

BAB I

PENDAHULUAN

A. Latar Belakang Penelitian

Internet merupakan jaringan komputer yang terhubung satu sama lain melalui media komunikasi, seperti kabel, satelit atau gelombang frekuensi. jaringan ini bisa berukuran kecil seperti *LAN (local area network)* yang bisa dipakai secara internal di kantor-kantor, bank-bank, rental komputer, perpustakaan dan sebagainya bisa juga jaringan super besar yang dikenal dengan internet.¹ Melalui dunia internet atau disebut juga *cyber space*, apapun dapat dilakukan. Sisi positif yang di dapat dari dunia maya ini tentu saja menambah nilai yang ada pada perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia.² Namun dampak negatif pun tidak bisa dihindari. Seiring dengan perkembangan teknologi dan Internet, menyebabkan munculnya kejahatan yang disebut dengan *Cyber crime* atau kejahatan melalui jaringan Internet. beberapa contoh kasus *Cyber crime* yang pernah terjadi di Indonesia, seperti pencurian kartu kredit, *hacking* beberapa situs, menyadap transmisi data orang lain, misalnya email, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam programmer komputer.

¹ Redha manthovani, *dan solusi penanganan kejahatan cyber di Indonesia*, PT malibu, Jakarta, 2006, hlm.1.

² Eliasta ketaren, *cybercrime , cyber space, dan cyber law*, Jurnal TIMES Vol. V No.2, 2016, hlm.35.

Sehingga dalam kejahatan komputer dimungkinkan adanya delik formil dan delik materil. Delik formil adalah perbuatan seseorang yang memasuki komputer orang lain tanpa ijin, sedangkan delik materil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain.³ Adanya *Cybercrime* telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet dan intranet.

Penjelasan *cyber crime* menurut andi hamzah yaitu :⁴

Penggunaan komputer secara *illegal*, secara umum dapat diartikan sebagai kejahatan di bidang komputer.

Menurut Agus rahardjo :⁵

Segala bentuk kejahatan yang terjadi di dunia maya atau internet dapat diartikan sebagai *cybercrime* .

Menurut Morrison :⁶

Kejahatan komputer sebagai aksi criminal dimana komputer digunakan sebagai senjata utama merupakan definisi dari *cyber crime*.

³ *Ibid*, hlm.35

⁴ Andi Hamzah, *Aspek-aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta, 1989. hlm 23.

⁵ Agus Rahardjo, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung PT Citra Aditya Bakti, 2002, hlm.10

⁶ Deris Setiawan, *Sistem Keamanan Komputer*, PT Elex Media Komputindo, Jakarta, 2005, hlm 34

Cyber crime merupakan kejahatan yang memanfaatkan perkembangan teknologi untuk dapat meretas dan mengakses suatu komputer dengan akses yang illegal. Oleh karena itu *cyber crime* dapat di identifikasikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer berbasis pada kecanggihan dan perkembangan teknologi internet.

Cyber crime dapat pula dirumuskan sebagai kejahatan yang dimana sarana atau alat utama yang digunakannya adalah komputer dan jaringan internet. Maka objek utama dalam hal ini adalah komputer yang digunakan sebagai alat melakukan tindak pidana meretas dan atau mengakses komputer orang lain secara melawan hukum dengan maksud menguntungkan diri si pelaku ataupun membuat kerugian bagi orang lain.

Cyber crime bukanlah kejahatan yang sederhana mengingat penggunaan dari kejahatan ini bukan menggunakan sarana yang konvensional melainkan menggunakan komputer dan jaringan internet. Kejahatan ini pun tidak terbatas dari hanya suatu negara bahkan menyangkut berbagai Kawasan sampai dengan antar negara. Maka dari itu kejahatan *cyber crime* ini merupakan kejahatan yang paling sulit untuk dibuktikan karena penggunaan dari kecanggihan teknologi yang dimilikinya membuat sulitnya untuk menegakan kejahatan dalam bidang *cyber crime* ini. Dengan adanya kejahatan di

dunia maya yang terkait dengan pemanfaatan teknologi informasi digunakanlah beberapa istilah yakni hukum teknologi informasi (*law of information technology*), hukum dunia maya (*virtual world law*), dan hukum mayaantara. Istilah hukum siber digunakan dalam tulisan ini, dilandasi pemikiran bahwa *cyber* jika diidentikan dengan dunia maya maka penegak hukum akan cukup menghadapi persoalan Ketika terkait dengan pembuktian dan penegakan hukumnya. Hal ini mengingat para penegak hukum akan menghadapi kesulitan jika harus membuktikan suatu persoalan yang diasumsikan sebagai maya sesuatu yang tidak terlihat dan semu.⁷

Salah satu yang membuat kejahatan *cyber crime* ini menjadi sulit adalah dalam proses pembuktiannya. Jenis Tindakan yang sulit untuk dibuktikan salah satu contoh adalah tindak pidana *cyber hacking* dan *cracking* . Kedua tindak pidana ini belum diatur dalam Kitab Undang-undang hukum Pidana (KUHP) tetapi telah diatur secara khusus dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik). Dalam Pasal 30 menyatakan bahwa :

⁷ Maman Budiman, *kejahatan korporasi di Indonesia*, setara press, malang, 2020, hlm.10.

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

Penjelasan dalam Pasal 30 tersebut sudah jelas telah mengatur mengenai tindak pidana *cyber hacking* dan *cracking* dimana Pasal tersebut memiliki unsur sebagai berikut :

Unsur ayat (1) :

1. Setiap orang
2. Dengan sengaja, tanpa hak atau melawan hukum
3. Mengakses komputer dan/atau sistem elektronik
4. Milik orang lain dengan cara apapun

Unsur ayat (2) :

1. Setiap orang

2. Dengan sengaja, tanpa haka tau melawan hukum
3. Mengakses Komputer dan/atau Sistem Elektronik
4. Dengan cara apa pun
5. Dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

Unsur ayat (3) :

1. Setiap orang
2. Dengan sengaja, tanpa haka tau melawan hukum
3. Mengakses Komputer dan/atau Sistem Elektronik
4. Dengan cara apapun
5. Dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Unsur dalam Pasal 30 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik tersebut sudah memperjelas bahwa tindak pidana *cyber hacking* dan *cracking* telah diatur dengan jelas dan setiap Tindakan tersebut dapat dikenakan sebagai Tindakan criminal.

Permasalahan yang dihadapi selanjutnya adalah bukan lagi mengenai penjelasan mengenai Tindakan *cyber hacking* dan *cracking* sebagai tindak pidana yang telah diatur dalam hukum pidana Indonesia kita, tetapi permasalahan selanjutnya yang dihadapi

adalah bagaimana sistem pembuktian yang dapat membuktikan, bahwa pelaku tindak pidana *cyber hacking* dan *cracking* telah memenuhi unsur dalam Pasal 30 tersebut. Karena di dalam Pasal 183 KUHAP dinyatakan bahwa hakim tidak boleh menjatuhkan pidana kepada seorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwa yang bersalah melakukannya.

Problematika dari hal ini adalah mengenai bagaimana pembuktian terhadap tindak pidana *cyber hacking* dan *cracking* berkaitan dengan Pasal 44 UU No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Dimana dalam Pasal ini hanya mengatur bahwa alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut:

- a. alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dan
- b. 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).

Sistem pembuktian hukum acara pidana yang menganut *stelsel negatief wettelijk*, hanya alat-alat bukti yang sah menurut undang-

undang yang dapat dipergunakan untuk pembuktian.⁸ Maka dari itu di luar dari ketentuan tersebut tidak dapat dipergunakan sebagai alat bukti yang sah.

Pasal 184 ayat (1) Kitab Undang-undang Hukum Acara Pidana tidak menjelaskan mengenai bagaimana alat bukti dari elektronik ini dapat diterima dalam persidangan sebagai alat bukti yang sah. Penggunaan data elektronik sebagai alat bukti dalam tindak pidana *cyber hacking* dan *cracking* sebenarnya sudah dilakukan dalam perkara no 1347/Pid.Sus/2019/PN Bdg dan perkara 1102/Pid.Sus/2018/PN Bdg . Namun dalam hal ini diperlukan proses lanjut terhadap data elektronik tersebut agar data elektronik itu dapat dijadikan sebagai alat bukti yang sah, dan memenuhi syarat dalam Pasal 184 ayat (1) Kitab Undang-undang Hukum Acara Pidana (KUHAP). Proses tersebut tidak mudah untuk dilakukan, karena data elektronik yang berupa digital tersebut harus di print-out dan di cetak ke dalam kertas oleh laboratorium forensik komputer dan ditandatangani oleh ahli forensik komputer sehingga dapat dijamin keasliannya dan keakuratannya, sehingga data elektronik tersebut dapat diubah menjadi keterangan ahli, surat dan ataupun petunjuk.

Permasalahan inilah yang membuat penulis tertarik untuk mendalami lagi mengenai pembuktian dalam tindak pidana *cyber*

⁸ NFN Ramiyanto, *Bukti Elektronik Sebagai Alat Bukti yang Sah Dalam Hukum Acara Pidana*, Jurnal Hukum Dan Peradilan, 2017 .hlm. 25

hacking dan *cracking* karena dalam pembuktian inilah banyak masalah menarik yang dapat dijadikan untuk pengembangan pengetahuan bagi pembaca dan penulis dan juga diharapkan dalam penulisan tugas akhir ini karya dari penulis dapat menjadi rujukan untuk perkembangan ilmu pengetahuan. Dari faktor – faktor itulah yang membuat penulis tertarik untuk melakukan penelitian skripsi yang berjudul **Pengaturan Alat Bukti Dalam Tindak Pidana *Cyber hacking* dan *Cracking* Dikaitkan Dengan UU No. 19 Tahun 2016 Tentang Perubahan Atas UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.**

B. Identifikasi Masalah

1. Bagaimana pembuktian yang dilakukan oleh jaksa penuntut umum mengenai tindak pidana *cyber hacking* dan *cracking* ?
2. Kendala apa sajakah yang terjadi dalam pembuktian *cyber hacking* dan *cracking* berkaitan dengan Pasal 43 UU No. 19 Tahun 2016 Tentang Perubahan Atas UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.?
3. Bagaimana upaya yang dapat dilakukan oleh Pemerintah untuk menyelesaikan persoalan pembuktian dalam tindak pidana *cyber hacking* dan *cracking* agar sesuai dengan Peraturan Perundang-Undangan ?

C. Tujuan Penelitian

1. Ingin meneliti dan mengkaji pembuktian yang dilakukan oleh jaksa penuntut umum mengenai tindak pidana *cyber hacking* dan *cracking* .
2. Ingin mengetahui kendala yang terjadi dalam pembuktian *cyber hacking* dan *cracking* berkaitan dengan Pasal 43 UU No. 19 Tahun 2016 Tentang Perubahan Atas UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.
3. Ingin mengetahui dan meneliti upaya yang dapat dilakukan untuk menyelesaikan persoalan pembuktian dalam tindak pidana *cyber hacking* dan *cracking* agar sesuai dengan Peraturan Perundang – undangan.

D. Kegunaan Penelitian

Kegiatan penelitian yang dilakukan oleh penulis ini diharapkan dapat memberikan kegunaan baik itu secara teoritis yang dapat mengembangkan ilmu pengetahuan maupun secara praktis yaitu untuk memecahkan masalah yang ada, yaitu sebagai berikut :

1. Kegunaan Teoritis

Hasil Penelitian ini diharapkan dapat memberikan penambahan dalam ilmu pengetahuan hukum serta memberikan manfaat untuk perkembangan hukum pembuktian berkaitan dengan alat bukti dan juga diharapkan dapat memberikan kontribusi terhadap perkembangan sistem peradilan Indonesia.

2. Kegunaan Praktis

Hasil Penelitian ini diharapkan dapat menjadi masukan dan rujukan bagi masyarakat sebagai suatu sumber informasi dan referensi mengenai pembuktian tindak pidana *cyber hacking* dan *cracking* dalam sistem pembuktian peradilan di Indonesia, dan dapat dijadikan sebagai landasan bagi penelitian lebih lanjut.

E. Kerangka Pemikiran

Pasal 28 D Ayat 1 Undang-Undang Dasar RI Tahun 1945 menyatakan bahwa :

Setiap orang berhak atas pengakuan, jaminan, perlindungan, dan kepastian hukum yang adil serta perlakuan yang sama di hadapan hukum.

Pasal ini menjelaskan bahwa kepastian hukum harus tetap diutamakan mengingat dalam Pasal 1 ayat (3) Undang-Undang Dasar 1945 menjelaskan bahwa negara Indonesia adalah negara hukum. Maka dari itu peristiwa hukum yang ada di Indonesia harus sudah diatur oleh peraturan perundang – undangan supaya tidak terjadi yang namanya kekosongan hukum dan dapat pula terjadinya kepastian hukum bagi setiap warga negara Indonesia. Berkaitan mengenai pembuktian tindak pidana *cyber hacking* dan *cracking* juga harus sudah dapat diatur oleh peraturan perundang – undangan yang berlaku.

Negara mempunyai kewajiban untuk memberikan kepastian hukum dan mengupayakan untuk mencegah agar tidak terjadinya

Tindakan yang belum diatur dalam kehidupan yang ada dalam masyarakat. Dengan adanya kepastian hukum maka akan terjadi upaya untuk melakukan pengaturan hukum terhadap sesuatu yang belum diatur melalui suatu peraturan perundang – undangan yang ditetapkan oleh pemerintah.

Kepastian hukum mempunyai arti yaitu dalam negara hukum yang perlu dan harus diutamakan adalah landasan peraturan perundangundangan, kepatutan, dan keadilan dalam setiap kebijakan penyelenggaraan negara. Makna dalam asas ini yaitu menghendaki dihormatinya hak yang telah diperoleh seseorang berdasarkan suatu keputusan dari badan atau pejabat administrasi negara yang memberikan kepastian hukum tersebut.

Hukum harus bisa menjadi pedoman, mengayomi dan melindungi masyarakat dari berbagai tindak kejahatan, dan hal ini merupakan salah satu tanggung jawab dalam penyelenggaraan suatu negara. Supaya kepastian hukum dapat digunakan untuk memastikan bahwa hukum dapat dijalankan dan dipatuhi sehingga tidak akan menimbulkan kerugian bagi siapapun.

Selanjutnya mengenai Pasal 28C ayat (1) dan Pasal 28F menjelaskan bahwa :

Pasal 28C :

Untuk meningkatkan kualitas hidup dan kesejahteraan umat manusia, setiap orang atau individu diberikan hak

oleh negara untuk melakukan pengembangan diri melalui pemenuhan kebutuhan dasar, mendapatkan Pendidikan dan memperoleh manfaat dari ilmu pengetahuan dan teknologi, seni dan budaya.

Penjelasan Pasal ini adalah bahwa kemajuan dari suatu teknologi tidak dapat di tahan atau dihambat karena kemajuan teknologi ini adalah bagian dari manfaat ilmu pengetahuan yang bertujuan meningkatkan kualitas hidup seseorang dan juga untuk mensejahterakan kehidupan masyarakat. Dan hal ini pun adalah bagian dari pengembangan diri yang diperoleh dari suatu informasi dengan berbagai saluran yang tersedia, khususnya dari media elektronik.

Keberadaan internet sangat memudahkan manusia dalam menjalankan kegiatan-kegiatannya dalam memperoleh, mengolah dan menyajikan informasi baik itu di tingkat nasional ataupun di tingkat internasional, contohnya adalah dalam bidang perdagangan, Pendidikan, perbankan, kebudayaan, kesenian dan kekerabatan. Perkembangan internet pun mempengaruhi urusan dalam bidang Kesehatan, transportasi dan pengembangan hukum dan politik menjadi semakin maju dan berkembang.⁹

Selain keuntungan yang di dapat dengan adanya kemajuan teknologi, kerugian yang akan di dapat pun pasti akan ada. Kerugian

⁹ Agus Tri P.H, *Cyber crime dalam Perspektif Hukum Pidana*, Skripsi, 2010, hlm 22

yang timbul dari kemajuan teknologi tersebut adalah pemanfaatan dari suatu ilmu pengetahuan dengan niat buruk dan jalan yang tidak benar untuk menguntungkan diri sendiri ataupun pihak lain, hal ini dapat disebut dengan kejahatan. Contoh dari kejahatan tersebut adalah seperti pemalsuan, penipuan, pencurian, pornografi, perjudian, pembajakan hak cipta, bahkan kejahatan dalam dunia teknologi pun dapat menyerang pada kehormatan seseorang (penghinaan, pencemaran nama baik). Ketika kerugian itu sudah menimbulkan korban maka hal itu dapat dikatakan sebagai kejahatan *cyber*, terlebih kejahatan mengenai *cyber hacking* dan *cracking*.

Tindakan *cyber hacking* dan *cracking* sudah sangat banyak terjadi di Indonesia, dan ini merupakan kejahatan yang sangat sulit untuk di awasi. *Hacking* mempunyai pengertian yaitu serangkaian kegiatan yang dilakukan oleh hacker yang mencari dan memanfaatkan kelemahan dalam suatu sistem dan membobol masuk kedalam sistem tersebut atau biasa disebut dengan *unauthorized access*.¹⁰ *Cracking* adalah serangkaian kegiatan yang dilakukan oleh cracker untuk membobol sistem yang ada pada komputer dengan tujuan mengambil data tersebut. Kejahatan tindak pidana *cyber hacking* dan *cracking* merupakan dampak dari kemajuan dari ilmu pengetahuan, khususnya dalam bidang

¹⁰mastel.id/hlmo-sobat-mastel-sudah-tau-belum-apa-itu-cyber-crime/#:~:text=Hacking%20%2F%20Cracking&text=Hacker%20%3A%20Menganalisa%20kelemahan%20suatu%20sistem,keuntungan%20dari%20kerugian%20pihak%20lain. Di akses pada 20 oktober 2020, 18.30 WIB

teknologi yang membuat tindak pidana *cyber hacking* dan *cracking* ini menjadi tindak pidana yang dapat dilakukan oleh setiap orang yang mempunyai komputer dan jaringan internet dengan niat tidak baik dan menyalahgunakan kemajuan teknologi tersebut.

Tindak pidana *cyber hacking* dan *cracking* adalah salah satu kejahatan yang termasuk dalam kejahatan transnasional. Maka jika kejahatan ini sudah menyangkut kedalam kejahatan transnasional akan sulit bagi para penegak hukum untuk melakukan pembuktian terhadap tindak pidana tersebut. Karena penegak hukum akan kesulitan dalam hal melakukan penyelidikan dan penyidikan terkait tindak pidana tersebut, mengingat kejahatan ini bukan hanya dilakukan di Indonesia tetapi juga bisa dilakukan di negara lain, yang dimana hal ini pun akan menyebabkan pelaku tindak pidana *cyber hacking* dan *cracking* sulit untuk ditemukan.

Kemajuan teknologi ini seharusnya dapat memajukan juga segi penegakan hukum dalam bidang teknologi dan informasinya, khususnya penegakan hukum dalam pembuktian tindak pidana *cyber hacking* dan *cracking* . Tetapi kurangnya perhatian dari penegak hukum menyebabkan kelemahan – kelemahan terhadap penegakan tersebut menjadi masalah yang terus sering terjadi dalam kaitannya tindak pidana *cyber hacking* dan *cracking* ini. Proses pembuktian ini adalah salah satu hal yang penting mengingat dalam pembuktian ini dapat menentukan

apakah kejahatan ini merupakan kejahatan yang berdampak besar atau kecil.

Ada pengertian dari beberapa ahli hukum mengenai pembuktian, contohnya adalah pengertian dari :

menurut Sudikno Mertokusumo :

Arti yuridis dari konteks pembuktian adalah upaya untuk memberi dasar-dasar yang cukup kepada hakim yang memeriksa perkara yang bersangkutan guna memberi kepastian tentang kebenaran peristiwa hukum yang diajukan tersebut.

menurut Hari :

pembuktian yang sah adalah pembuktian yang telah diatur oleh hukum acara pidana, dimana hal – hal yang diatur tersebut adalah macam – macam alat bukti yang sah, sistem pembuktian dan bagaimana syarat-syarat dan tata cara mengajukan bukti itu. Dan hakim pun memiliki kewenangan untuk menerima, menolak, dan menilai suatu pembuktian tersebut.¹¹

menurut Pitlo :

pembuktian merupakan suatu upaya yang dilakukan oleh dua pihak atau lebih yang berperkara dalam hal tujuannya untuk dapat meyakinkan hakim atas dalil dalil yang telah dinyatakan para pihak supaya dengan hal tersebut para pihak tersebut dapat mendapatkan keyakinan hakim tersebut. Maka dari itu pembuktian adalah suatu cara yang dilakukan oleh para pihak untuk bisa meyakinkan hakim dengan menggunakan alat-alat bukti yang telah diatur dan ditetapkan oleh undang-undang.

menurut Subekti :

¹¹ Hari Sasangka dan Lily Rosita, *Hukum Pembuktian Dalam Perkara Pidana*, Mandar Maju, Bandung, 2003, hlm.10.

bagaimana cara untuk meyakinkan hakim agar dalil kebenaran yang telah di terangkan oleh para pihak yang bersengketa dapat dibenarkan dalam persengketaan tersebut hal ini merupakan suatu pembuktian.¹²

Tujuan dari pembuktian adalah untuk memberikan gambaran berkaitan tentang kebenaran atas suatu peristiwa, sehingga dari peristiwa tersebut dapat diperoleh kebenaran yang dapat diterima oleh akal. Pembuktian mengandung arti bahwa benar suatu peristiwa pidana telah terjadi dan terdakwa yang bersalah melakukannya, sehingga harus mempertanggungjawabkannya. Pembuktian adalah ketentuan-ketentuan yang berisi penggarisan dan pedoman tentang cara-cara yang dibenarkan undang-undang membuktikan kesalahan yang didakwakan kepada terdakwa. Pembuktian juga merupakan ketentuan yang mengatur alat-alat bukti yang dibenarkan undang-undang dan boleh dipergunakan hakim membuktikan kesalahan yang didakwakan.¹³

Berkaitan tentang pembuktian, dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP) yang didalamnya mengatur tata cara beracara pidana di pengadilan. Memang tidaklah dijelaskan secara mendalam berkaitan dengan konteks pembuktian, hanya saja didalam KUHAP terdapat Pasal 183 yang mengatur berkaitan tentang hakim tidak boleh menjatuhkan pidana pada seorang kecuali ditemukan sekurang-kurangnya terdapat 2 (dua) alat bukti yang sah dan atasnya memperoleh

¹² Subekti, *Hukum Pembuktian*, (Pradnya Paramitha), Jakarta, 2001, hlm 1.

¹³ M.Yahya Harahap, *Pembahasan Permasalahan dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali*: Edisi Kedua, Sinar Grafika, Jakarta, 2006, hlm 273.

keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwa yang bersalah melakukannya. dan jenis-jenis alat bukti yang sah menurut hukum, yang tertuang dalam Pasal 184 ayat (1) KUHAP yaitu:

- a. keterangan saksi;
- b. keterangan ahli;
- c. surat;
- d. petunjuk; dan
- e. keterangan terdakwa.

Jika dilihat dari konteks Pasal 183 KUHAP, maka dapat diambil kesimpulan bahwa KUHAP di Indonesia memiliki sistem pembuktian yang bersifat *negative wettelijk*. Hal tersebut dapat dilihat dari praktik beracara yang lumrah terjadi pada pengadilan Indonesia yakni upaya pembuktian dari masing-masing pihak dengan menghadirkan bermacam-macam bukti-bukti beserta keyakinan hakim terhadap suatu kesalahan berdasarkan bukti-bukti tersebut.¹⁴

Berdasarkan teori pembuktian menurut undang-undang negatif (*negatief wettelijke*) yang dimana teori ini adalah teori yang dipakai dalam sistem pembuktian Indonesia yang tercantum dalam Pasal 183 KUHAP, yang menjelaskan bahwa hakim tidak bisa menjatuhkan pidana kepada terdakwa hanya berdasarkan 2 alat bukti saja, tetapi hakim harus

¹⁴ *Ibid, hlm.319.*

juga memakai keyakinannya untuk dapat memastikan bahwa terdakwa memang benar-benar telah melakukan tindak pidana.

Dalam kejahatan mengenai *cyber hacking* dan *cracking*, ketentuan dalam Pasal 183 KUHAP dapat diterapkan walaupun harus dilakukan pembuktian secara lebih lanjut. Yang harus dilakukan terlebih dahulu dalam pembuktian terhadap Tindakan *cyber hacking* dan *cracking* adalah penggunaan bukti petunjuk yang dapat diperoleh dari keterangan saksi, surat, dan keterangan terdakwa (Pasal 188 ayat (2) KUHAP). Bila mengenai keterangan saksi dan keterangan terdakwa tidak dapat ditemukan, maka petunjuk dapat diperoleh dari surat atau dokumen yang ditemukan, tentunya hal ini harus ditemukan persesuaian satu dengan yang lainnya mengenai alat bukti tersebut. Jika terdapat kesamaan bentuk, metode atau cara dalam melakukan suatu kejahatan *hacking* dan *cracking* maka dari itu akan diperoleh petunjuk atau bisa disebut sebagai bukti awal, yang nantinya tetap harus dibuktikan dengan bantuan seorang ahli untuk menjelaskan perkara tersebut.

Alat bukti surat yang tercantum dalam Pasal 184 ayat (1) KUHAP, dapat juga diterapkan dalam kaitannya tindak pidana *cyber hacking* dan *cracking*, tetapi harus terlebih dahulu dijamin keasliannya dengan melegalisasi surat tersebut oleh pihak yang berwenang sehingga surat tersebut dapat menjadi alat bukti yang sah di pengadilan.

Selain dalam KUHAP pengaturan mengenai pembuktian tindak pidana *cyber hacking* dan *cracking*, diatur juga dalam Undang – undang N0.19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik. Dalam Pasal 5 ayat (1), (2), dan (3) menyatakan bahwa :

- 1) alat bukti hukum yang sah dalam pembuktian kaitannya dengan kejahatan *cyber* adalah Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya.
- 2) Sebagaimana yang telah dijelaskan dalam ayat (1) tersebut bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya adalah perluasan dari alat bukti yang sah dan sesuai dengan Hukum Acara yang berlaku di Indonesia.
- 3) dinyatakan sah sebagai alat bukti apabila Informasi Elektronik dan/atau Dokumen Elektronik menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam UndangUndang ini.

Tetapi, walaupun mengenai pembuktian tersebut telah diatur dalam peraturan perundang - undangan, ada pula faktor penghambat dalam proses pembuktian tersebut yaitu penegak hukum yang tidak mengikuti perkembangan zaman atau ketinggalan zaman yang membuat proses pembuktian terhadap kejahatan teknologi tidak bisa diantisipasi dengan baik. Keadaan ini pula lah yang membuat jalannya proses penegakan hukum mengenai kejahatan teknologi, khususnya dalam Tindakan *cyber hacking* dan *cracking* menjadi terhambat dan mengalami banyak kendala dalam proses pembuktiannya. Yang menjadi masalah pula adalah penegak hukum yang tidak mau mengembangkan ilmu pengetahuan teknologi untuk dijadikan sebagai pengetahuan baru terhadap proses pembuktian.

Para penegak hukum pun mempunyai permasalahan mengenai fasilitas - fasilitas yang dimiliki terkait dengan menindaklanjuti perkara-perkara yang berhubungan dengan teknologi. Dan hal ini pun menjadi masalah dalam suatu perkara mengenai penggunaan teknologi sebagai sarana utamanya, hakim terkadang masih mempelajari sampai sejauh mana hal tersebut dapat terbukti dan dapat diputuskan secara adil.

Hal ini pun dapat terlihat dalam putusan - putusan hakim yang terkait dengan penyalahgunaan teknologi, dimana para pakar dalam bidang teknologi berpandangan bahwa seharusnya ada kejahatan yang jelas – jelas merupakan kejahatan yang serius dan dapat di pidana dengan hukuman berat, tetapi hakim berpandangan sebaliknya mengenai hal tersebut dan menyatakan bahwa kejahatan tersebut adalah kejahatan yang biasa. Hal ini merupakan masalah – masalah yang harus di perhatikan supaya tidak terjadi kesalahan yang menimbulkan kerugian bagi masyarakat banyak.

F. Metode Penelitian

prosedur atau cara memperoleh pengetahuan yang benar atau kebenaran melalui langkah-langkah yang sistematis merupakan definisi dari metode penelitian.¹⁵

¹⁵ Peter R. Senn, *Metode Penelitian Hukum*, PT. Raja Grafindo Persada, Jakarta, 2003, hlm.46.

Tahap-tahap yang akan digunakan oleh penulis untuk Menyusun dan membuat usulan penelitian ini adalah sebagai berikut :

1. Spesifikasi Penelitian

Dalam spesifikasi penelitian ini penulis akan menggunakan spesifikasi deskriptif-analitis yaitu penelitian yang akan menggambarkan dan juga menganalisis suatu peraturan perundang – undangan yang berlaku, lalu dikaitkan terhadap praktek pelaksanaan pembuktian Tindak pidana kejahatan *cyber hacking* dan *cracking* di Indonesia yang dihubungkan dengan Pasal 44 UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

2. Metode Pendekatan

Metode yang akan digunakan dalam penelitian ini adalah metode pendekatan yuridis empiris, dimana penulis akan memulai dengan menganalisa Pasal 44 UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang berkaitan mengenai alat bukti elektronik, lalu setelah itu menghubungkannya dengan penanganan perkara tindak pidana kejahatan *cyber hacking* dan *cracking* , serta menghubungkannya juga dengan perundang-undangan lain yang termasuk kedalam permasalahan mengenai *cyber crime*. Metode penelitian ini, digunakan dengan memperhatikan bahwa permasalahan yang akan diteliti berpusat pada penerapan dalam praktik dan hubungannya dengan peraturan yang satu dengan peraturan yang lainnya.

3. Tahap Penelitian

Ada 2 (dua) tahap penelitian Menurut Rony Hanitijo Soemitro yaitu terdiri dari :¹⁶

a. Penelitian Kepustakaan (Library Research)

penelitian kepustakaan adalah kegiatan yang dilakukan secara sistematis untuk mengumpulkan, mengolah, dan menyimpulkan data dengan menggunakan metode/Teknik tertentu guna mencari jawaban atas permasalahan yang dihadapi melalui penelitian kepustakaan.¹⁷ Penelitian kepustakaan dalam bidang hukum dapat diartikan sebagai penelitian terhadap data sekunder. Dalam bidang hukum pun data sekunder dapat dibagi menjadi 3 (tiga) bagian yaitu bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier.

Penelitian ini dimaksudkan untuk mendapatkan data sekunder, yaitu :

- 1) Bahan hukum primer yaitu bahan hukum yang berkaitan dengan peraturan perundang – undangan yang akan digunakan yaitu :

¹⁶ Ronny hanitijo soemitro, *metodologi penelitian hukum dan jurimetri*, Ghlmia Indonesia, Jakarta, 1990, Hlm.11

¹⁷ Milya Sari, ‘*Penelitian Kepustakaan (Library Research) Dalam Penelitian Pendidikan IPA*’, *Natural Science: Jurnal Penelitian Bidang IPA Dan Pendidikan IPA*, 6.1 (2020), hlm.44.

- a. Undang – Undang Dasar Republik Indonesia Tahun 1945
 - b. Kitab Undang – Undang Hukum Acara Pidana
 - c. Undang – Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik.
- 2) Bahan hukum sekunder yaitu bahan hukum yang akan memberikan penjelasan terhadap bahan hukum primer nantinya, yang kaitannya erat dengan buku ataupun jurnal. Bahan hukum sekunder yang digunakan adalah studi Pustaka terhadap buku – buku mengenai *cyber crime* khususnya tentang kejahatan *cyber hacking* dan *cracking* , hasil karya ilmiah para sarjana, dan dari tulisan – tulisan yang ada pada jurnal – jurnal yang berkaitan dengan Tindakan *cyber hacking* dan *cracking* .
- 3) Bahan hukum tersier adalah bahan hukum yang menggunakan sumber lain dan memberikan petunjuk atau penjelasan terhadap bahan hukum primer dan sekunder. Bahan hukum tersier yang digunakan adalah :
- a. Kamus Besar Bahasa Indonesia (KBBI)
 - b. Kamus Hukum
 - c. Tulisan – Tulisan yang ada di internet yang berkaitan mengenai Tindakan *cyber hacking* dan *cracking* .

b. Penelitian Lapangan

Penelitian lapangan termasuk kedalam data primer, dan teknik pengumpulan data yang dilakukan yaitu dengan cara wawancara (*interview*) dengan aparat penegak hukum yang terlibat dalam peradilan pidana, seperti Polisi, Jaksa dan hakim dalam perkara *cyber crime* khususnya dalam perkara *cyber hacking* dan *cracking* . untuk penunjang data sekunder maka penulis melakukan pengumpulan data, meneliti serta menggambarkan data primer yang diperoleh dari penelitian lapangan ini.

4. Teknik Pengumpulan Data

Karena dalam penelitian ini pendekatan yang digunakan penulis adalah yuridis – Empiris, maka Teknik pengumpulan data yang digunakan adalah Teknik pengumpulan data yang dapat diperoleh dalam peraturan perundang – undangan, buku teks, jurnal, hasil penelitian, ensiklopedi, bibliografi, dan lain lain. Maka untuk mendapatkan data tersebut dilakukan dengan cara sebagai berikut :

a. Studi dokumen dan studi kepustakaan

Studi dokumen atau studi kepustakaan yaitu suatu penelitian hukum normatif yang dilakukan dengan cara mengkaji dan meneliti bahan Pustaka atau dokumen yang merupakan data sekunder. Studi kepustakaan ini bertujuan untuk mencari

konsep-konsep, teori-teori, pendapat-pendapat ataupun penemuan-penemuan yang berhubungan dan berkaitan erat dengan pokok permasalahan dalam penelitian ini yaitu mengenai pembuktian *cyber hacking* dan *cracking* .

b. Wawancara

Wawancara merupakan suatu teknik pengumpulan data yang digunakan secara langsung dengan melangsungkan wawancara pada narasumber atau pihak-pihak yang terlibat untuk mendapatkan data pendukung yakni pendukung data sekunder.

5. Alat Pengumpulan Data

Alat pengumpulan data untuk mendapatkan hasil dari studi dokumen atau bahan pustaka dan wawancara untuk menunjang data penelitian ini yaitu :

- a. Alat pengumpulan data dalam penelitian studi dokumen atau kepustakaa berupa buku catatan, laptop, dan handphone.
- b. Alat pengumpulan data dalam penelitian lapangan berupa daftar pertanyaan, handphone, perekam, dan lain – lain.

6. Analisis Data

Analisis dapat dirumuskan sebagai suatu proses penguraian secara sistematis dan konsisten terhadap gejala-gejala tertentu. Dari pengertian yang demikian, nampak analisis memiliki kaitan erat

dengan pendekatan masalah.¹⁸ Oleh karena itu, sebagai metode untuk menarik kesimpulan dari hasil penelitian yang telah terkumpul, akan digunakan metode analisis yuridis-kualitatif. Yuridis, karena penelitian ini dimulai dengan regulasi yaitu peraturan yang ada sebagai norma hukum positif. Sedangkan kualitatif berarti analisis data didasarkan pada upaya untuk menemukan prinsip dan informasi, yang merupakan monograf yang diungkapkan oleh responden atau narasumber.

7. Lokasi Penelitian

a. Perpustakaan

1. Perpustakaan Fakultas Hukum Universitas Pasundan Bandung, Jl. Lengkong Besar No.68 Bandung.
2. Dinas Perpustakaan dan Kearsipan Daerah Provinsi Jawa Barat (DISPUSIPDA JABAR), Jl. Kawaluyaan Indah II No. 4, Soekarno Hatta Bandung

b. Instansi

1. Pengadilan Negeri Bandung Kelas 1 A Khusus, Jl. L. L. R.E. Martadinata No.74-80, Cihapit, Kec. Bandung Wetan, Kota Bandung, Jawa Barat

¹⁸ Soejono Soekanto, *Kesadaran Hukum dan Kepatuhan Hukum*, CV Rajawali, Jakarta, 1982, him.37

2. Kejaksaan Negeri Kabupaten Bandung, Jl. Jaksa Naranata, Baleendah, Kec. Baleendah, Bandung, Jawa Barat