BAB I

PENDAHULUAN

A. Latar Belakang

Peningkatan aktivitas sosial dan ekonomi dengan konsetelasi masyarakat dunia telah memasuki suatu masyarakat yang berorientasi kepada informasi. Sistem informasi dan teknologi telah digunakan pada banyak sektor kehidupan, mulai dari perdagangan/bisnis (*electronic commerce atau e-commerce*), pendidikan (*electronic education*), kesehatan (*tele-medicine*), telekarya, transportasi, industri, pariwisata, lingkungan sampai ke sektor hiburan.[1] Maka dapat kita sadari bahwa dunia sedang berada dalam era informasi (*information age*), yang merupakan tahapan selanjutnya setelah era prasejarah, era agraris dan era industri. [2]

Informasi merupakan inti globalisasi, khususnya bagi Negara-negara yang berambisi membangun dan mewujudkan perubahan.[3] Globlisasi sebagai suatu proses yang pada akhirnya akan membawa seluruh penduduk planet bumi menjadi suatu *world society*.[4] Globalisasi teknologi elektronika, dan informasi komputer telah mempersempit wilayah dunia dan memper pendek jarak komunikasi, di samping memperpadat mobilisasi orang dan barang. Namun perlu kita sadari

---

[1] Danrivanto Budhijanto, 2010, *Hukum Telekomunikasi, Penyiaran dan Teknologi Informasi : Regulasi dan Konvergensi*, Bandung, Refika Aditama, hlm. 1.

[2] Edmon Makarim, 2005, *Pengantar Hukum Telematika*, Jakarta, Raja Grafindo Persada, hlm.27

[3] Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara (Cyber Crime)*. Bandung, Rafika Aditama, hlm. 5.

[4] *Ibid.*, hlm. 6

bahwa, globalisasi membawa dua akibat atau makna. Pada satu sisi melahirkan dunia tanpa batas, menimbulkan keunggulan kompetitif, sementara di sisi lain globalisasi membangkitkan reaksi balik dengan akibat untung rugi.

Era global ini, selain ada hal positif yang bias dimanfaatkan oleh setiap bangsa, khususnya di bidang teknologi, juga menyimpan kerawanan yang tentu saja sangat membahayakan. Bukan hanya soal kejahatan konvensional yang gagal diberantas akibat terimbas oleh pola-pola moderenitas yang gagal mengedepankan prinsip humanitas, tetapi juga munculnya kejahatan jenis baru di alam maya yang telah menjadi realitas masyarakat dunia.

Seiring dengan semakin pesatnya perkembangan komunikasi melalui internet, memunculkan berbagai kejahatan yang dilakukan dengan media internet. Tidak dapat dipungkiri bahwa penggunaan internet yang canggih dan cepat tersebut memunculkan pula kejahatan yang sangat canggih dan sulit untuk diketahui pelakunya. Hal ini disebabkan karena internet merupakan suatu media komunikasi yang tidak terlihat (*maya*), sehingga pelaku kejahatan dapat dengan mudah menghilangkan jejak tanpa dapat diketahui dengan jelas. Kejahatan ini lebih dikenal dengan *cybercrime* atau tindak pidana mayantara.[5]

Mencermati hal tersebut dapatlah disepakati bahwa kejahatan teknologi informasi atau *cybercrime* memiliki karakter yang berbeda

[5] Barda Nawawi Arief, 2006, *Tindak Pidana Mayantara*, Jakarta, PT. Raja Grafindo, hlm. 239.

dengan tindak pidana lainnya baik dari segi pelaku, korban, modus operandi dan tempat kejadian perkara sehingga butuh penanganan dan pengaturan khusus di luar Kitab Undang-Undang Hukum Pidana (KUHP) dan juga Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

Kejahatan *cybercrime* di Negara Indonesia sangat memprihatinkan, yakni data menunjukan bahwa Indonesia berada di urutan kedua dalam daftar lima besar negara asal serangan kejahatan siber atau *cybercrime*, hal ini berdasarkan laporan *State of The Internet* pada tahun 2013. [6] Menurut Rudy Sumadi, *Head of Small and Medium Business Market* Microsoft Indonesia mengatakan bahwa pada tahun 2015 jumlah kasus kejahatan siber di Indonesia meningkat signifikan hingga 389% dari tahun 2014.[7] Hal ini ditegaskan juga oleh Wakil Direktur Tindak Pidana Ekonomi Khusus Bareskrim Polri Kombespol Agung Setya mengatakan, dalam kurun waktu tiga tahun terakhir, tercatat 36,6 juta serangan *cyber crime* terjadi di Indonesia. Sejak 2012 sampai dengan April 2015, Subdit IT/ Cyber Crime telah menangkap 497 orang tersangka kasus kejahatan di dunia maya. Dari jumlah tersebut, sebanyak 389 orang di antaranya merupakan warga negara asing, dan 108 orang merupakan warga negara Indonesia. Total kerugian *cybercrime* di Indonesia mencapai Rp 33,29 miliar. Sementara itu, sepanjang 2012 sampai dengan 2014, terdapat 101

---

[6] Dea Chadiza Syafina, *Indonesia Urutan Kedua Terbesar Negara Asal "Cyber Crime" di Dunia*, 12 Mei 2015 ,http://nasional.kompas.com/read/2015/05/12/06551741/Indonesia.Urutan.Kedua.Terbesar.Negara.Asal.Cyber.Crime.di.Dunia, (11.29).

[7] Redaksi, *Kejahatan Cyber di Indonesia Meningkat*, 28 Novemvber 2016 http://krjogja.com/web/news/read/16701/Kejahatan_Cyber_di_Indonesia_Meningkat. (11.33).

permintaan penyelidikan terhadap kasus *fraud* atau penipuan dari seluruh dunia. Kombespol Agung Setya menyimpulkan bahwa setiap 10 hari terdapat satu kejadian kejahatan *cybercrime* selama tiga tahun terakhir ini.[8]

Jika melihat kuantitas kasus yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi, baik dalam lingkup lokal maupun global (internet) dengan memanfaatkan teknologi informasi berbasis komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual. Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan atau transaksi secara online atau melalui media sosial, khususnya dalam hal pembuktian.

Terkait dengan hukum pembuktian biasanya akan memunculkan sebuah posisi dilema, di salah satu sisi diharapkan agar hukum dapat mengikuti perkembangan zaman dan teknologi, di sisi yang lain perlu juga pengakuan hukum terhadap berbagai jenis-jenis perkembangan teknologi digital untuk berfungsi sebagai alat bukti di pengadilan.[9]

Pembuktian memegang peranan yang penting dalam proses pemeriksaan sidang pengadilan. Pembuktian inilah yang menentukan bersalah atau tidaknya seseorang yang diajukan di muka pengadilan. Apabila hasil pembuktian dengan alat bukti yang ditentukan dengan undang-undang tidak cukup membuktikan kesalahan dari orang tersebut maka akan dilepaskan dari hukuman, sebaliknya apabila kesalahan dapat dibuktikan maka dinyatakan bersalah dan dijatuhi hukuman. Oleh karena

[8] Dea Chadiza Syafina, *Loc. Cit.*

[9] Munir Fuady, 2001, *Teori Hukum Pembuktian (Pidana dan Perdata)*, Bandung, Citra Aditya Bakti, hlm.151.

itu harus berhati-hati, cermat dan matang dalam menilai dan mempertimbangkan masalah pembuktian.

Suatu alat bukti dikatakan sebagai alat bukti yang sah adalah tidak hanya alat bukti tersebut diatur dalam suatu undang-undang (*bewijsmiddelen*) tetapi bagaimana alat bukti tersebut diperoleh dan cara pengajuan alat bukti tersebut di pengadilan (*bewijsvoering*), serta kekuatan pembuktian (*bewijskracht*) atas masing-masing alat bukti yang diajukan tersebut juga sangat mempengaruhi pertimbangan hakim dalam menilai keabsahan suatu alat bukti.

Proses pembuktian pada kasus *cybercrime* pada dasarnya tidak berbeda dengan pembuktian pada kasus pidana konvensional, tetapi dalam kasus *cybercrime* ada beberapa hal yang bersifat elektronik yang menjadi hal utama dalam pembuktian, antara lain adanya informasi elektronik atau dokumen elektronik, ketentuan hukum mengenai pembuktian atas kasus *cybercrime* telah diatur dalam Pasal 5 ayat (1) dan ayat (2) Undang-Undang Nomor 11 Tahun 2008, yang menyatakan bahwa informasi dan atau dokumen elektronik dianggap sebagai alat bukti yang sah dalam proses pembuktian kasus *cybercrime* dan alat bukti elektronik tersebut dianggap pula sebagai perluasan dari alat bukti yang berlaku dalam hukum acara pidana yang berlaku di Indonesia, dalam hal ini alat-alat bukti yang terdapat dalam Pasal 184 KUHAP.[10]

[10] Syaibatul Hamdi, Suhaimi, dan Mujibussalim, "Bukti Elektronik dalam Sistem Pembuktian Pidana", *Jurnal Ilmu Hukum Pascasarjana Universitas Syiah Kuala*, Volume 1 Nomor 4 (November, 2013), hlm. 27.

Kesulitan mendasar penggunaan bukti elektronik dalam proses pembuktian perkara pidana, khususnya mengenai tindak pidana *cybercrime*, yaitu tidak adanya patokan atau dasar penggunaan bukti elektronik di dalam perundang-undangan kita.[11] Dalam penyelesaian tindak pidana di bidang teknologi informasi, kondisi yang *paperless* (tidak menggunakan kertas) ini menimbulkan masalah dalam pembuktian mengenai informasi yang diproses, disimpan, atau dikirim secara elektronik. Informasi atau Dokumen Elektronik yang mudah diubah sering menimbulkan pertanyaan hukum mengenai keotentikan informasi atau dokumen yang dimaksud.[12]

Syarat keabsahan suatu alat bukti elektronik telah disebutkan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terdapat dalam Pasal 6 yakni ....Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan. Unsur dijamin keutuhannya menjadi penting dalam proses pembuktian mengingat Penjelasan Umum Undang-Undang Informasi dan Transaksi Elektronik menyatakan bahwa informasi elektronik ternyata sangat rentan untuk diubah, disadap, dipalsukan, dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik. Dengan demikian, dampak yang

[11] Edmon Makarim, 2005, *Pengantar Hukum Telematika*, Jakarta, Raja Grafindo Persada, hlm. 455.

[12] Josua Sitompul, 2012, *Cyberspace Cybercrimes Cyberlaw Tinjauan Aspek Hukum Pidana*, Jakarta, Tatanusa, hlm. 262.

diakibatkannya pun bisa kompleks dan rumit. Menurut O. C. Kaligis yang menyatakan bahwa belum ada hukum positif Indonesia yang mengatur secara detail, komprehensif serta seragam mengenai keabsahan alat bukti elektronik yang dijamin keutuhannya, sehingga menyebabkan di dalam proses persidangan terjadi perbedaan pendapat dari keterangan ahli mengenai terjaminnya keutuhan alat bukti elektronik tersebut.[13]

Multi tafsir akibat dari pemaknaan unsur dapat diakses, ditampilkan, dijamin keutuhannya dan dapat dipertanggungjawabkan yang berdasarkan Pasal 6 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik bisa berpengaruh terhadap keyakinan hakim dalam menilai dari keabsahan suatu alat bukti elektronik tersebut.

Berdasarkan atas pemaparan dari latar belakang tersebut, bahwa alat bukti elektronik sangatlah diperlukan dalam sidang peradilan, khususnya dalam kasus tindak pidana *cybercrime.* Namun pengaturan mengenai hal tersebut, yakni penentuan mengenai keabsahan alat bukti eleketronik tersebut dapat diterima dalam persidangan belumlah ada mengingat pentingnya alat bukti elektronik dalam membantu mengungkap suatu tindak pidana *cybercrime* dari yang samar-samar sebagai tindak pidana menjadi terang, apakah itu tindak pidana atau bukan. Untuk mengetahui hal tersebut maka perlu diadakan penelitian.

---

[13] O.C.Kaligis, 2012, *Penerapan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Dalam Prakteknya,* Jakarta, Yarsif Watamponehlm. 297.

B. Rumusan Masalah

Berdasarkan uraian-uraian sebagaimana terurai di atas, maka permasalahan hukum yang akan diteliti dalam penelitian ini adalah:

1. Bagaimanakah menentukan keabsahan alat bukti elektronik dalam pembuktian tindak pidana *cybercrime*.
2. Bagaimana penerapan penggunaan alat bukti elektronik dalam pembuktian tindak pidana *cybercrime* .

C. Tujuan Penelitian

Berdasarkan pada pokok permasalahan tersebut di atas, maka tujuan penelitian ini adalah:

1. Untuk mengetahui parameter yang digunakan untuk menentukan keabsahan alat bukti elektronik dalam pembuktian tindak pidana *cybercrime*.
2. Untuk mengetahui penerapan penggunaan alat bukti elektronik dalam pembuktian tindak pidana *cybercrime*.

D. Tinjauan Pustaka

1. Tinjauan Mengenai Tindak Pidana *Cybercrime*

a. Definisi *Cybercrime*

Menurut Didik M. Arif Mansur bahwa pada dasarnya *cybercrime* meliputi semua tindak pidana yang berkenaan dengan sistem informasi, sistem informasi (*information system)* itu sendiri, serta sistem komunikasi yang merupakan sarana untuk

penyampaian/pertukaraan informasi kepada pihak lainnya (*transmitter/originator to recipent).*"[14]

Cybercrime di sisi lain, bukan hanya menggunakan kecanggihan teknologi komputer, akan tetapi juga melibatkan teknologi telekomunikasi di dalam pengoprasiannya. Hal ini dapat dilihat pada pandangan Indra Safitri yang mengemukakan bahwa "kejahatan dunia maya adalah jenis kejahataan yang berkaitan dengan pemaanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang diakses oleh pelanggan internet."[15]

Didalam masalah ini tentunya antara cyber crime membutuhkan *cyberlaw* untuk mengatur dalam *cybercrime* kita juga mengenal istilah *cyber space,* dalam memahami sistem kerja komputer dan telekomunikasi yang menghasilkan internet yang kemudian disebut *cyber space* yang membutuhkan atauran yang disebut dengan *cyberlaw*.

b. Ruang Lingkup Tindak Pidana *Cybercrime*

Membahas ruang lingkup kejahatan telematika (*cybercrime*) adalah hal yang terpenting dalam rangka memberi batasan cakupan kejahatan telematika. Disadarai bahwa

[14] Didik M. Arief Mansur, 2005, *Cyber Law-Aspek Hukum Teknologi Informasi*, Bandung, Refika Aditama, hlm. 10.

[15] Indra Safitri, 1999, *Tindak Pidana di Dunia Cyber*, Jakarta, Insider , hlm. 4.

perkembangan telematika (internet) yang begitu cepat berbanding lurus dengan modus kejahatan yang muncul. Beberapa tahun yang lalu, puluhan ribu pemakai internet terkena virus e-mail *melissa* dan *ex plore.zip.worm* yang meneyebar dengan cepat, menghapuskan arsip-arsip, menghapuskan sistem-sistem, dan menyebabkan perusahaan-perusahaan harus mengueluarkan jutaan dolar untuk mendapatkan bantuan dan batas waktu.[16]

Berangkat pada uraian di atas, maka dapat dikatakan bahawa lingkup cakupan tindak pidana *cybercrime*, yaitu : (a) pembajakan ; (b) peneipuan; (c) pencurian; (d) pornografi; (e) pelecehan; (f) pemfitnahan; dan (g) pemalsuan.

c. Karakteristik Tindak Pidana *Cybercrime*

Berdasarkan beberapa literatur serta praktiknya, menurut Abdul Wahid dan M. Labib *cybercrime* memiliki beberapa karakteristik, yaitu:

1) Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/ wilayah siber/ *cyber (cyberspace),* sehingaa tidak dapat dipastikan yuridiksi negara mana yang berlaku terhadapnya.
2) Perbuatan tersebut dilakukan dengan menggunakan peralatan apa pun yang terhubung dengan internet.

[16] Maskun, 2013, *Kejahata Siber (Cyber crime) Suatu Pengantar,* Jakarta, Kencana, hlm. 50.

3) Perbuatan tersebut mengakibatakan kerugian materiil maupun immateriil (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahsiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
4) Pelakunya adalaah orang yang menguasi penggunaan internet beserta aplikasinya
5) Perbuatan tersebut sering dilakukan secara transnasional melitas batas negara.[17]

d. Bentuk-Bentuk Tindak Pidana C*ybercrime*.

Kejahatan yang berhubungan dengan komputer (*cybercrime)* sudah diatur oleh instrument internasional. Namun dalam UU ITE juga mengatur bentuk *cybercrime* yakni kejahatan yang menjadikan komputer sebagai sasaran kejahatan dan kejahatan konvensional yang menggunakan komputer.[18] Secara umum terdapat beberapa bentuk kejahatan yang berhubungan erat dengan penggunaan teknologi informasi, antara lain :[19]

1) Unauthorized acces to computer system and service
2) Ilegal Contents.
3) Data Forgery
4) Cyber espionage

[17] Abdul Wahid dan M. Labib, 2005, *Kejahatan Mayantara Cybercrime,* Bandung , Refika Aditama, hlm. 45.
[18] Widodo, 2013, *Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law) : Telaah Teoritik dan Bedah Kasus,* Yogyakarta, Aswaja Pressindo, hlm 74.
[19] Budi Suhariyanto, 2012, *Tindak Pidana Teknologi* (*Cybercrime*) *: Urgensi Pengaturan dan Celah Hukumnya,* Jakarta, Raja Grafindo Persada, hlm.14-16.

5) *Cyber Sabotage and extorition*

6) *Offense against intellestual property*

7) *Infrengments of privacy.*

2. Tinjauan Pembuktian Tindak Pidana *Cybercrime*

a. Arti Pembuktian

Yahya Harahap mengemukakan bahwa pembuktian adalah ketentuan-ketentuan yang berisi penggarisan dan pedoman tentang cara-cara yang dibenarkan undang-undang dalam membuktikan kesalahan yang didalwakan kepada terdakawa.[20] Dasar hukum tentang pembuktian dalam hukum acara pidana mengacu pada Pasal 183-189 KUHAP. Menurut Pasal 183 KUHAP bahwa hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya. Ketentuan ini adalah untuk menjamin tegaknya kebenaran, kadilan dan kepastian hukum bagi seseorang.

b. Sistem Pembuktian

Tujuan Hukum Acara Pidana adalah mencari kelemahan materiil dan untuk mencapai tujuan tersebut perlu dipahami adanya beberapa teori/sistem pembuktian. Hakim di Indonesia berperan untuk menilai alat-alat bukti yang diajukan dengan keyakinan

[20] Yahya Harahap, *Op. Cit*, hlm. 273

sendiri. Kewenangan hakim untuk menilai kekuatan alat-alat bukti didasari dengan dapat ditelusuri melalui pemahaman atau 4 (empat) klasifikasi teori/sistem pembuktian di bawah ini:[21]

1. *Conviction-in Time*

   Sistem pembuktian conviction –in Time menetukan salah tidaknya seorang terdakwa, semata-mata ditentukan oleh penilaian "keyakinan" hakim. Keyakinan hakim yang menetukan keteruktian kesalahan terdakwa. Dari mana hakim menarik dan menyimpulkan keyakinan, tidak menjadi masalah dalam sisitem ini.

2. *Conviction-Raisonee*

   Dalam system ini pun dapat dikatakan "keyakinan hakim" tetap memegang peranan penting dalam menentukan salah tidaknya terdakwa. Akan tetapi dalam system ini, factor keyakinan hakim dibatasi, sebab keyakinan hakim harus dengan alasan alasan yang jelas

3. Pembuktian Menurut Undang –Undang Secara Positif

   Pembuktian menurut undang-undang secara positif merupakan pembuktian yang bertolak belakang dengan

[21] *Ibid.,* 277

system pembuktian menurut keyakinan-atau *conviction-in-time.*

4. Pembuktian Menurut Undang-undang Secara Negatif (*Negatief Weterlijk Stelsel)*

   Sistem pembuktian menurut undang-undang secara negative merupakan teori antara system pembuktian menurut undang-undang secara positif dengan system pembuktian menurut keyakinan atau *conviction-in time.*

c. Macam-macam Alat bukti dalam KUHAP

Alat-alat bukti yang dibenarkan undang-undang yang boleh dipergunakan hakim membuktikan kesalahan yang didakwakan. Dalam Pasal 184 ayat (1) KUHAP, alat bukti yang sah ialah:

1) Keterangan saksi
2) Keterangan ahli
3) Surat
4) Petunjuk
5) Keterangan terdakwa

Akibat dari kemajuan teknologi membuat perkembangan tindak pidana semakin beragam sehingga dalam hal pembuktian diterimalah alat-alat bukti elektronik dalam mengungkap kejahatan tersebut. Kedudukan Alat bukti elektronik dalam pembuktian Tindak Pidana yang bersifat konvensional dikategorikan sebagai alat bukti surat maupun alat bukti petunjuk. Namun dalam

Pembuktian Tindak Pidana *cybercrime* Alat bukti elektronik dapat menjadi alat bukti yang sah yang dapat diterima dalam persidangan. Hal tersebut telah diatur dalam Pasal 5 Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Alat bukti elektronik dalam sistem hukum pembuktian di Indonesia terbagi atas dua jenis, yaitu informasi elektronik dan dokumen elektronik. Informasi dan dokumen elektronik ini tidak hanya terbatas pada informasi yang tersimpan dalam medium yang diperuntukkan untuk itu, tetapi juga mencakup transkrip atau hasil cetaknya.

Informasi dan/atau transaksi elektronik maupun hasil cetaknya merupakan alat bukti hukum yang sah, sekaligus merupakan perluasan dari jenis-jenis alat bukti yang diatur dalam perundang-undangan sebelumnya diatur secara tegas dalam Pasal 5 UU ITE. Klasifikasi alat bukti elektronik yakni *Real evidence, Testamentary evidence, dan Circumstantial evidence.*

Informasi elektronik dalam Pasal 1 angka (1) UU ITE didefinisikan sebagai berikut:

> "Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange

(EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya."

Sementara itu, dalam Pasal 1 Angka (4) UU ITE, dokumen elektronik didefinisikan sebagai berikut :

"Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya."

E. Metode Penelitian

1. Jenis Penelitian

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian normatif yaitu, penelitian hukum yang meletakan hukum sebagai sebuah bangunan sistem norma. Sistem norma yang dimaksud adalah mengenai asas-asas norma, kaidah dari peraturan perundangan,

putusan pengadilan, perjanjian serta doktrin (ajaran).[22] Penelitian normatif (penelitian kepustakaan) dalam penelitian ini dengan mencari asas-asas, doktrin-doktrin dan sumber hukum dalam arti filosofis yuridis untuk memahami kedudukan alat bukti elektronik dalam pembuktian tindak pidana *cybercrime* penelitian juga mengacu pada norma-norma hukum yang terdapat dalam peraturan perundang-undangan dan putusan pengadilan yang berkaitan dengan alat bukti elektronik dan pembuktian perkara tindak pidana *cybercrime*. Dengan menggunakan Pendekatan Perundang-undangan dan Analitis, yang mana penelitian menggunakan peraturan perundang-undangan sebagai dasar awal melakukan analisis dengan dilanjutkan dengan mencari makna pada istilah-istilah hukum yang terdapat di dalam perundang-undangan, dengan begitu peneliti memperoleh pengertian atau makna baru dari istilah-istilah hukum dan menguji penerapannya secara praktis dengan menganalisis putusan-putusan hukum.

2. Sumber Data

Sumber data dalam penelitian ini adalah data sekunder, yaitu data yang diperoleh dari hasil penelaahan kepustakaan atau penelaahan terhadap berbagai literatur atau bahan pustaka yang berkaitan dengan masalah atau materi penelitian mengenai alat bukti elektronik sebagai alat bukti yang sah dalam pembuktian tindak pidana *cybercrime.*

[22] Mukti Fajar dan Yulianto Achmad, 2013, *Dualisme Penelitian Hukum Normatif & Empiris,* Yogyakarta, Pustaka Pelajar, hlm. 34.

Untuk menjawab permasalahan utama penelitian ini. Bahan hukum sebagai bahan penelitian diambil dari bahan kepustakaan yang berupa bahan hukum primer, bahan hukum sekunder, bahan hukum tersier dan bahan non hukum.

a. Bahan hukum primer, merupakan bahan pustaka yang berisikan peraturan perundangan yang terdiri dari:
    1) Kitab Undang-undang Hukum Pidana (KUHP);
    2) Undang-undang Nomor 8 Tahun 1981 tentang Kitab Undang-undang Hukum Acara Pidana;
    3) Undang-undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan;
    4) Undang-undang Nomor 36 Tahun 1999 tentang Telekomuniksai;
    5) Undang-undang Nomor 20 Tahun 2001 tentang Perubahan Atas Undang-undang No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi;
    6) Undang-undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme;
    7) Undang-undang Nomor 25 Tahun 2003 tentang Pencucian Uang;
    8) Undang-undang Nomor 21 Tahun 2007 tentang Perdagangan Orang;

9) Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
10) Putusan Nomor 476/Pid. Sus/2013/PN.Slmn, Putusan Nomor 037/Pid. Sus/ 2015/Pn. Smn dan Putusan Nomor 535/Pid. Sus/2016/PN. Smn.

b. Bahan Hukum Sekunder, yaitu bahan-bahan yang erat kaitannya dengan bahan hukum primer, dan dapat membantu untuk proses analisis, yaitu:
1) Buku-buku ilmiah yang terkait;
2) Hasil penelitian terkait;
3) Makalah-makalah seminar yang terkait;
4) Jurnal-jurnal dan literatur yang terkait;
5) Doktrin, pendapat dan kesaksian dari ahli hukum baik yang tertulis maupun tidak tertulis.

c. Bahan Hukum Tersier, yaitu berupa kamus dan ensiklopedi.

d. Bahan Non Hukum, yaitu bahan yang digunakan sebagai pelengkap bahan hukum yaitu:
1) Buku buku tentang Informasi dan Transaksi Elektronik dan Telekomunikasi, dan telekomunikasi maupun ITE, elektronik, dan digital;
2) Hasil penelitian tentang alat bukti elektronik;

3) Hasil penelitian tentang pembuktian tindak pidana *cybercrime*;
4) Hasil penelitian tentang perkara tindak pidana *cybercrime*;
5) Jurnal tentang alat bukti elektroni;
6) Jurnal tentang pembuktian perkara tindak pidana *cybercrime*;
7) Jurnal tentang perkara tindak pidana *cybercrime*.

3. Narasumber

Metode pengumpulan data melalui wawancara terstruktur dengan narasumber sebagai berikut:

a. Bripka Dion Agung N dan Bripka Nur Hariyanto, S. H, Penyidik Madya Unit IT dan Cyber Crime Direktorat Reserse Kriminal Khusus Polda D.I. Yogyakarta;
b. Muh. Ismet Karnawa, S.H., M.H, Jaksa Muda dan Jaksa Penuntut Umum dari Kejaksaan Negeri Sleman;
c. Putu Agus Wiranta, S.H., M.H., Hakim dari Pengadilan Negeri Sleman.

4. Teknik Pengumpulan Data

Teknik Pengumpulan Data yang dilakukan penulis dalam penelitian ini adalah dengan cara sebagai berikut:

a. Study Kepustakaan

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah studi pustaka yakni dengan data sekunder dikumpulkan

dengan melakukan study kepustakaan yaitu, dengan mencari dan mengumpulkan serta mengkaji berbagai peraturan perundang-undangan dan buku-buku yang berhubungan dengan alat bukti elektronik dalam pembuktian tindak pidana *cybercrime*.

b. Wawancara

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah dengan melakukan pengambilan data langsung melalui wawancara dengan Penyidik pada Unit Cybercrime Polda DIY, Jaksa pada Kejaksaan Negeri Sleman, Hakim Pengadilan Negeri Sleman yang pernah mengadili dan memutus kasus tindak pidana *cybercrime* guna mencari jawaban atas keabsahan alat bukti elektronik dalam pembuktian tindak pidana *cybercrime*. Untuk Wawancara teknik pengolahan data adalah dengan cara memeriksa kembali informasi yang diperoleh dari narasumber. Kemudian data-data tersebut diperiksa kelengkapanya dan relevansinya, setelah itu diklasifikasikan sehingga dengan jelas dapat diketahui data yang mana dipergunakan untuk menjawab permaslahan yang ada.

5. Analisis Data

Metode penelitian yang digunakan adalah deskriptif kualitatif, artinya data yang diperoleh akan digambarkan sedemikian rupa dengan tolok ukur peraturan perundang-undangan yang berlaku dan berhubungan dengan judul serta membandingkan dengan teori yang

berlaku dan fakta yang diperoleh. Penyajian analisis dengan memberikan gambaran dan menerangkan data-data dan fakta-fakta yang diperoleh dengan menggunakan narasi atau uraian untuk menjelaskan hasil penelitian. Dipilih data-data yang ada kaitannya dengan permasalahan dan dapat digambarkan keadaan sebenarnya dilapangan. Hal ini diharapkan dapat memudahkan dalam memahami kendala kondisi di lapangan.

F. Sistematika Penulisan

Pembahasan dalam skripsi ini agar dapat sistematis dan mudah dipahami maka disusun dalam beberapa bagian. Penulis membagi penulis telah membagi penulisan ini menjadi 5 (lima) bab. Bagian dalam penulisan hukum (skripsi) yang dibuat oleh penulis adalah sebagai berikut:

Bab pertama merupakan bab pendahuluan yaitu membahas tentang latar belakang masalah, rumusan masalah, tujuan penelitian, tinjauan pustaka, metode penelitian dan sistematika penulisan. Bab pertama ini dalam latar belakang masalah yaitu merupakan pemaparan pentingnya penelitian ini dan mengapa peneliti memilih untuk meneliti tentang kedudukan alat bukti elektronik sebagai alat bukti yang sah dalam pembuktian tindak pidana *cybercrime*. Kemudian rumusan masalah memiliki tujuan yaitu untuk mengetahui jawaban dari permasalahan yang akan diteliti dan kegunaan penelitian. Tujuan penelitian berguna untuk memberikan pemahaman kepada masyarakat maksud dari dilakukan penelitian ini. Tinjauan pustaka berfungsi sebagai dasar tentang penelitian

kedudukan alat bukti elektronik dalam pembuktian tindak pidana *cybercrime*. Metode penelitian yaitu menjelaskan tentang metode-metode yang akan digunakan untuk menganalisis permasalahn dalam penelitian, dan sistematika pembahasan.

Bab kedua, menjelaskan mengenai gambaran umum tentaang tindak pidana *cybercrime* dari pengertian tindak pidana *cybercrime*, bentuk-bentuk tindak pidana *cybercrime*, pengaturan tindak pidana *Cybercrime* di Indonesia, Yurisprudensi dalam tindak pidana *Cybercrime* di Indonesia, faktor-faktor yang mempengaruhi meningkatnya Tindak Pidana *cybercrime*, dan Penegakan Hukum terhadap tindak pidana *Cybercrime* di Indonesia.

Bab ketiga, membahas mengenai pembuktian tindak pidana *cybercrime* dari pengertian pembuktian, sistem pembuktian, alat-alat bukti, pengertian alat bukti elektronik, pengaturan alat bukti elektronik.

Bab keempat, menganalisis mengenai penetuan keabsahan alat bukti elektronik dalam pembuktian tindak pidana *cybercrime* serta penerapan penggunaan alat bukti elektronik sebagi alat bukti yang sah dalam pembuktian tindak pidana *cybercrime*.

Bab kelima, berupa kesimpulan dari jawaban atas rumusan masalah dan memberikan saran atau rekomedasi sebagai bahan refleksi bagi semua pihak terkait temuan-temuan berdasarkan peraturan dan berdasarkan teori-teori hukum mengenai kedudukan alat bukti elektronik sebagai alat bukti yang sah dalam pembuktian tindak pidana *cybercrime*.