulasi, Pembuktian, dan Ancaman Cybercrime, *Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora*, 4 (2) April 2025

Soerjono Soekanto, Ilmu Politik & Hukum, *Jurnal Hukum & Pembangunan*, 18, (3) 2017

Sry Wahyuni, Yoserwan, Pertanggungjawaban Pidana terhadap Pencemaran Nama Baik melalui Media Sosial, *Unes Law Review*, 6 (1) 2023

Steve Morgan, Cyber Crime Costs Projected To Reach $2 Trillion by 2019. *Forbes*. Retrieved September 22, 2016

Supriyono. Criminology Study of Crime of Fencing the Stolen Goods. *Jurnal Daulat Hukum*, 3 (1) March 2020

Synthiana Rachmie, Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website, *Jurnal Litigasi*, 21 (1) April 2020

Victor R Kebande, Nickson M Karie and H.s. Venter. A Generic Digital Forensic Readiness Model for BYOD using Honeypot Technology, *2016 IST-Africa Week Conference*, Durban, South Africa, 2016