BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Salah satu tujuan Negara Republik Indonesia (selanjutnya disebut NRI) dalam Alinea ke-4 Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (selanjutnya disebut UUD Tahun 1945) adalah melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia. Melindungi dalam hal ini salah satunya adalah melindungi rakyat Indonesia dari ancaman kejahatan yang bisa mengganggu ketertiban masyarakat, bangsa dan Negara, salah satunya adalah kejahatan dengan menggunakan sarana teknologi informasi (*information technology*/IT).

Pesatnya perkembangan teknologi informasi[1] tidak hanya berdampak positif terhadap umat manusia sebagai pengguna (*user*), namun tidak sedikit pula memberi kontribusi negatif terhadap meningkatnya angka kejahatan yang menggunakan perangkat teknologi informasi. Jika sebelum era teknologi informasi, pola kejahatan dilakukan secara konvensional, maka saat ini kejahatan dilakukan lebih canggih dengan

[1] Perkembangan Teknologi Informasi memacu suatu cara baru dalam kehidupan, dari kehidupan dimulai sampai dengan berakhir, kehidupan seperti ini dikenal dengan *e-life*, artinya kehidupan ini sudah dipengaruhi oleh berbagai kebutuhan secara elektronik. Dan sekarang ini sedang semarak dengan berbagai huruf yang dimulai dengan awalan "e" seperti *e-commerce*, *e-government*, *e-education*, *e-library*, *e-journal*, *e-medicine*, *e-laboratory*, *e-biodiversity*, dan yang lainnya lagi yang berbasis elektronika, dikutip dari: Utama Andri, *Mata Diklat: Pengenalan Teknologi Informasi*, Materi Pelengkap Modul (Bahan Ajar) Diklat Fungsional Pranata Komputer Tingkat Ahli, Pusat Pendidikan Dan Pelatihan Badan Pusat Statistik RI (PUSDIKLAT BPS RI), Jakarta, 2019, hal 1.

menggunakan beragam sarana, termasuk teknologi informasi yang tersedia bebas di pasaran. Teknologi informasi sendiri dapat dikelompokkan menjadi 6 (enam) teknologi, yaitu teknologi komunikasi, teknologi masukan, teknologi keluaran, teknologi perangkat lunak, teknologi penyimpanan, dan teknologi mesin pemrosesan.[2] Dalam hal ini, teknologi komunikasi dengan menggunakan perangkat *mobile phone*, menjadi media atau sarana yang paling sering digunakan oleh pelaku kejahatan, selain komputer.

Sejumlah istilah digunakan untuk menyebut kejahatan yang menggunakan perangkat teknologi informasi, seperti kejahatan komputer (*computer crime*), kejahatan siber (*cybercrime*), kejahatan mayantara atau kejahatan telematika. Pada beberapa literatur menyebutkan bahwa apa yang disebut dengan kejahatan telematika (konvergensi), itu pula yang disebut kejahatan *cyber*.[3] Semua istilah dalam kejahatan ini menggunakan perangkat teknologi informasi dalam menjalankan aksinya. "Induk" dari *cybercrime* adalah apa yang disebut dengan "*cyber space*". *Cyber space* dipandang sebagai sebuah dunia komunikasi yang berbasis komputer. Dalam hal ini, *cyber space* dianggap sebagai sebuah realitas baru dalam kehidupan manusia yang dalam bahasa sehari-hari dikenal dengan internet.[4]

---

[2] *Ibid* hal 3.

[3] Judhariksawan, *Pengantar Hukum Telekomunikasi*, Rajawali Press, Jakarta, 2005, hal 12-13.

[4] Maskun, *Kejahatan Siber (Cyber Crime); Suatu Pengantar*, Penerbit Kencana Prenada Media Group, Jakarta, 2013, hal 47.

Kejahatan di bidang teknologi informasi dan komunikasi memiliki karakteristik unik yaitu: 1) bersifat global (melintasi batas negara), menyebabkan sulit menentukan yurisdiksi hukum negara mana yang berlaku terhadapnya; 2) sifat kejahatan, tidak menimbulkan kekacauan yang mudah terlihat (*non-violence*), sehingga ketakutan terhadap kejahatan tersebut tidak mudah timbul; 3) pelaku kejahatan, pelakunya tidak mudah diidentifikasi, namun memiliki ciri khusus yaitu pelakunya menguasai penggunaan internet/komputer; 4) modus kejahatan, hanya dapat dimengerti oleh orang yang mengerti dan menguasai bidang teknologi informasi; 5) jenis kerugian, kerugian yang ditimbulkan lebih luas, termasuk kerugian di bidang politik, ekonomi, sosial dan budaya. [5]

Beberapa jenis kejahatan siber yang berkembang di era digital ini antara lain: 1) *unauthorized access*, yaitu jenis kejahatan dengan cara menyusup ke dalam sistem komputer tanpa izin dan tanpa sepengetahuan pemilik sistem. Dengan cara ini, pelaku dapat mencuri data-data pemilik sistem sehingga dapat melakukan pembajakan dan perusakan sistem (*hacking* dan cracking). 2) *illegal contents*, yaitu jenis kejahatan berupa penyebaran sesuatu yang menyesatkan ataupun tidak etis yang melanggar norma-norma masyarakat seperti misalnya penyebaran berita bohong (hoax) dan penyebaran konten pornografi. 3) penyebaran virus, kejahatan dengan tujuan melumpuhkan perangkat korban hingga

[5] Abdul Wahid dan Mohamad Labib. *Kejahatan Mayantara (Cyber Crime).* Refika Aditama, Bandung, 2005.

pencurian dan perusakan data dengan cara menyusupkan virus seperti yang terkenal adalah *trojan* dan *ransomware*.[6]

Data dari elektronik Manajemen Penyidikan (e-MP) Robinopsnal Markas Besar Kepolisian Republik Indonesia (selanjutnya disebut Mabes Polri) menyebutkan sejak 1 Januari hingga 22 Desember 2022, Kepolisian menindak 8.831 kasus kejahatan dengan menggunakan sarana teknologi informasi atau kejahatan siber (*cyber*). Seluruh satuan kerja di Bareskrim Polri dan Kepolisian Daerah (selanjutnya disebut Polda) di Indonesia melakukan penindakan terhadap kasus tersebut. Polda Metro Jaya menjadi satuan kerja dengan jumlah penindakan paling banyak terhadap kasus kejahatan siber yaitu 3.709 perkara.[7] Sementara pada periode yang sama di 2021, jumlah penindakan yaitu 612 di seluruh Indonesia. Hanya 26 satuan kerja yang melakukan penindakan.

Kejahatan siber ini dalam bentuk beragam. Data penindakan Polri dalam kurun waktu tersebut memetakan 10 (sepuluh) jenis kasus dengan jumlah penindakan terbanyak. Kesepuluh jenis itu yaitu; 1) manipulasi data autentik (3.723 kasus); 2) penipuan melalui media elektronik (2.131 kasus); 3) *cybercrime* (1.098 kasus); 4) pencemaran nama baik melalui media elektronik dan yang juga berbentuk persekusi (835 kasus); 5) mengakses sistem secara tidak sah (38 kasus); 6) judi online (164 kasus); 7) pengancaman melalui media elektronik/medsos dan juga yang

[6] *Ibid*.

[7] "Kejahatan Siber di Indonesia Naik Berkali-kali Lipat", dikutip dari https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat. Data akses 15 Mei 2023 pukul 22.25 wita.

berbentuk persekusi (145 kasus); 8) pornografi atau prostitusi melalui media elektronik (143 kasus); 9) penghinaan melalui media elektronik dan yang juga berbentuk persekusi (59 kasus); dan 10) *hate speech* (43 kasus).[8]

Perkembangan kejahatan dengan menggunakan perangkat elektronik, tentu menjadi tantangan penegakan hukum itu sendiri. Jika awalnya terhadap kejahatan konvensional[9] penegakan hukumnya juga dilakukan secara konvensional, maka terhadap kejahatan elektronik, perlakuannya tentu berbeda. Dibutuhkan perangkat hukum yang memadai, baik dari sisi peraturan perundang-undangan, maupun kualitas sumber daya manusia. Substansi hukum dalam peraturan perundang-undangan yang mengatur tindak pidana elektronik harus mampu membaca dan mengenali karakter kejahatan elektronik yang membedakannya dengan kejahatan konvensional. Pun juga, sumberdaya manusia dalam hal ini aparat penegak hukum dibekali dengan penguatan pengetahuan dan teknis penyelidikan dan penyidikan kejahatan elektronik yang tentu berbeda dengan penyelidikan dan penyidikan kejahatan konvensional. Perpaduan dua aspek itu diharapkan akan mampu mewujudkan penegakan hukum yang maksimal terhadap penindakan kejahatan elektronik. Hukum tidak boleh tertinggal dari kejahatan itu sendiri karena dapat berakibat fatal terhadap ketertiban masyarakat,

[8] *Ibid*.

[9] Kejahatan konvensional yang dimaksud adalah kejahatan yang tidak menggunakan perangkat elektronik, atau menggunakan perangkat elektronik namun bukan sebagai tindak pidana elektronik.

bangsa dan Negara. Dapat dibayangkan apabila kejahatan berkuasa diatas hukum, apabila dikaitkan dengan pepatah belanda "*het recht hinkt achter de feiten aan*" (*the law lags behind the facts*) yang dapat diterjemahkan dengan bebas bahwa "hukum selalu tertatih-tatih mengejar perkembangan zaman".[10]

Sehubungan dengan hal itu, tantangan terberat dalam penegakan hukum tindak pidana elektronik adalah ketersediaan, kecukupan dan kualitas alat bukti. Alat bukti dalam setiap perkara, termasuk tindak pidana elektronik, memegang peran penting untuk menentukan apakah seseorang bersalah melakukan tindak pidana atau tidak. Alat bukti elektronik berbeda dengan alat bukti konvensional. Bukti elektronik mempunyai karakteristik yang khas yaitu tidak terlihat, sangat rapuh karena mudah berubah, mudah rusak karena sensitif terhadap waktu, mudah dimusnahkan, dan mudah dimodifikasi (rekayasa). Di samping itu, bukti elektronik juga dapat berpindah dengan mudah, serta jika akan melihat atau membacanya memerlukan bantuan alat, baik itu alat yang berupa perangkat keras (*hardware*) maupun perangkat lunak (*software*).[11]

---

[10] Dalam ilmu kriminologi dan literatur hukum, kita sering menjumpai idiom atau ungkapan bahasa Belanda yang berbunyi "*achter de feiten aanlopen*" yang dalam bahasa Inggris diterjemahkan menjadi "*lag behind events*" atau dalam bahasa Indonesia berarti "tertinggal dari peristiwa/kenyataan". Dalam dunia hukum tertulis sering kita menjumpai ungkapan "*het recht hinkt achter de feiten aan*" *(the law lags behind the facts*) yang dapat diterjemahkan dengan bebas bahwa "hukum selalu tertatih-tatih mengejar perkembangan zaman", dikutip dari Laode M. Syarif (mantan Komisioner KPK), "Melawan Stigma "Penegak Hukum Selalu Tertinggal", pengantar dalam Jurnal Integritas, Vol 4. No2. 2018.

[11] Army, H. Eddy, *Bukti Elektronik Dalam Praktik Peradilan*, Sinar Grafika: Jakarta, 2020, hlm. 105.

Dasar pemikiran lahirnya Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE),[12] karena karakteristik kekhususan yang melekat pada informasi elektronik dan sistem elektronik. Ketentuan hukum yang ada dirasakan belum dapat menjangkau perkembangan yang demikian pesat, bahkan optimalisasi ketentuan yang ada pun dirasakan kurang memberikan jawaban dan tidak sesuai dengan keunikan yang melekat pada sistem elektronik tersebut. Oleh karenanya, hadirnya UU ITE adalah dalam rangka menjawab kebutuhan tersebut. Keberadaan UU ITE ditujukan agar dapat dipergunakan untuk menjawab semua permasalahan hukum yang ada sepanjang melibatkan informasi elektronik dan/atau dokumen elektronik sebagai alat buktinya. Karena hanya dalam UU ITE diatur lebih khusus bagaimana suatu informasi elektronik dan/atau dokumen elektronik menjadi alat bukti yang sah di muka pengadilan.[13]

Sebelum, bahkan setelah lahirnya UU ITE, tetap terjadi perbedaan yang tajam soal kapan bukti elektronik menjadi alat bukti elektronik, serta sejauhmana bukti elektronik dapat diakui sebagai alat bukti hukum yang sah dari sisi pembuktian. Kaligis menyatakan bahwa belum ada hukum positif Indonesia yang mengatur secara detail, komprehensif serta seragam mengenai keabsahan alat bukti elektronik yang dijamin

[12] Diubah dengan Undang-Undang Nomor 19 Tahun 2016 (perubahan) pertama, dan Undang-Undang Nomor 1 Tahun 2024 (perubahan kedua)

[13] Edmon Makarim, *Notaris dan Transaksi Elektronik; Kajian Hukum Tentang Cybernotary Atau Electronic Notary*, edisi ke-3, Rajawali Pres, Jakarta, 2020, hlm 34.

keutuhannya.[14] Pernyaaan ini menarik karena dikeluarkan pada saat UU ITE telah berlaku. Tidak hanya itu, perbedaan pendapat juga mengomentari soal apakah bukti elektronik merupakan perluasan dari alat bukti dalam Pasal 184 KUHAP[15] atau berdiri sendiri.[16]

Pasca lahirnya UU ITE, silang pendapat ini terakomodir dalam Pasal 5 ayat (1) UU ITE yang menerangkan bahwa informasi elektronik[17] dan/atau dokumen elektronik[18] dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Kemudian ayat (2) menerangkan bahwa bukti elektronik merupakan perluasan dari alat bukti yang sah, sesuai dengan hukum acara yang berlaku di Indonesia. Pada prinsipnya informasi elektronik dapat dibedakan tetapi tidak dapat dipisahkan dengan dokumen elektronik. Informasi elektronik ialah data atau kumpulan data dalam berbagai bentuk, sedangkan dokumen elektronik ialah wadah atau 'bungkus' dari informasi elektronik.

---

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

[15] Pasal 184 KUHAP, alat-alat bukti yang sah adalah: 1) keterangan saksi, 2) keterangan ahli, 3) surat, 4) petunjuk, dan 5) keterangan terdakwa.

[16] Perbedaan ini dapat dibaca dalam buku Edmon Makarim, *Op.cit*

[17] Pasal 1 angka 1 UU ITE: 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.

[18] Pasal 1 angka 4 UU ITE: 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.

Pasal 5 ayat (1) UU ITE dapat dikelompokkan menjadi dua bagian. Pertama informasi elektronik dan/atau dokumen elektronik. Kedua, hasil cetak dari informasi elektronik dan/atau hasil cetak dari dokumen elektronik. Informasi elektronik dan dokumen elektronik tersebut yang akan menjadi Alat Bukti Elektronik (*Digital Evidence*). Sedangkan hasil cetak dari informasi elektronik dan dokumen elektronik akan menjadi alat bukti surat. Pasal 5 ayat (2) UU ITE mengatur bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan perluasan dari alat bukti hukum yang sah sesuai dengan hukum acara yang berlaku di Indonesia. Yang dimaksud dengan perluasan di sini harus dihubungkan dengan jenis alat bukti yang diatur dalam Pasal 5 ayat (1) UU ITE. Perluasan di sini maksudnya:[19] a. Menambah alat bukti yang telah diatur dalam hukum acara pidana di Indonesia, misalnya Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP). Informasi elektronik dan/atau dokumen elektronik sebagai Alat Bukti Elektronik menambah jenis alat bukti yang diatur dalam KUHAP; b. Memperluas cakupan dari alat bukti yang telah diatur dalam hukum acara pidana di Indonesia, misalnya dalam KUHAP. Hasil cetak dari informasi atau dokumen elektronik merupakan alat bukti surat yang diatur dalam KUHAP.

Selain dalam UU ITE, alat bukti elektronik juga diatur dalam sejumlah peraturan perundang-undangan dengan predikat "*serious crime*". Dalam

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

tindak pidana pencucian uang, bukti elektronik diatur dalam Pasal 73 Undang-Undang Nomor 8 Tahun 2010 (UU TPPU). Dalam Undang-Undang Nomor 20 Tahun 2001 Tentang Pemberantasan Tindak Pidana Korupsi,[20] bukti elektronik diatur dalam Pasal 26A sebagai perluasan alat bukti petunjuk. Dalam Undang-Undang Nomor 15 Tahun 2003 (UU Terorisme), alat bukti elektronik diatur dalam Pasal 27. Dalam Undang-Undang Nomor 35 Tahun 2009 Tentang Narkotika (UU Narkotika), alat bukti elektronik diatur dalam Pasal 86. Dalam Undang-Undang Nomor 21 Tahun 2007 Tentang Pemberantasan Tindak Pidana Perdagangan Orang (UU TPPO), bukti elektronik diatur dalam Pasal 29. Dalam UU Perlindungan Data Pribadi, alat bukti elektronik diatur dalam Pasal 64. Terhadap alat bukti elektronik dalam perundang-undangan tersebut diatas, berdiri sendiri, tidak terikat dengan UU ITE sebagaimana diterangkan dalam Pasal 5 ayat (4) UU ITE No 1 Tahun 2024.[21]

Meskipun berdiri sendiri, alat bukti elektronik dalam perundang-undang tersebut diatas tetap terikat dengan Pasal 5 ayat (3) UU ITE yang mensyaratkan bahwa Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini. Silogismenya adalah, pengaturan alat bukti elektronik dalam perundang-undangan tersebut

[20] Perubahan Undang-Undang Nomor 31 Tahun 1999.

[21] Perubahan Kedua UU ITE No 11 Tahun 2008. Pasal 5 ayat (4) UU ITE: Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (l) tidak berlaku dalam hal diatur lain dalam Undang-Undang.

diatas tidak akan dinyatakan sah sebagai alat bukti apabila tidak menggunakan sistem elektronik dalam proses pengumpulannya.

Edmon Makarim menerangkan bahwa pada dasarnya melihat kedudukan informasi elektronik tidak dapat lepas dari karakteristik sistem elektronik yang menjadi dasar pemprosesannya, sementara keberadaannya pun harus dilihat berdasarkan kontekstualnya. Sementara itu, letak dan karakteristik media penyimpanannya juga menentukan reliabilitasnya, apakah informasi elektronik tersebut tersimpan pada suatu media sekunder (contoh: *computer stored data*) secara *offline*, ataukah informasi elektronik yang diterima dari suatu sistem komunikasi secara elektronik (contoh: *communication data message*). Varian pertama mempunyai kriteria keutuhan, otorisasi, dan autentisitas, sementara untuk varian kedua ditambah lagi dengan kriteria kerahasiaan dan nir-sangkal. Pemahaman tersebut diatas akan memperlihatkan bahwa sesungguhnya terdapat rentang atau spectrum dalam menentukan nilai pembobotan terhadap kekuatan pembuktian suatu informasi elektronik, dari yang paling lemah sampai yang paling kuat.[22]

Bukti di dalam Kamus Besar Bahasa Indonesia adalah sesuatu yang menyatakan kebenaran suatu peristiwa; keterangan nyata; atau tanda.[23] Sedangkan yang dimaksud alat bukti adalah segala sesuatu hal maupun benda yang ada hubungan dan kaitannya dengan suatu kejadian atau peristiwa tertentu. Soebekti mendefinisikan bukti sebagai sesuatu untuk

[22] Edmon Makarim, *Op.cit.,*hlm 29.
[23] https://kbbi.web.id/bukti.

meyakinkan akan kebenaran suatu dalil atau pendirian. Sedangkan alat bukti, alat pembuktian, upaya pembuktian (*Bewisjemiddle*) adalah alat-alat yang dipergunakan untuk dipakai membuktikan dalil-dalil suatu pihak dimuka pengadilan. Misalnya, bukti-bukti tulisan, kesaksian, persangkaan, sumpah.[24]

Di dalam dunia peradilan, pembuktian adalah proses terpenting dalam persidangan, baik itu dalam perkara pidana maupun perdata. Pembuktian merupakan titik sentral pemeriksaan perkara dalam sidang pengadilan. Ia berisikan ketentuan-ketentuan mengenai pedoman tentang tata cara yang dibenarkan undang-undang untuk membuktikan kesalahan yang didakwakan kepada terdakwa. Undang-Undang Nomor 1 Tahun 1981 Tentang Hukum Acara Pidana (selanjutnya disebut KUHAP) telah mengatur alat-alat bukti yang dibenarkan undang-undang yang boleh dipergunakan hakim dalam membuktikan kesalahan yang didakwakan, sehingga majelis hakim tidak bisa secara subjektif memvonis terdakwa.[25] Berdasarkan Pasal 184 KUHAP, alat-alat bukti yang sah adalah: 1) keterangan saksi, 2) keterangan ahli, 3) surat, 4) petunjuk, dan 5) keterangan terdakwa.

Ketika perdebatan soal alat bukti elektronik dianggap telah diakomodir dalam Pasal 5 ayat (1) dan (2) UU ITE, masalah lain yang penting untuk dipastikan adalah soal keabsahan bukti elektronik.

---

[24] Soebekti dan R Tjitrosoedibio, *Kamus Hukum,* Pradnya Paramita, Jakarta, 1980, hal 21.

[25] Andi Hamzah, *Hukum Acara Pidana Indonesia*, Edisi Kedua, Sinar Grafika, Jakarta, 2015.

Bagaimana informasi elektronik dan dokumen elektronik dalam Pasal 5 ayat (1), sebagai “perluasan dari alat bukti hukum yang sah sesuai dengan hukum acara yang berlaku di Indonesia” dalam ayat (2) yang mana merujuk pada Pasal 184 KUHAP, bisa “dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini” dalam ayat (3).

Memang penjelasan soal sistem elektronik dalam ayat (3) tersebut diterangkan dalam Pasal 16 UU ITE bahwa sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum: a. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan; b. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut; c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut; d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau symbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Penjelasan tentang sistem elektronik tersebut diatas tetap tidak menjawab pertanyaan penting, dengan cara apa bukti elektronik (misalnya yang diperoleh dari kegiatan penyelidikan dan penyidikan tindak pidana) bisa diakui sebagai alat bukti (elektronik) hukum yang sah dalam Pasal 5 UU ITE? Bagaimana bisa memastikan jika informasi atau dokumen elektronik tersebut; a. dapat dijamin keotentikannya, keutuhannya, ketersediaannya, dan dapat dipertanggungjawabkan, sehingga menerangkan suatu keadaan; b. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi; c. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan; d. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut; e. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau symbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan f. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk? UU ITE dan peraturan perundang-undangan yang menyangkut tindak pidana dengan predikat "*serious crime*", tidak menjelaskan itu.

Sebagaimana diterangkan Edmon Makarim dalam prinsip kesetaraan fungsional (*functional equivalent approach*), bahwa agar informasi elektronik dan/atau dokumen elektronik dapat dikatakan sama dengan bukti tertulis sehingga memiliki kekuatan pembuktian, maka harus

dipenuhi tiga dasar, yaitu; pertama, dapat disimpan dan ditemukan kembali; kedua, tidak berubah substansinya (terjamin keautentikannya), serta bertandatangan apabila terdapat informasi yang menjelaskan adanya suatu subjek hukum yang bertanggung jawab diatasnya atau terdapat sistem autentikasi yang realible yang menjelaskan identitas dan otoritas atau verifikasi dari pihak tersebut.[26] Maka, bagaimana cara kerja sistem elektronik yang dimaksud dalam Pasal 5 ayat (3) UU ITE itu mampu menghasilkan apa yang dituntut dalam prinsip kesetaraan fungsional tersebut juga tidak melalui proses yang ter-autentikasi.

Meskipun dipahami jika Pasal 5 UU ITE berlaku secara umum, dalam arti digunakan untuk semua pembuktian dalam setiap perkara, tidak hanya perkara pidana, lebih khusus lagi tindak pidana elektronik, namun setidak-tidaknya, untuk menciptakan kepastian hukum, ada norma yang menguatkan penggunaan sistem elektronik dalam Pasal 5 ayat (3), bahwa "sistem elektronik" yang dimaksud dalam Pasal 5 ayat (3) tersebut salah satunya atau misalnya dengan menggunakan digital forensik. Karena hanya dengan digital forensik, informasi elektronik atau dokumen elektronik dalam Pasal 5 UU ITE, maupun alat bukti elektronik yang tersebar dalam undang-undang yang mengatur tindak pidana dengan predikat *serious crime*, dapat membuat terang peristiwa pidana karena telah melalui proses *scientific crime*, sehingga dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan, sehingga

[26] Edmon Makarim, (2015), *Keotentikan Dokumen Publik Elektronik Dalam Administrasi Pemerintahan Dan Pemerintahan Publik*, Jurnal Hukum dan Pembangunan, No. 4., hlm 532.

menerangkan suatu keadaan. Dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi; c. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan.

Frasa "…menggunakan sistem elektronik.." dalam Pasal 5 ayat (3) UU ITE masih absurd dan jamak karena tidak menjelaskan sistem elektronik seperti apa yang dimaksud. UU ITE tersebut tidak dijelaskan dengan rinci dengan cara apa suatu bukti elektronik dapat diakses, ditampilkan, dijamin keutuhannya dan dapat dipertanggungjawabkan. Sehingga hal ini menimbulkan suatu kekaburan hukum yang menyebabkan masih adanya perkara-perkara khususnya perkara *cybercrime* yang tidak menerapkan digital forensik dalam pembuktiannya.

Frasa "sistem elektronik" dalam frasa dimaksud tidak merujuk pada misalnya yang dikenal dengan "digital forensik". Sementara digital forensik sendiri tidak menjadi norma untuk menjelaskan jika sistem elektronik yang dimaksud dalam Pasal *a quo* adalah digital forensik. Situasi demikian berpengaruh terhadap penilaian hakim terhadap bukti elektronik dalam sidang pembuktian. Tidak ada pedoman Mahkamah Agung terhadap kualitas bukti elektronik yang dihadirkan di pengadilan. Dalam memeriksa dan memutus tindak pidana elektronik, Hakim sebatas meyakini jika bukti elektronik yang dihadapkan dalam sidang pembuktian adalah bukti elektronik yang diajukan oleh penuntut umum. Hakim tidak sampai pada dengan cara apa suatu bukti elektronik dapat diakses, ditampilkan, dijamin

keutuhannya dan dapat dipertanggungjawabkan secara hukum sebagai alat bukti.

Ketika kepolisian mengusut sebuah kasus tindak pidana yang dalam menjalankan modus operandinya menggunakan media teknologi informasi, maka cara yang digunakan tentu berbeda ketika mengusut kasus tindak pidana biasa. Pengumpulan data informasi dari perangkat teknologi informasi yang disita sebagai barang bukti membutuhkan teknik-teknik tertentu yang hanya dipahami oleh seseorang yang menguasai pengetahuan di bidang teknologi informasi. Apalagi ketika pada situasi dimana data dan informasi tersebut telah dihapus oleh pelaku kejahatan untuk menghilangkan jejak atau bukti, maka cara yang dilakukan adalah dengan menggunakan digital forensik guna melacak kembali data dan informasi yang telah dihapus tersebut untuk membuat terang sebuah peristiwa pidana.

Pengumpulan bukti kejahatan tersebut dengan melakukan analisis menggunakan digital forensik kepolisian. Digital forensik merupakan ilmu yang membahas tentang temuan yang berupa bukti digital setelah peristiwa yang berkaitan dengan keamanan komputer terjadi. Digital forensik bisa dikatakan penerapan ilmu pengetahuan untuk memulihkan bukti digital dari suatu perangkat baik itu komputer maupun *smartphone* dengan metode tertentu yang bertujuan untuk mengumpulkan data yang

dapat diterima oleh pengadilan sebagai salah satu pembuktian.[27] Salah satu media digital forensik adalah *mobile forensic*. Mobile forensik bertujuan untuk melakukan pengembalian data dari perangkat mobile.

Proses digital forensik dan mobile forensik tersebut biasa digunakan Kepolisian dalam melakukan penyelidikan atau penyidikan dalam kasus dugaan tindak pidana penyalahgunaan informasi teknologi. Proses pengumpulan bahan dan data tersebut menjadi barang bukti, dan setelah dipilah sesuai kebutuhannya, menjadi alat bukti yang akan dihadirkan di persidangan. Pembuktian di dalam sebuah hukum pidana merupakan suatu yang sangat penting dan utama. Dalam Pasal 6 ayat (2) Undang-Undang Nomor 48 Tahun 2009 tentang Kekuasaan Kehakiman (selanjutnya disebut UU Kekuasaan Kehakiman), dinyatakan tidak seorangpun dapat dijatuhi pidana kecuali apabila pengadilan, karena alat pembuktian yang sah menurut undang-undang, mendapat keyakinan bahwa seorang yang dianggap dapat bertanggung jawab, telah bersalah atas perbuatan yang didakwakan atas dirinya. Dalam perkara pidana, pembuktian perkara bertujuan untuk mencari kebenaran material, yaitu kebenaran sejati atau sesungguhnya.[28] Berbeda dengan perkara perdata, dimana pembuktian bertujuan untuk mencari kebenaran formil, yang artinya hakim tidak boleh melampaui batas-batas yang diajukan oleh para pihak yang berperkara. Hakim dalam mencari kebenaran formal cukup

[27] Deris Setiawan, *Sistem Keamanan Komputer*, PT. Elex Media. Komputindo: Jakarta, 2005.

[28] Yahya Harahap, *Pembahasan Permasalahan dan Penerapan KUHAP Penyidikan dan Penuntutan*. Sinar Grafika, Jakarta, 2006, hal 101.

membuktikan dengan "*preponderance of evidence*", sedangkan hakim pidana dalam mencari kebenaran material, maka peristiwanya harus terbukti.[29]

Pada situasi demikian, digital forensik memegang peran penting dalam memudahkan penyidik untuk melakukan pelacakan terhadap pelaku atau jaringannya, termasuk modus operandi yang digunakan. Bukti yang dikumpulkan tersebut dinamakan bukti elektronik. Melalui bukti elektronik, dapat diketahui perencanaan (motif) suatu kejahatan melalui berbagai media seperti *e-mail*, telepon, aplikasi *chat* online, pesan dalam gambar, suara, video, dan media-media lain.[30]

Karena bukti elektronik yang diperoleh dari sistem elektronik tidak menjamin serta merta dianggap sebagai alat bukti elektronik. pertimbangan dalam Putusan Mahkamah Konstitusi Nomor: 20/PUU/XIV/2016, poin [3.11]., disebutkan bahwa rekaman - termasuk bukti elektronik lainnya - memiliki nilai pembuktian oleh pengadilan dengan memperhatikan parameter pembuktian pidana "*bewijsvoering*" penguraian cara mengajukan alat bukti kepada hakim di persidangan. Alat bukti yang diperoleh penegak hukum secara tidak sah (*unlawful legal evidence*) akan dikesampingkan oleh hakim atau dianggap tidak mempunyai nilai pembuktian oleh pengadilan.[31] *Bewijsvoering* pada dasarnya sangat terkait erat dengan fundamental

[29] *Ibid*.

[30] Efa Laela Fakhira, *Kedudukan Bukti Elektronik Sebagai Alat Bukti di Pengadilan* Art Pers: Bandung, 2008, hal. 8.

[31] Putusan Mahkamah Konstitusi Nomor: 20/PUU/XIV/2016, hlm 40.

pembuktian yang disebut dengan *exclusionary rules*. Hal tersebut menandakan bahwa apabila bukti tersebut diperoleh dengan jalan yang tidak sah, maka konsekuensinya demi hukum adalah pemeriksaan perkara tersebut harus dibatalkan. Sehingga pentingnya melembagakan digital forensik sebagai proses dalam pengumpulan informasi elektronik atau dokumen elektronik dalam UU ITE sebagai acuan penegak hukum dalam mengumpulkan bukti elektronik.

Pentingnya dilakukan pembuktian digital forensik dapat dilihat dari Putusan Nomor 103/Pid.Sus/2020/PN.Blg[32] terkait ujaran kebencian di media sosial. Salah satu Hakim Anggota I yang menyebutkan bahwa pembuktian digital forensik dalam rangka membuktikan perbuatan Terpidana atas dakwaan dari Penuntut Umum sangatlah penting dilakukan guna membuktikan apakah benar Terpidana adalah pemilik akun Facebook atas nama Imran Baron dan Imran Haryono S tersebut,

[32] Kasus ini menjerat IMRAN HARYONO SIMAMORA Als PAK KEYLA dalam perkara pidana Nomor 103/Pid.Sus/2020/PN.Blg terkait dugaan penyebar ujaran kebencian terhadap SARA yang dilakukan oleh IMRAN HARYONO SIMAMORA Als PAK KEYLA (Terpidana/Terlapor) kepada RAPIDIN SIMBOLON (Korban/Pelapor) pada salah satu media sosial yaitu Facebook. Kasus ini bermula dari adanya postingan dari akun Facebook milik Terpidana atas nama IMRAN BARON. Akun Facebook tersebut memposting tulisan "Bupati Samosir Marga Simbolon Keturunan Anjing Babi" pada dinding grup "SAMOSIR-DANAU TOBA-INDONESIA" melalui Handphone merk Samsung warna Hitam dengan Nomor IMEI 1: 359891/06/092197/9 dan IMEI 2: 359892/06/092197/7 milik Terpidana. Kemudian melalui akun Facebook lain atas nama IMRAN HARYONO S, Terpidana memposting tulisan "Rapidin Simbolon Bupati Anjing Bupati yang Gagal dalam Semua Hal" ke dinding grup "MENUJU SAMOSIR MAJU" melalui Handphone merk Samsung warna Hitam dengan Nomor IMEI 1: 359891/06/092197/9 dan IMEI 2: 359892/06/092197/7 milik Terpidana. Bahwa tulisan yang unggah Terpidana pada grup media sosial Facebook "SAMOSIR-DANAU TOBA-INDONESIA" dan grup media sosial Facebook "MENUJU SAMOSIR MAJU" telah dilihat oleh beberapa orang. Yang mana dalam perkara ini Terpidana dikenakan Pasal 45A ayat (2) UndangUndang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Jo. Pasal 28 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

serta apakah benar Terpidana adalah orang yang menggunakan akun Facebook atas nama Imran Baron dan menuliskan kata-kata atau tulisan “Bupati Samosir Marga Simbolon keturunan Anjing Babi” pada dinding grup “SAMOSIR-DANAU TOBA-INDONESIA” dan tulisan atau kata-kata “Rapidin Simbolon Bupati Anjing Bupati yang Gagal dalam Semua Hal” pada dinding gup “MENUJU SAMOSIR MAJU” melalui akun Facebook Imran Haryono S, menggunakan Handphone milik Terpidana. Sehingga oleh karena digital forensik ini sama sekali tidak dilakukan dalam proses pembuktian, tentunya Terpidana belumlah dapat dinyatakan sebagai orang yang bersalah karena telah melakukan perbuatan tersebut.

Kedua, sebagai tindak pidana yang memiliki ciri, karakteristik, dan kerumitan khusus, jumlah kasus tindak pidana elektronik yang ditangani Kepolisian, tidak sebanding dengan jumlah (kuantitas)[33] dan kualitas penyidik yang menangani, mengingat keterbatasan jumlah penyidik yang menguasai bidang teknologi informasi. Hal ini tentu akan berakibat pada kualitas penyidikan dan pengumpulan alat bukti. Tindak pidana elektronik memiliki karakteristik atau ciri khusus, satu diantaranya yaitu pola kejahatan ini menggunakan teknologi informasi yang sulit dimengerti oleh orang-orang yang tidak menguasai seluk beluk dunia siber. Hal ini tentu mendatangkan kesulitan pada proses penyidikan ketika kejahatan ini ditangani oleh penyidik yang kurang menguasai, atau sama sekali tidak

[33] “Polri Akui Jumlah Penyidik Kejahatan Siber Tak Sebanding dengan Laporan”, Kompas.com (21/8/2023). https://nasional.kompas.com/read/2023/08/21/22550451/polri-akui-jumlah-penyidik-kejahatan-siber-tak-sebanding-dengan-laporan.

menguasai ilmu teknologi informasi, khususnya digital forensik. Apalagi ketika pelaku utama kejahatan tersebut sangat memahami seluk beluk teknologi informasi, memudahkan menghilangkan bukti yang mengarah pada dirinya hanya dengan menggunakan perangkat teknologi informasi dan mengutak-atik jaringannya. Situasi demikian tentu menjadi kendala besar dalam proses pengumpulan bukti tindak pidana pada tahap penyidikan.

Salah satu kasus TPE dengan tingkat kerumitan tinggi yang ditangani oleh penulis adalah kasus dengan Laporan Polisi Nomor: LP/137/IX/2023/POLRESTABES MAKASSAR, tertanggal 14 September 2023, dengan pelapor berinisial LAT. Kasus ini mengenai investasi fiktif di media sosial. Awalnya para korban menerima chat dari aplikasi *whatsapp,* yang menawarkan pekerjaan sampingan untuk mendapatkan penghasilan. Pekerjaan itu adalah cukup me'*like*' akun tertentu yang menampilkan video di aplikasi youtube, dengan menyertakan bukti *screenshot* yang diarahkan oleh pelaku kepada korban. Selanjutnya korban di iming-imingi akan mendapatkan komisi (fee) dari sekali "*like"* pada setiap video yang berbeda*.* Setelah berulang-ulang, pada *like* yang kesekian kalinya, korban diarahkan oleh pelaku untuk mentransfer sejumlah uang senilai ratusan juta sebagai deposito dengan iming-iming korban akan menerima jumlah yang berkali lipat dari nilai deposito. Para korban mempercayai pelaku dan mengirimkan sejumlah uang yang diminta tersebut. Hingga pada saat

korban menyadari telah ditipu ketika korban tidak menerima hasil balik dari deposito yang mereka setorkan.

Kasus ini melibatkan jaringan yang terstruktur dan lintas Negara. Pada awalnya penyidik sangat kesulitan mengusut dan membongkar dikarenakan tidak menggunakan digital forensic ISO 17025 tahun 2017 dalam mengolah dan menganalisis berbagai petunjuk (elektronik) yang didapatkan. Penyidik mulai bisa menganalisis, memetakan, dan mengusut jaringan penipuan tersebut dengan menangkap sejumlah tersangka, dengan bantuan digital forensik pada Laboratorium Forensik Polda Sulsel. Penggunaan digital forensik ini untuk memperkuat informasi elektronik dan dokumen elektronik dan hasil cetaknya sebagai alat bukti hukum yang sah dalam Pasal 5 dan Pasal 6 UU ITE.

Ketiga, peraturan internal di lingkup Kepolisian juga belum menopang efektivitas penanganan tindak pidana elektronik, padahal sesuai data penanganan tindak pidana elektronik diatas, jumlah penanganan terhadap kasus ini cukup besar dengan pola yang beragam dan tingkat kerumitan tertentu. Sebagai satu jenis kejahatan kontemporer yang memiliki karakteristik khusus, diperlukan penguatan penegakan hukum terhadap tindak pidana elektronik melalui peraturan di lingkup kepolisian yang mencakup kuantitas dan kualitas sumber daya penyidik, sarana prasarana, anggaran, dan aspek teknis lainnya yang dianggap perlu untuk mengoptimalkan kinerja kepolisian dalam penanganan kasus ini.

Keputusan Bersama Menteri Komunikasi dan Informatika Republik Indonesia, Jaksa Agung Republik Indonesia, dan Kepala Kepolisian Republik Indonesia, Nomor; 229 Tahun 2021, Nomor 154 Tahun 2021, dan Nomor KB/2/VI/2021, Tentang Pedoman Implementasi Atas Pasal Tertentu Dalam UU ITE, belum cukup kuat dalam mendukung penegakan hukum di bidang tindak pidana elektronik. Keputusan Bersama ini tidak dikenal dalam hierarki perundang-undangan, sehingga rawan dipersoalkan oleh pihak-pihak yang merasa dirugikan apabila hal ini dipakai sebagai acuan dalam proses pengumpulan bukti tindak pidana elektronik.

Oleh karena itu, sejauh mana urgensi digital forensik mendukung peraturan dalam lingkup kepolisian dalam penanganan tindak pidana elektronik, serta sejauh mana sumberdaya penyidik kepolisian yang menangani kasus tindak pidana elektronik memiliki kualitas pengetahuan mengenai tindak pidana elektronik dan digital forensik.

B. Rumusan Masalah

1. Apakah urgensi digital forensik pada proses penyidikan tindak pidana elektronik di Kepolisian?
2. Bagaimanakah proses pengumpulan bukti melalui digital forensik pada penyidikan tindak pidana elektronik di Kepolisian?
3. Bagaimanakah konsep ideal penguatan digital forensic dalam penanganan tindak pidana elektronik pada tahap penyidikan di Kepolisian?

C. Tujuan dan Kegunaan Penelitian

Tujuan penelitian:

1. Untuk menganalisis urgensi digital forensik pada proses penyidikan tindak pidana elektronik di Kepolisian.
2. Untuk menganalisis proses pengumpulan bukti melalui digital forensik pada penyidikan tindak pidana elektronik di Kepolisian.
3. Untuk merumuskan konsep ideal penguatan digital forensic dalam penanganan tindak pidana elektronik pada tahap penyidikan di Kepolisian.

Manfaat atau kegunaan penelitian: Manfaat yang diharapkan dapat dicapai melalui penelitian dengan tiga pokok permasalahan ini pada hakikatnya yaitu manfaat akademis yang bersifat teoritis dan manfaat yang bersifat praktis seperti berikut:

1. Manfaat Teoritis: Hasil penelitian ini diharapkan dapat memberikan sumbangan untuk pengembangan ilmu hukum khususnya mengenai hukum pidana, lebih khusus lagi tindak pidana yang menggunakan perangkat teknologi informasi .
2. Manfaat Praktis. Di lain pihak manfaat praktis dari penelitian ini dapat disumbangkan kepada beberapa individu ataupun lembaga yaitu:
    a. Untuk pihak pemerintah sebagai masukan (input) agar hasil penelitian nantinya dapat bermanfaat dalam pengembangan

ilmu hukum dan pembinaan hukum, khususnya dalam bidang hukum dan transaksi elektronik.

b. Untuk pihak penegak hukum; Kepolisian atau Kejaksaan agar dapat mengoptimalkan upaya penindakan terhadap kejahatan yang menggunakan media atau perangkat elektronik.

c. Bagi peneliti, adalah untuk memenuhi persyaratan memperoleh gelar Doktor Ilmu Hukum pada Program Pascasarjana Universitas Hasanuddin Makassar.

D. Orisinalitas Penelitian

Tujuan dari orisinalitas penelitian yaitu untuk menghindari kesamaan atau kemiripan dari penelitian terdahulu. Dari penelusuran pelbagai kepustakaan maupun melalui media elektronik (*website*) bahwa ada beberapa judul penelitian terdahulu yang dilakukan oleh peneliti sebelumnya baik judul penelitian disertasi, tesis maupun jurnal hukum terakreditasi dari pelbagai perguruan tinggi yang ada di Indonesia, yaitu:

1. Dian Eka Kusuma Wardani, "*Penegakan Hukum Oleh Kepolisian RI Terhadap Kejahatan Skimming di Indonesia*", disertasi Program Doktor Ilmu Hukum Universitas Hasanuddin, (2021).[34] Disertasi ini meneliti tentang *skimming* sebagai suatu bentuk kejahatan menurut hukum di Indonesia, serta mengkaji menganalisis sejauh mana kejahatan *skimming* dapat dibuktikan

[34]Penelitian dapat di lihat di: http://repository.unhas.ac.id/id/eprint/6192/2/P0400316409_disertasi%201-2.pdf.

menurut hukum di Indonesia. Perbedaan Disertasi Dian Eka Kusuma Wardani dengan penelitian ini adalah, penelitian Dian Eka membatasi isu penelitiannya hanya pada kejahatan *skimming* sebagai satu bentuk kejahatan elektronik, sedangkan penelitian ini tidak membatasi kasusnya dalam satu bentuk kejahatan elektronik, namun berfokus pada urgensi digital forensik pada tahap penyidikan tindak pidana elektronik melalui pengaturan norma digital forensik dalam UU ITE, penguatan peraturan kepolisian terkait penyidikan tindak pidana elektronik serta penguatan kapasitas sumberdaya manusia penyidik Polri dalam penanganan tindak pidana elektronik melalui pelatihan di bidang ITE dan digital forensik.

2. Sarwo Waskito, *Hakikat Pengaturan Alat Bukti Elektronik Dalam Hukum Acara Pidana*, Disertasi Program Doktor Ilmu Hukum Universitas 17 Agustus 1945 Surabaya, (2021).[35] Disertasi ini bertujuan untuk menganalisis dan menemukan hakikat alat bukti elektronik dalam hukum acara pidana, serta untuk menganalisis dan menemukan konsep pengaturan alat bukti elektronik hukum acara pidana. Perbedaan disertasi Sarwo Waskito dengan penelitian ini adalah; dalam penelitiannya, Sarwo Waskito menghendaki alat bukti elektronik diperjelas pengaturannya dalam KUHAP, dengan mengoreksi Pasal 184 KUHAP Ayat (1)

[35] Penelitian dapat di lihat di: http://repository.untag-sby.ac.id/11631/1/ABSTRAK.pdf.

untuk menambahkan bukti elektronik sebagai alat bukti. Sarwo Waskito melupakan satu hal bahwa Pasal 5 ayat (1) UU ITE menentukan bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Jadi sebetulnya tidak perlu lagi ada pengaturan tambahan pada Pasal 184 Ayat (1)KUHAP, karena Pasal 5 Ayat (1) UU ITE merupakan "perluasan alat bukti" dalam KUHAP, terhadap tindak pidana khusus atau tindak pidana tertentu, dalam hal ini tindak pidana elektronik. Sementara penelitian ini tidak bermaksud mengoreksi Pasal 184 Ayat (1) KUHAP, karena Pasal Pasal 5 Ayat (1) UU ITE sudah terang dan jelas menyebut informasi elektronik dan surat/dokumen elektronik sebagai alat bukti yang sah. Legal isu penelitian ini fokus mengkaji urgensi digital forensik pada tahap penyidikan tindak pidana elektronik melalui pengaturan norma digital forensik dalam UU ITE, penguatan peraturan kepolisian terkait penyidikan tindak pidana elektronik serta penguatan kapasitas sumberdaya manusia penyidik Polri dalam penanganan tindak pidana elektronik melalui pelatihan di bidang ITE dan digital forensik.

3. Hendri, *Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Teknologi Informasi Dan Transaksi Elektronik Terkait Kebebasan Berpendapat*. Disertasi Program Doktor Ilmu Hukum Universitas Airlangga Surabaya, 2021. Disertasi ini meneliti

tentang pengaturan terhadap tindak pidana teknologi informasi dan transaksi elektronik terkait kebebasan berpendapat dalam sistem hukum pidana di Indonesia dan di Filipina, serta menganalisis pertanggungjawaban pidana terhadap tindak pidana teknologi informasi dan transaksi elektronik terkait kebebasan berpendapat di Indonesia dan di Filipina.

Perbedaan disertasi Hendri dengan penelitian ini adalah, disertasi Hendri mengkaji tentang pertanggungjawaban pidana terhadap pelaku tindak pidana teknologi informasi dan transaksi elektronik terkait kebebasan berpendapat, sementara penelitian ini mengkaji tentang urgensi digital forensik pada tahap penyidikan tindak pidana elektronik melalui pengaturan norma digital forensik dalam UU ITE, penguatan peraturan kepolisian terkait penyidikan tindak pidana elektronik serta penguatan kapasitas sumberdaya manusia penyidik Polri dalam penanganan tindak pidana elektronik melalui pelatihan di bidang ITE dan digital forensik.

BAB II

TINJAUAN PUSTAKA

A. Teknologi Informasi

1. Perkembangan Teknologi Informasi

Perkembangan teknologi informasi yang diawali dengan perkembangan komputer dan telekomunikasi telah merubah cara hidup masyarakat di dunia dalam menjalankan aktivitasnya sehari-hari. Era globalisasi terjadi lebih cepat dari yang dibayangkan sebelumnya sebagai akibat dari perkembangan teknologi informasi ini di segala sektor kehidupan. Pengaruh perkembangan teknologi informasi ini berdampak tidak hanya pada sisi makro ekonomi dan politik masing masing Negara yang dipengaruhinya, tetapi juga berpengaruh pada aspek-aspek sosial budaya manusia.[36]

Teknologi komunikasi merupakan satu diantara produk ilmu pengetahuan serta teknologi. Teknologi komunikasi membuat perubahan besar terhadap pola interaksi antar manusia menjadikan komunikasi dengan komunitas lain dengan lebih mudah, dalam arti komunikasi dapat dilakukan dimana saja tanpa meninggalkan, bisa dilakukan dimana saja dan kapan saja. Interaksi sosial tidak lagi terkungkung dalam sekat teritorial suatu negara. Teknologi komunikasi telah membawa manusia kepada suatu peradaban baru

[36] Rachmad Santoso, Hisbulloh Ahlis Munawi, Duwi Sukmawati, *Perkembangan Teknologi Informasi Dan Telekomunikasi Terhadap Perubahan Perilaku Masyarakat*, prociding "Conference on Research & Community Services" Jombang, 2019, hal 586.

dengan struktur sosial beserta tata nilainya. Sistem tata nilai dalam suatu masyarakat berubah, dari yang bersifat lokal partikular menjadi global universal. Hal ini pada akhirnya membawa dampak pergeseran nilai, norma, moral dan kesusilaan.[37]

Teknologi informasi berasal dari 2 (dua) unsur, yaitu teknologi dan informasi. Secara etimologis, kata teknologi berasal dari kata (*technology*) berasal dari bahasa yunani techne yang berarti seni, kerajinan, atau keterampilan, dan logia yang berarti kata, studi, atau tubuh ilmu pengetahuan. secara terminologis, teknologi merupakan pengetahuan untuk membuat sesuatu.[38] Menurut Iskandar Alisyahbana, teknologi adalah cara yang dilakukan manusia untuk memenuhi kebutuhannya dengan bantuan alat dan akal, untuk menghemat tenaga.[39] Secara umum, teknologi dapat dimaknai sebagai hasil karya manusia untuk membantu memecahkan permasalahan yang dihadapi atau mempermudah kegiatan manusia dan diharapkan dapat meningkatkan kinerja manusia.

Sedangkan informasi adalah data yang sudah diolah menjadi bentuk yang berarti bagi pengguna, yang dimanfaatkan pada saat pengambilan keputusan saat ini atau mendukung sumber informasi.[40]

---

[37] Abdul Wahid dan Mohamad Labib. *Kejahatan Mayantara (Cyber Crime), loc.cit*.

[38] Muhammad Yaumi, *Media Dan Teknologi Pembelajaran*, Cetakan Pertama, Prenadamedia Group, Jakarta, 2018, hal 24.

[39] Erlisa Dwi Ananda, "Pemanfaatan Teknologi Informasi", 5. https://journal.unair.ac.id, Diakses pada 16 Mei 2023 pukul 22.05 wita..

[40] Kusrini & Andri Koniyo, *Tuntunan Praktis Membangun Sistem Informasi Akuntansi Dengan Visual Basic Dan Microsoft Sql Server*, Cv Andi Offset, Yogyakarta, 2007, hal 7.

Menurut kamus besar bahasa Indonesia, informasi adalah pemberitahuan, kabar, atau berita tentang sesuatu.[41] Dengan kata lain informasi memberikan atau menyampaikan pesan terhadap seseorang atau khalayak umum tentang sesuatu. Selain itu, Informasi juga dianggap sebagai ilmu pengetahuan, karena dengan adanya informasi seseorang dapat mengetahui sesuatu yang baru, membuat lebih berwawasan luas.

Dalam suatu era globalisasi, setiap aspek akan selalu berkembang tanpa batasan apa pun, entah batasan waktu, jarak, tempat, ataupun batasan-batasan lainnya. Perkembangan aspek seperti ini dapat terwujud dikarenakan adanya penerapan dari teknologi informasi.[42] Kemajuan-kemajuan dalam bidang teknologi komputer dan telekomunikasi mendorong pula perkembangan teknologi yang sekarang dikenal dengan nama internet. Dengan internet, penyebaran informasi menjadi lebih cepat dan mudah dari era sebelumnya, dengan demikian teknologi ini menjadi ladang emas bagi pebisnis dunia modern dimana internet menjadi salah satu media penting untuk menunjang sebuah aktivitas bisnis.[43]

Teknologi Informasi (TI), atau dalam bahasa Inggris dikenal dengan istilah "*Information technology* (IT)" adalah istilah umum untuk teknologi apa pun yang membantu manusia dalam membuat,

[41] Herry Irawan & Puspita Kencana Sari, *Bisnis Informasi*, Cetakan Pertama, Uwais Inspirasi Indonesia, Ponorogo, 2018, hal 3.

[42] Juhriyansyah Dalle, A.A Karim, Baharuddin, *Pengantar Teknologi Informasi*, Rajawali Press, Jakarta, 2020. hal 6.

[43] *Ibid* hal 166.

mengubah, menyimpan, mengomunikasikan dan/atau menyebarkan informasi. TI menyatukan komputasi dan komunikasi berkecepatan tinggi untuk data, suara, dan video. Contoh dari Teknologi Informasi bukan hanya berupa komputer pribadi, tetapi juga telepon, TV, peralatan rumah tangga elektronik, dan peranti genggam modern (misalnya ponsel).[44] Teknologi informasi baik secara implisit maupun eksplisit tidak sekedar berupa teknologi komputer, tetapi juga mencakup teknologi komunikasi. Dengan kata lain, yang disebut teknologi informasi adalah gabungan antara teknologi komputer dan teknologi komunikasi.

Perkembangan Teknologi Informasi memacu suatu cara baru dalam kehidupan, dari kehidupan dimulai sampai dengan berakhir, kehidupan seperti ini dikenal dengan "*e-life*", artinya kehidupan ini sudah dipengaruhi oleh berbagai kebutuhan secara elektronik. Dan sekarang ini sedang semarak dengan berbagai huruf yang dimulai dengan awalan "e" seperti *e-commerce*, *e- government*, *e-education*, *e-library*, *e-journal*, *e-medicine*, *e-laboratory*, *e-biodiversity*, dan yang lainnya lagi yang berbasis elektronika.[45] Orang menjadi terbiasa menggunakan surat elektronik (*e-mail*) dalam berkomunikasi yang sebelumnya menggunakan surat kertas konvensional (surat Pos). Orang lebih suka menggunakan program-program pengolah kata untuk membuat dokumen daripada memakai mesin ketik biasa. Dan

[44] Utama Andri, *Mata Diklat: Pengenalan Teknologi Informasi, loc.cit*.
[45] *Ibid* hal 1.

banyak lagi hal yang terjadi seiring dengan perkembangan teknologi informasi.[46]

Williams dan Sawyer berpendapat bahwa, teknologi informasi adalah suatu teknologi yang merupakan hasil gabungan dari jalur komunikasi berkecepatan tinggi dengan komputasi (komputer), yang mana jalur komunikasi tersebut membawa video, suara, dan data. Kemudian menurut pendapat dari Martin.[47] Menurut Martin, suatu teknologi informasi tidak hanya memiliki keterbatasan pada teknologi komputer (perangkat lunak dan perangkat keras) yang digunakan sebagai alat untuk menyimpan dan memproses informasi, melainkan juga mencangkup suatu teknologi komunikasi.[48]

Dari sejumlah pengertian di atas, bisa disimpulkan bahwa pengertian teknologi informasi adalah suatu alat hasil ciptaan manusia yang membantu manusia dalam mencari informasi, mengelola informasi ataupun menyampaikan informasi kepada seseorang atau khalayak umum yang bermanfaat sebagai ilmu pengetahuan ataupun untuk mengambil suatu keputusan. Teknologi informasi berhubungan dengan pengambilan, pengumpulan, pengolahan, penyimpanan, penyebaran, dan penyajian informasi.

---

[46] *Ibid* hal 7.

[47] Williams, & Sawyer. *Using Information Technology,* (terjemahan Indonesia). Penerbit ANDI: Yogyakarta, 2007, dikutip dari Juhriyansyah Dalle, A.A Karim, Baharuddin, *ibid,* hal 1.

[48] Martin, E. *Managing Information Technology What Managers Need To Know*, (3rd ed.). Pearson Education International: New Jersey, 1999, *ibid*.

Teknologi Informasi dan Komunikasi (selanjutnya disebut TIK) mencakup dua aspek, yaitu Teknologi Informasi dan Teknologi Komunikasi.[49] Teknologi Informasi adalah meliputi segala hal yang berkaitan dengan proses, penggunaan sebagai alat bantu, manipulasi, dan pengelolaan informasi.[50] Teknologi Komunikasi adalah segala hal yang berkaitan dengan penggunaan alat bantu untuk memproses dan mentransfer data dari perangkat yang satu ke lainnya. Teknologi Informasi dan Komunikasi suatu padanan yang tidak terpisahkan yang mengandung pengertian luas tentang segala kegiatan yang terkait dengan memproses, manipulasi, pengelolaan, dan transfer/pemindahan informasi antar media.

Menurut Susanto, TIK adalah sebuah media atau alat bantu yang digunakan untuk transfer data baik itu untuk memperoleh suatu data/informasi maupun memberikan informasi kepada orang lain serta dapat digunakan untuk alat berkomunikasi baik satu arah maupun dua arah. Sedangkan menurut Anatta Sannai, TIK adalah sebuah media atau alat bantu dalam memperoleh pengetahuan antara seseorang kepada orang lain.[51] Dapat disimpulkan bahwa TIK adalah sebuah media atau alat bantu untuk menyampaikan, memproses dan mentransfer data dari perangkat yang satu ke lainnya dengan menggunakan perangkat teknologi.

---

[49] Arief Sadiman, *Media Pendidikan*, Raja Grafindo Persada, Jakarta, 2008.
[50] Azhar Arsyad, *Media Pembelajaran*, Raja Grafindo Persada, Jakarta, 2006.
[51] *Ibid*.

2. Kejahatan Elektronik (*Cybercrime*)

a. Definisi *Cybercrime*

Dalam beberapa kepustakaan, *cybercrime* sering diidentikkan sebagai *computer crime*. The U.S. Department of Justice menyebut *computer crime* sebagai: "*Any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution"*. Pendapat lain dikemukakan oleh Organization for Economic Cooperation Development (OECD) yang menggunakan istilah computer related crime yang berarti: "*Any illegal, unethical or unauthorized behavior involving automatic data processing and/or transmission data*".[52]

Berdasarkan instrumen Perserikatan Bangsa Bangsa (PBB) dalam *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders* yang diselenggarakan di Vienna, 10-17 April 2000, kategori *cybercrime* dapat dilihat secara sempit maupun secara luas, yaitu: 1) *Cyber crime in a narrow sense ("computer crime"): any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them*; 2) *Cyber crime in a broader sense ("computer-related crime"): any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or*

[52] Maskun, *loc.cit*., hal 47.

distributing information by means of a computer system or network.

Convention on Cybercrime (Budapest, 23.XI.2001)[53] tidak memberikan definisi *cybercrimes*, tetapi memberikan ketentuan-ketentuan yang dapat diklasifikasikan menjadi: Title 1; *Offences against the confidentiality, integrity and availability of computer data and systems*; Title 2; *Computer-related offences*; Title 3; *Content-related offences*; Title 4: *Offences related to infringements of copyright and related rights*; Title 5: *Ancillary liability and sanctions Corporate Liability*. Sementara dalam Black's Law Dictionary 9th Edition, definisi computer crime adalah sebagai: *A crime involving the use of a computer, such as sabotaging or stealing electronically stored data. - Also termed cybercrime*.[54]

Terdapat beberapa istilah Kejahatan di bidang Teknologi Informasi, yaitu; *cybercrime* (kejahatan mayantara),[55] *computer crime*, *computer abuse*, *computer fraud*, *computer related crime*, dan lain-lain. *Cybercrime* atau kejahatan mayantara, yaitu perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan

[53] Convention on Cybercrime Budapest, 23.XI.2001 https://rm.coe.int/1680081561.
[54] Black's Law Dictionary 9th Edition.
[55] Barda Nawawi A, *Tindak Pidana Mayantara: Perkembangan Kajian Cybercrime di Indonesia*, cet ke-2, Raja Grafindo Persada, Jakarta, 2007.

telekomunikasi.[56] *Cybercrime* merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapatkan perhatian luas di dunia internasional.

Volodymyr Golubev menyebutnya sebagai "*the new form of anti-social behavior*". Beberapa julukan/sebutan lainnya diberikan kepada jenis kejahatan baru ini di dalam berbagai tulisan, antara lain, sebagai kejahatan dunia maya (*cyberspace*/*virtual space offence*), dimensi baru dari *high tech crime*, dimensi baru dan transnasional crime, dan dimensi baru dari *white collar crime*.[57] *Computer crime* adalah perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana / alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.[58]

Cybercrime merupakan bentuk-bentuk kejahatan yang ditimbulkan karena pemanfaatan teknologi internet. Dapat juga didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi. Dalam "*Background paper*" Kongres PBB X untuk *Workshop On Crimes Related To The Computer Network*, dokumen A/CONF.187/10,3-2200,

[56] Teguh Wahyono, *Kejahatan Teknologi Informasi Cyber Crime*, Sinar Grafika, Jakarta, 2006.

[57] M. Syukri Akub, (2018). *Pengaturan Tindak Pidana Mayantara (Cyber Crime) Dalam Sistem Hukum Indonesia*, Jurnal Al-Ishlah, Jurnal Ilmiah Hukum, Vol 21. No 2, hal 1. Mengutip Barda Nawawi A, *Tindak Pidana Mayantara: Perkembangan Kajian Cybercrime di Indonesia*, *op.cit*.

[58] Teguh Wahyono, *op.cit*.

halaman 5 dijelaskan bahwa cybercrime dibagi dua kategori yaitu:[59]

1. *Cybercrime* dalam arti sempit disebut *computer crime*, yaitu perilaku ilegal/melanggar yang secara langsung menyerang sistem keamanan komputer dan data yang diproses oleh komputer.
2. *Cybercrime* dalam arti luas disebut *computer related crime* , yaitu perilaku ilegal/melanggar yang berkaitan dengan sistem komputer atau jaringan.

Didik M.Arief Mansur dan Elisatris Gultom dalam bukunya "Cyber Law-Aspek Hukum Teknologi Informasi" menyatakan bahwa secara umum yang dimaksud kejahatan komputer atau kejahatan di dunia *cyber* (*cybercrime*) adalah upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut.[60] Dari beberapa pengertian di atas, *cybercrime* dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/alat komputer sebagai objek,

[59] M. Syukri Akub, *op.cit*.

[60] Didik M.Arief Mansur dan Elisatris Gultom, *Cyber Law-Aspek Hukum Teknologi Informasi*, Bandung: PT Refika Aditama, 2009, hlm.8

baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.

b. Klasifikasi *Cybercrime*

Cybercrime dapat diklasifikasikan menjadi tiga, yaitu:

1. *Cyberpiracy,* yaitu penggunaan teknologi komputer untuk mencetak ulang *software* atau informasi, lalu mendistribusikan informasi atau software tersebut lewat teknologi komputer misalnya pembajakan software.
2. *Cybertrespass,* yaitu penggunaan teknologi komputer untuk meningkatkan akses pada sistem komputer suatu organisasi atau individu misalnya *hacking exploit system* dan seluruh kegiatan yang berhubungan dengannya.
3. *Cybervandalism* yaitu penggunaan teknologi komputer untuk membuat program yang mengganggu proses transmisi elektronik, dan menghancurkan data di sistem komputer misalnya virus, trojan, worm, metode DoS, *http attack*, *BruteForce Attack,* dan lain sebagainya.[61]

c. Jenis-Jenis *Cybercrime*

Cybercrime merupakan tindak pidana yang timbul akibat penyalahgunaan teknologi informasi yang ditandai dengan

[61] Mas Wigrantoro Roes Setiyadi dan Mirna Dian Avanti Siregar, *Naskah Akademik Rancangan Undang-Undang Tindak Pidana di Bidang Teknologi Informasi*, November, 2003, h.25 dalam http://www.gipi.or.id/download/Naskah%20Akademik. Data akses 20 Agustus 2023 pukul 22.15 wita.

lahirnya internet yang membentuk ruang *cyber*. Dalam "*Draft Convention on Cybercrime*" (Draf No. 19 dan No.25 Rev.5) th.2000 dan "*Draft Explanatory Memorandum to the Draft Convention on Cybercrime th 2001*", yang dipersiapkan oleh *European Committee on Crime Problems*, ada berbagai kategori dari *cybercrime* yaitu sebagai berikut:[62]

1. *Joy Computing*, yaitu pemakaian komputer orang lain tanpa izin. Hal ini termasuk pencurian waktu operasi komputer.
2. *Hacking*, yaitu mengakses secara tidak sah atau tanpa izin dengan alat suatu terminal.
3. *The Trojan Horse*, yaitu manipulasi data atau program dengan jalan mengubah data atau instruksi pada sebuah program, menghapus, menambah, menjadikan tidak terjangkau dengan tujuan untuk kepentingan pribadi atau orang lain.
4. *Data Leakage*, yaitu menyangkut bocornya data ke luar terutama mengenai data yang harus dirahasiakan. Pembocoran data komputer itu bisa berupa rahasia negara, perusahaan, data yang dipercayakan kepada seseorang dan data dalam situasi tertentu.

[62] Agus Raharjo. *Cybercrime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, PT.Citra Aditya Bakti, Bandung, 2002, hal 203-205.

5. Data *Diddling*, yaitu suatu perbuatan yang mengubah data valid atau sah dengan cara tidak sah, mengubah input data, atau output data.
6. *To Frustate data communication* atau penyia-nyiaan komputer.
7. *Software Piracy*, yaitu pembajakan perangkat lunak terhadap hak cipta yang dilindungi HAKI.
8. *Cyber Espionage*, merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized*. Biasanya si penyerang menyusupkan sebuah program mata-mata yang dapat kita sebut sebagai *spyware*.
9. *Infringements of Privacy*, kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain maka

dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

10. *Data Forgery*, merupakan kejahatan dengan memalsukan data pada dokumen - dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi “salah ketik” yang pada akhirnya akan menguntungkan pelaku.
11. *Unauthorized Access to Computer System and Service*, kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi.
12. *Cyber Sabotage and Extortion*, merupakan kejahatan yang paling mengenaskan.Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem

jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai *cyber-terrorism*.

13. *Offense against Intellectual Property*, kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada *web page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.
14. *Illegal Contents*, merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat

dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya adalah pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah, dan sebagainya. Dari bentuk *cybercrime* tersebut di atas, nampak bahwa pada dasarnya *cybercrime* adalah penyerangan pada *content*, computer system dan *communication system* milik orang lain atau umum di dalam *cyberspace*.

Selain itu terdapat juga jenis lainnya berdasarkan jenis aktivitasnya, kegiatan ini yang marak di lakukan baik di Indonesia sendiri atau di negara lain,yaitu:

1) Data *Theft* adalah kejahatan memperoleh data komputer secara tidak sah baik untuk digunakan sendiri ataupun untuk diberikan kepada orang lain.
2) *Cracking* adalah kejahatan yang paling mengenaskan. Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

3. Kejahatan Elektronik Sebagai Tindak Pidana

Penetapan suatu perbuatan sebagai tindak pidana di bidang Teknologi Informasi dan Komunikasi (TIK) merupakan masalah kebijakan kriminalisasi dengan menggunakan sarana penal (kebijakan penal). Kewenangan tersebut berada pada pembentuk undang-undang, dalam hal ini Pemerintah (Presiden) dan DPR. *Crimes is any act that lawmakers designate as "court-punishable behaviour*".[63]

Karakteristik dari suatu tindak pidana adalah; pertama, bertentangan dengan atau merugikan kepentingan umum (*a public wrong*). Mengenai hal ini Sir Carleton Allen menyatakan: *crime is crime because it consists in wrongdoing which directly and in serious degree threatens the security or well-being of society, and because it is not safe to leave it redressable only by compensation of the party injured*.[64] Kedua, Bertentangan dengan moral masyarakat (*a moral wrong*).

Dalam hukum pidana terdapat tiga permasalahan yang senantiasa menjadi pembicaraan, yaitu: Perbuatan yang dilarang; Pelaku perbuatan yang dilarang; dan Ancaman pidananya. Perbuatan yang dilarang adalah perbuatan yang bertentangan dengan hukum, suatu perbuatan melawan hukum atau tidak

[63] James Levin, et.al., *Criminal Justice A Public Policy Approach*, Harcourt Brace Jovanovich, New York, 1980, hlm. 63-64.

[64] J.C. Smith dan Brian Hogan, *Criminal Law*, English Language Book Society/Butterworths, London, 1988, hlm. 18.

memenuhi perintah hukum. Perbuatan ini ada yang bersifat nyata-nyata berlawanan dengan ketentuan undang-undang dan ada pula yang menentang rasa keadilan masyarakat tetapi tidak melanggar ketentuan hukum formal. Perbuatan yang nyata-nyata berlawanan dengan ketentuan undang-undang disebut perbuatan melawan hukum yang formal (*formeele wederechtelijkeheidsbegrip*), sedangkan perbuatan yang menentang rasa keadilan masyarakat tetapi tidak melanggar ketentuan hukum formal disebut perbuatan melawan hukum yang materil (materiele wederechtelijkheidbegrip). Perbuatan yang mengandung sifat melawan hukum formal yang dapat diproses secara pidana menurut ketentuan pidana yang ada. Suatu perbuatan yang merugikan masyarakat yang belum dirumuskan dalam hukum pidana positif sebagai perbuatan pidana, secara yuridis belum dianggap sepenuhnya sebagai kejahatan.[65]

Dasar pemikiran yang berkaitan dengan hal tersebut adalah mengenai urgensi pengunaan hukum pidana dalam menanggulangi *cybercrime* dan kriminalisasi suatu perbuatan menjadi tindak pidana. Dalam penggunaan hukum pidana tersebut Nigel Walker mensyaratkan 6 (enam) prinsip yang harus diperhatikan oleh

[65] Bdgk, J.C. Smith dan Brian Hogan, *Criminal Law*, English Language Book Society/Butterworths, London, 1988, hlm. 18 yang memuat penyataan Sir Carleton Allen sebagai berikut: *crime is crime because it consists in wrongdoing which directly and in serious degree threatens the security or well-being of society, and because it is not safe to leave it redressable only by compensation of the party injure*.

pembentuk undang-undang, yaitu:[66] Pertama, hukum pidana tidak digunakan semata-mata untuk tujuan pembalasan. Kedua, tindak pidana yang dilakukan harus menimbulkan kerugian dan korban yang jelas. Ketiga, hukum pidana tidak digunakan apabila masih ada cara lain yang lebih baik dan lebih damai. Keempat, kerugian yang ditimbulkan karena pemidanaan harus lebih kecil daripada akibat tindak pidana. Kelima, harus mendapat dukungan masyarakat, dan keenam harus dapat diterapkan dengan efektif.

Pandangan lain berkaitan dengan penggunaan hukum pidana dan proses kriminalisasi suatu perbuatan menjadi tindak pidana dikemukakan oleh Sudarto, sebagai berikut :[67] Hukum pidana harus digunakan untuk mewujudkan masyarakat adil dan makmur merata material dan spirituial. Hukum pidana bertugas untuk menanggulangi kejahatan dan juga pengugeran terhadap tindakan penanggulangan itu sendiri untuk kesejahteraan masyarakat atau untuk pengayoman masyarakat. Hukum pidana digunakan untuk mencegah atau menanggulangi perbuatan yang tidak dikehendaki, yaitu perbuatan yang mendatangkan kerugian pada masyarakat.

Penggunaan sarana hukum pidana dengan sanksi yang negatif perlu disertai perhitungan biaya yang harus dikeluarkan dan hasil yang diharapkan akan dicapai (*cost and benefit principles*). Dalam pembuatan peraturan hukum pidana perlu diperhatikan kemampuan

[66] Muladi, *Proyeksi Hukum Pidana Materiil Indonesia di Masa Datang*, Pidato Pengukuhan Guru Besar Universitas Diponegoro, Semarang, 1990, hlm. 7 dan 28.
[67] Sudarto, *Hukum dan Hukum Pidana*, Alumni, Bandung, 1986, hlm. 36-40.

daya kerja dari badan-badan tersebut, jangan sampai ada kelampauan beban tugas (*overbelasting*). Prinsip-prinsip tersebut menjadi dasar pertimbangan dalam perumusan ketentuan pidana dari suatu undang-undang agar pembentukan hukum pidana tersebut dapat sejalan dengan fungsinya, yaitu untuk mengatur tata kehidupan masyarakat dan melindungi kepentingan-kepentingan hukum dari perbuatan-perbuatan yang hendak 'memperkosanya'.

Suatu perbuatan dijadikan perbuatan pidana karena berbagai alasan. Pertama, bahwa perbuatan tersebut merugikan masyarakat. Kedua, sudah berulang-ulang dilakukan. Ketiga, terdapat reaksi sosial atas perbuatan tersebut. Keempat, adanya unsur bukti. Berdasarkan keempat parameter ini, maka tidak serta merta setiap perbuatan yang merugikan dapat dirumuskan secara formal sebagai perbuatan pidana. Oleh karena itu, di dalam dunia cyber perlu dipilah-pilah dengan seksama, mana saja perbuatan-perbuatan yang layak dikategorikan sebagai *cybercrime*.

Pada hakikatnya *cybercrime* tetaplah merupakan kejahatan yang dilakukan dengan komunikasi baik secara tertulis (libel) maupun secara lisan (*slander*). Tetapi memang ada perbedaan kualitatif yang cukup besar antara *cybercrime* dengan delik komunikasi biasa, yaitu saluran yang digunakan. Jaringan internet atau jaringan komputer terlalu canggih jika dibandingkan dengan media cetak dan media elektronik biasa. Kecanggihan *cyber communication* membuat

kejahatan yang diciptakannya (*cybercrime*) juga amat canggih. Artinya jauh lebih sulit pengusutannya daripada pengusutan delik media cetak dan delik media elektronik biasa. Siapa yang akan diusut, dijadikan terdakwa atau dihukum jika terjadi *cybercrime*, bagaimana menemukan pelakunya. Hampir sama sulitnya mengusut kejahatan yang menggunakan selebaran gelap. Apalagi yang dikirim dari Negara lain. Juga *cybercrime* bisa melalui beberapa Negara (jaringan internet global) yang tidak sama sistem hukumnya.

Perbedaan *cybercrime* dengan kebanyakan kejahatan terrestrial dapat disebabkan antara lain adalah: pertama, mudah dipelajari cara melakukannya. Kedua, memerlukan sedikit sumber daya relatif terhadap kerugian potensial disebabkannya. Ketiga, dapat dilakukan dalam suatu yurisdiksi tanpa hadir secara fisik didalamnya. Sering tidak secara jelas antara illegal dan tidak illegal.[68]

B. Konvensi Internasional Tentang *Cybercrime*

Dua instrument internasional tentang *cybercrime* adalah Konvensi PBB Tentang *Cybercrime* (*United Nations Convensiton Against Cybercrime*) yang diprakarsai dalam Kongres PBB ke-10 di Wina Austria pada 10-17 April 2000 yang kemudian diadopsi oleh Majelis Umum PBB pada 7 Agustus 2024 lalu, [69] dan *EU Convention on Cybercrime*, 2001" yang telah dibuat pada tanggal 23 November 2001 di kota Budapest,

[68] BPHN, *Op.cit*., hlm 17-18.

[69] https://www.unodc.org/unodc/en/cybercrime/convention/home.html. Data akses 22 Mei 2025 pukul 21.32 WIT.

Hongaria, oleh negara-negara yang tergabung dalam Uni Eropa (Council of Europe).[70] Pada UN CC, Istilah *cybercrime* dibagi dalam dua kategori. Pertama, *cybercrime* dalam arti sempit (*in a narrow sense*) disebut *computer crime*. Kedua, *cybercrime* dalam arti luas (*in a broader sense*) disebut *computer related crime*. Lengkapnya sebagai berikut:

1. *Cybercrime in a narrow sense (computer crime): any legal behavior directed by means of electronic operations that targets the security of computer system and the data processed by them.*
2. *Cybercrime in a broader sense (computer related crime): any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possession, offering or distributing information by means of a computer system or network.*

Konvensi ini dirancang untuk memberikan standar internasional dalam pencegahan, penyidikan, dan penuntutan kejahatan siber dengan mengklasifikasikan berbagai bentuk kejahatan, seperti akses ilegal ke sistem komputer, gangguan data, penyalahgunaan perangkat, dan kejahatan berbasis konten. Standarisasi definisi ini penting agar negara-negara memiliki pemahaman yang sama dalam penanganannya. Selain itu, konvensi mendorong negara anggota untuk menyelaraskan undang-undang domestik mereka dengan standar internasional. Harmonisasi ini memungkinkan adanya pendekatan hukum yang seragam dan memperlancar kerjasama lintas negara. Konvensi juga menyediakan pedoman untuk teknik penyidikan digital, termasuk pengumpulan dan

[70] "Kajian EU Convention On Cybercrime Dikaitkan Dengan Upaya Regulasi Tindak Pidana Teknologi Informasi", BPHN, *Loc.cit*.

pelestarian bukti elektronik, yang penting karena kejahatan siber tidak jarang untuk melibatkan data yang mudah dimanipulasi atau dihapus.[71]

Konvensi memuat berbagai pasal penting terkait kejahatan siber yang mendapat perhatian dunia. Pada Pasal 10 Konvensi memungkinkan negara meminta bukti elektronik dari negara lain untuk kejahatan dengan ancaman hukuman minimal empat tahun.[72] Pasal 11 mengatur larangan penyalahgunaan perangkat yang dirancang untuk kejahatan siber dengan pengecualian untuk penggunaan sah.[73] Pasal 12 mengatur pemalsuan data elektronik untuk tujuan penipuan.[74] Pasal 13 mengatur tentang

---

[71] Andi Rania Risya Zamayya dkk, (2025), *Kajian Teoritis Implikasi The United Nations Convention Against Cybercrime Terhadap Pengaturan Tindak Pidana Siber Indonesia*, Jurnal Ikraith-Humaniora, Vol 9 No 2.

[72] Article 10. *Interference with an information and communications technology system [agreed ad referendum] Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the serious hindering of the functioning of an information and communications technology system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing electronic data.*

[73] Article 11. Misuse of devices [agreed ad referendum]: *1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: (a) The obtaining, production, sale, procurement for use, import, distribution or otherwise making available of: (i) A device, including a program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with articles 7 to 10 of this Convention; or (ii) A password, access credentials, electronic signature or similar data by which the whole or any part of an information and communications technology system is capable of being accessed; with the intent that the device, including a program, or the password, access credentials, electronic signature or similar data be used for the purpose of committing any of the offences established in accordance with articles 7 to 10 of this Convention; and (b) The possession of an item referred to in paragraph 1 (a) (i) or (ii) of this article, with intent that it be used for the purpose of committing any of the offences established in accordance with articles 7 to 10 of this Convention. 2. This article shall not be interpreted as imposing criminal liability where the obtaining, production, sale, procurement for use, import, distribution or otherwise making available, or the possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with articles 7 to 10 of this Convention, such as for the authorized testing or protection of an information and communications technology system. 3. Each State Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (ii) of this article.*

[74] *Each State 1. Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed*

pencurian atau penipuan melalui sistem teknologi informasi.[75] Kemudian Pasal 14 Konvensi mengatur pelecehan seksual anak secara daring.[76]

Dalam UE Convention, substansi konvensi mencakup area yang cukup luas, bahkan mengandung kebijakan kriminal (*criminal policy*) yang

---

intentionally and without right, the input, alteration, deletion or suppression of electronic data resulting in inauthentic data with the intent that they be considered or acted upon for legal purposes as if they were authentic, regardless of whether or not the data are directly readable and intelligible. [agreed ad referendum]. 2. A State Party may require an intent to defraud, or a similar dishonest or criminal intent, before criminal liability attaches.

[75] *Article 13. Information and communications technology system-related theft or fraud Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by means of: [agreed ad referendum] (a) Any input, alteration, deletion or suppression of electronic data; [agreed in informals] (b) Any interference with the functioning of an information and communications technology system; [agreed ad referendum] (c) Any deception as to factual circumstances made through an information and communications technology system that causes a person to do or omit to do anything which that person would not otherwise do or omit to do; [agreed ad referendum] with the fraudulent or dishonest intent of procuring for oneself or for another person, without right, a gain in money or other property.*

[76] *Article 14. Offences related to online child sexual abuse or child sexual exploitation material 1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: (a) Producing, offering, selling, distributing, transmitting, broadcasting, displaying, publishing or otherwise making available child sexual abuse or child sexual exploitation material through an information and communications technology system; (b) Soliciting, procuring or accessing child sexual abuse or child sexual exploitation material through an information and communications technology system; (c) Possessing or controlling child sexual abuse or child sexual exploitation material stored in an information and communications technology system or another storage medium; (d) Financing the offences established in accordance with subparagraphs (a) to (c) of this paragraph, which States Parties may establish as a separate offence. 2. For the purposes of this article, the term "child sexual abuse or child sexual exploitation material" shall include visual material, and may include written or audio content, that depicts, describes or represents any person under 18 years of age: (a) Engaging in real or simulated sexual activity; (b) In the presence of a person engaging in any sexual activity; (c) Whose sexual parts are displayed for primarily sexual purposes; or (d) Subjected to torture or cruel, inhumane or degrading treatment or punishment and such material is sexual in nature. 3. A State Party may require that the material identified in paragraph 2 of this article be limited to material that: (a) Depicts, describes or represents an existing person; or (b) Visually depicts child sexual abuse or child sexual exploitation. 4. In accordance with their domestic law and consistent with applicable international obligations, States Parties may take steps to exclude the criminalization of: (a) Conduct by children for self-generated material depicting them; or (b) The consensual production, transmission, or possession of material described in paragraph 2 (a) to (c) of this article, where the underlying conduct depicted is legal as determined by domestic law, and where such material is maintained exclusively for the private and consensual use of the persons involved. 5. Nothing in this Convention shall affect any international obligations which are more conducive to the realization of the rights of the child.*

bertujuan untuk melindungi masyarakat dari *cybercrime*, baik melalui undang-undang maupun kerjasama internasional. Hal ini dilakukan dengan penuh kesadaran sehubungan dengan semakin meningkatnya intensitas digitalisasi, konvergensi, dan globalisasi yang berkelanjutan dari teknologi informasi, yang menurut pengalaman dapat juga digunakan untuk melakukan tindak pidana.[77]

Konvensi ini tidak memberikan definisi *cybercrime*, tetapi memberikan ketentuan-ketentuan yang dapat diklasifikasikan menjadi *cybercrime* yaitu: pertama, *offences against the confidentiality, integrity and availability of computer data and systems Illegal access* (tindak pidana terhadap kerahasiaan, keutuhan dan ketersediaan data dan sistem komputer akses secara ilegal), mencakup; a. *Illegal interception* (penyadapan ilegal); b. *Data interference* (gangguan data); c. *System interference* (gangguan sistem); dan d. *Misuse of devices* (penyalahgunaan perangkat). Kedua, *computer-related offences* (tindak pidana terkait komputer), mencakup; a. *Computer-related forgery* (pemalsuan terkait komputer), dan b. *Computer-related fraud* (penipuan terkait komputer). Ketiga, *content-related offences* (tindak pidana terkait konten), mencakup *offences related to child pornography* (Tindak pidana terkait pornografi anak). Keempat, *offences related to infringements of copyright and related rights* (tindak pidana terkait pelanggaran hak cipta dan hak terkait). Kelima, *ancillary liability and sanctions* (tanggung jawab

[77] BPHN, *Op.cit*.

dan sanksi tambahan), mencakup; a. *Attempt and aiding or abetting* (percobaan dan pembantuan atau pemufakatan jahat), dan b. *Corporate liability* (tanggung jawab korporasi). [78]

C. Ilmu Forensik dan Digital Forensik

1. Ilmu Forensik

Kata forensik berasal dari bahasa Latin yakni dari kata “forensic” yang berarti ”dari luar”, serumpun dengan kata “forum” yang berarti “tempat umum”. Arti forum itu sendiri adalah suatu tata cara perdebatan di depan umum.[79] Forensik adalah ilmu pengetahuan yang menggunakan ilmu multidisiplin untuk menerapkan ilmu pengetahuan alam, kimia, kedokteran, biologi, psikologi dan kriminologi dengan tujuan membuat terang guna membuktikan ada tidaknya kasus kejahatan/pelanggaran dengan memeriksa barang bukti atau “*physical evidence*” dalam kasus tersebut.[80]

Forensik adalah bidang ilmu pengetahuan yang digunakan untuk membantu proses penegakan keadilan melalui proses penerapan ilmu atau sains.[81] Feri Sulianta menjelaskan bahwa forensik memiliki arti “membawa ke pengadilan”. Istilah forensik adalah suatu proses ilmiah (didasari oleh ilmu pengetahuan) dalam mengumpulkan,

---

[78] Convention on Cybercrime Budapest, 23.XI.2001; https://rm.coe.int/1680081561

[79] Al-Azhar, M. N. *Digital Forensic Panduan Praktis Investigasi Komputer*. Salemba Infotek, Jakarta, 2012.

[80] *Ibid*.

[81] Abdussalam, *Forensik*, Restu Agung: Jakarta, 2006, hlm. 7.

menganalisa, dan menghadirkan berbagai bukti dalam sidang pengadilan terkait adanya suatu kasus hukum.[82]

Istilah forensic sering digunakan dalam ilmu kedokteran yang merupakan suatu proses ilmiah (didasari oleh ilmu pengetahuan) dalam menganalisis, mengumpulkan dan menghadirkan berbagai bukti dalam sidang yang bersangkutan dengan suatu kasus hukum.[83]. Pengertian ilmu forensik yang lebih mudah yaitu ilmu dalam melakukan proses pemeriksaan dan pengumpulan bukti-bukti fisik yang terdapat di tempat kejadian perkara, kemudian dihadirkan saat sidang pengadilan.[84] Ilmu forensik meliputi berbagai kelompok ilmu pengetahuan yang membantu dalam proses pengumpulan berbagai bukti melalui penerapan ilmu atau sains diantaranya ilmu fisika forensik, ilmu kimia forensik, ilmu psikologi forensik, ilmu kedokteran forensik, ilmu toksikologi forensik, ilmu psikiatri forensik, komputer forensik dan sebagainya.[85]

Forensik dalam bahasa hukum dapat diartikan sebagai hasil pemeriksaan yang diperlukan dalam proses pengadilan. Sedangkan forensik dalam pengertian bahasa Indonesia berarti berhubungan dengan pengadilan. Ilmu forensik (*Forensic Science*) adalah meliputi semua ilmu pengetahuan yang mempunyai kaitan dengan masalah

---

[82] Feri Sulianta, *Komputer Forensik*, Elex Media Komputindo, Jakarta, 2008, hlm. 2

[83] *Ibid*.

[84] Wiratama, Bramanda, Fredy Nur Pratama dan Ismail Eka Syahrial, (2015), "Peran Serta Proses Identifikasi Laboratorium Forensik dalam Penyidikan Kasus Pemalsuan Surat dan Tandatangan", Jurnal GEMA Vol. 50.

[85] *Ibid*.

kejahatan, atau dapat dikatakan bahwa dari segi perannya dalam penyelesaian kasus kejahatan maka ilmu-ilmu forensik memegang peranan penting.[86] Dari semua peranan ilmu-ilmu pengetahuan yang mempunyai kaitan dengan masalah kejahatan tersebut, ialah:[87] hukum pidana, hukum acara pidana, ilmu kedokteran forensic, ilmu kimia forensic, ilmu fisika (alam) forensic, kriminologi. psikologi forensic, dan psikiatri/neurologi forensic.

2. Digital Forensik

Seiring dengan perkembangan ilmu pengetahuan dan teknologi modern, menyebabkan penanganan terhadap kasus-kasus tindak pidana terutama dalam proses penyelidikan dan penyidikan mengalami kemajuan dan perkembangan. Diantaranya dapat dilihat dari bagaimana proses-proses penyelesaian perkara pidana dilakukan dengan penerapan ilmu penunjang lainnya oleh penyidik yang memiliki kompetensi sesuai dengan dimilikinya untuk memudahkan proses penanganan perkara tersebut.[88]

Dari keunikan yang terdapat dalam perangkat digital sebagai barang bukti dalam suatu perkara pidana yang menggunakan teknologi informasi ini, pada pelaksanaan investigasi penyidik memerlukan ilmu penunjang lain untuk mencari bukti digital yang

---

[86] R. Soeparmono, *Keterangan Ahli & Visum et Repertum dalam Aspek Hukum Acara Pidana,* Mandar Maju, Bandung, 2011, hal 11.

[87] *Ibid* hal 12.

[88] Synthiana Rachmie, (2020), *Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website*, Jurnal Litigasi (e-Journal), Vol. 21 (1), hal 106.

tersimpan di dalam komputer yang digunakan oleh pelaku kejahatan, ilmu penunjang dimaksud salah satunya yaitu ilmu digital forensik.

Digital forensik adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan atau penyaringan, dan dokumentasi bukti digital dalam kejahatan komputer.[89] Digital forensik adalah suatu rangkaian metodologi yang terdiri dari teknik dan prosedur untuk mengumpulkan bukti-bukti dari perangkat komputer, berbagai perangkat penyimpanan dan media digital agar dapat dipergunakan secara sah sebagai alat bukti di pengadilan.[90] Digital forensik adalah proses mengambil, menjaga, mengembalikan, dan menyajikan data yang telah diproses secara elektronik dan disimpan di media komputer.[91]

Diperlukan penerapan ilmu digital forensik ini untuk mengungkap fakta atau bukti yang berkaitan dengan kasus agar menjadi terang dan jelasnya suatu tindak pidana yang dimulai dari tahap penyidikan sampai pembuktian di persidangan. Dalam melakukan investigasi melalui digital forensik ada berbagai macam aplikasi sebagai analisis bantu yang beredar di pasar internet mulai dari aplikasi yang gratis maupun aplikasi yang berbayar, diantaranya yang terkenal yaitu

---

[89] Marcella, A. J dan Greenfiled, *Cyber Forensics a Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes*, CRC Press LLC: Florida, 2002, hlm. 10

[90] Sammes, Jenkinson, *Forensic Computing a Practitioner's Guide*, Springer: London, 2007, hlm. 22.

[91] I Made Wiryana, *SAFFA-NG Sistem Arsitektur Manajemen Kasus Forensik, Indonesian* Journal of Legal and Forensic Sciences (IJLFS). Http://ojs.unud.ac.id/index.php/ijlfs/article/view/3220 diakses 20 Oktober 2020

Encase, Access Data FTK, *Belkasoft*, *Autopsy* dan lain sebagainya untuk dapat melakukan pencarian alat bukti dalam proses penegakan hukum.[92]

Digital Forensic adalah suatu disiplin ilmu turunan keamanan komputer yang membahas tentang temuan bukti digital setelah suatu peristiwa terjadi. Kegiatan digital forensik sendiri adalah suatu proses mengidentifikasi, memelihara, menganalisa dan mempergunakan bukti digital menurut hukum yang berlaku.[93] Dalam digital forensic terdapat prinsip-prinsip dasar. Prinsip dasar Digital Forensic berdasarkan ACPO[94] antara lain:[95]

1. Lembaga hukum dan atau petugasnya dilarang mengubah data digital yang tersimpan dalam media penyimpanan yang selanjutnya dibawa ke pengadilan.
2. Seseorang yang merasa perlu mengakses data digital yang tersimpan dalam media penyimpanan barang bukti, maka orang tersebut harus jelas kompetensi, relevansi dan implikasi dari tindakan yang dilakukan terhadap barang bukti.
3. Catatan teknis dan praktis mengenai langkah-langkah yang dilakukan terhadap media penyimpanan selama proses

---

[92] Rizki, Sari dan Nursiti. (2018), *Analisis Digital Forensic Dalam Mengungkapkan Tindak Kejahatan Cyber Pada Tahap Pembuktian*, JIM Bidang Hukum Pidana : Vol.2, No.4.

[93] Asrizal, *Digital Forensik Apa dan Bagaimana*,diakses dari: http://e-dokumen.kemenag.go.id/files/VQ2Hv7uT1339506324.pdf.

[94] The Association of Chief Police Officers of England, Wales and Northern Ireland

[95] Yudha Fietyata, (2015). *Usb Analysis Tool Untuk Investigasi Forensik Digital*. Jurnal Teknoin Vol. 21 No. 4.

pemeriksaan dan analisa berlangsung, jika terdapat pihak ketiga yang melakukan investigasi terhadap media penyimpanan tersebut mendapatkan hasil yang sama.

Digital forensik merupakan ilmu yang membahas tentang temuan yang berupa bukti digital setelah peristiwa yang berkaitan dengan keamanan komputer terjadi. Digital forensik bisa dikatakan penerapan ilmu pengetahuan untuk memulihkan bukti digital dari suatu perangkat baik itu komputer maupun *smartphone* dengan metode tertentu yang bertujuan untuk mengumpulkan data yang dapat diterima oleh pengadilan sebagai salah satu pembuktian.[96] Salah satu media digital forensic adalah *mobile forensic*. Mobile forensik bertujuan untuk melakukan pengembalian data dari perangkat *mobile*.

Pada kejahatan *cyber*, kontak dapat terjadi ketika dua komputer melakukan kontak satu sama lain dalam sebuah jaringan sebagaimana yang disebutkan dalam teori "*Cyber Exchange*".[97] Maksud dari teori *Cyber Exchange* tersebut adalah bahwa kontak yang terjadi dengan perangkat elektronik tidak menimbulkan jejak secara fisik karena manusia tidak datang secara langsung dan tidak melakukan kontak secara fisik dengan tempat kejadian perkara. Namun kontak yang terjadi adalah kontak "maya". Maka jejak yang

[96] Deris Setiawan, *Sistem Keamanan Komputer*, *loc.cit*.

[97] Horiyah, *Prinsip Locard's Exchange dan Kaitannya Dengan Digital forensik*, Jurnal TeknikInformatika, e-journal online. <www.academia.edu> data akses 20 Mei 2023 pukul 21.35 wita.

ditinggalkan pada kontak tersebut disebut sebagai bukti digital. Untuk mencari bukti digital yang tersimpan di dalam komputer yang digunakan oleh pelaku kejahatan, diperlukan metode digital forensik, yaitu metode ilmiah untuk mengumpulkan dan menganalisis data-data dan jejak dari system komputer, jaringan, dan perangkat penyimpanan.

Penanganan digital forensik secara umum mengacu pada *National Institute of Justice* (NIJ) yang merupakan lembaga penelitian dan evaluasi Departemen Kehakiman Amerika Serikat yang memberikan standar model digital forensik dalam buku "Forensic Computing Models: Technical Overview",[98] dengan tahapan sebagai berikut:

1. Tahapan dan Prosedur Identifikasi

   Dalam tahapan identifikasi merujuk pada standar identifikasi dalam penanganan ISO 17025 tahun 2017 meliputi 4 unsur tahapan yaitu:[99]

   a. Proses identifikasi media atau biasa disebut *Electronically Stored Information* (ESI) yang dinilai dapat menjadi sumber data;
   b. Aktivitas pengumpulan;
   c. Aktivitas akuisisi data; dan

[98] Gulshan Shrivastava, Kavita Sharma, Akansha Dwivedi, *Forensic Computing Models:Technical Overview*, artikel diunduh di: : https://www.researchgate.net/publication/242524844.

[99] International Organization for Standardization 27037.

d. Proses preservasi (pengamanan) terhadap perangkat/bukti elektronik

Tahap identifikasi yaitu proses penanganan awal bukti elektronik di tempat kejadian perkara (TKP) yang bersifat *volatily* (mudah berubah, hilang, dan rusak). Dalam proses identifikasi perlu dilakukan pengidentifikasian beberapa media penyimpanan data (seperti hard disk, *flash drive*, CD, kartu memori, dll), perangkat elektronik (komputer, gawai, kamera, dll), dan log aktivitas jaringan dari penyedia internet yang memiliki relevansi dengan tindak pidana. Oleh karena itu perlu personil digital forensik yang berkompeten dalam memetakan bukti elektronik dan pemiliknya itu, untuk kemudian berkoordinasi dengan penyidik untuk melakukan sita terhadap bukti elektronik yang terkait tindak pidana.

2. Tahapan dan Prosedur Eksaminasi

Setelah perangkat elektronik yang mengandung bukti elektronik relevan telah diidentifikasi, personil harus memutuskan apakah akan mengumpulkan (koleksi) atau mengakuisisi pada proses berikutnya. Terdapat beberapa faktor penentu untuk menentukan pilihan itu, salah satunya kondisi sekitar dan kondisi

perangkat elektronik.[100] Koleksi adalah proses dalam penanganan bukti elektronik di mana perangkat yang berisi bukti elektronik dipindahkan dari lokasi asli ke laboratorium forensik atau lingkungan lain yang terkendali untuk akuisisi dan analisis selanjutnya. Sedangkan akuisisi yaitu proses pemindahan bukti elektronik dari perangkat elektronik asal ke penyimpanan personil/penyidik untuk dianalisis lebih lanjut.[101] Dalam proses pengumpulan perangkat elektronik, hal-hal yang perlu diperhatikan oleh personil diantaranya:[102]

a. Verifikasi integritas data untuk membuktikan bahwa data yang dikumpulkan tidak diubah atau dirusak.
b. Perlengkapan dalam proses pengumpulan perangkat elektronik, seperti penggunaan sarung tangan untuk menghindari tempering terhadap bukti laten (sidik jari, DNA, dll).
c. Pembungkusan terhadap perangkat elektronik dalam tamper-evident bag dan label, diberi nomor sesuai label bukti, nama FR, tanggal waktu pengumpulan, dan spesifikasi bukti. Hindari suhu ekstrim, magnet berukuran besar, air, lembap, dan kondisi lainnya yang mungkin mempengaruhi bukti elektronik.

[100] Rizki Zakariya, 2019. *Pemanfaatan Digital forensik Dalam Penanganan Perkara Tindak Pidana Pemilu*, artikel dalam Prosiding Call Paper dan Seminar Nasional Tata Kelola Pemilu, Komisi Pemilihan Umum: Jakarta, hal 21.

[101] *Ibid*.

[102] *Ibid* hal 22.

d. Pencatatan rincian perangkat elektronik yang dikumpulkan, kemudian pendokumentasian dalam *chain of custody*[103] dan dijelaskan juga alasan dikumpulkan.

Apabila tahapan itu selesai, selanjutnya perangkat elektronik dibawa oleh personil/penyidik ke laboratorium untuk dilakukan akuisisi dan analisis. Dalam akuisisi itu diperlukan kompetensi khusus selain kewenangan, seperti penggunaan metode akuisisi physical atau logical. Sehingga setelah diakuisisi bukti elektronik itu tidak berubah (message digest atau hashing) antara bukti asli di TKP dengan bukti yang disalin.[104]

3. Tahapan dan Prosedur Analisis

Setelah didapatkan data-data elektronik yang terkait tindak pidana, selanjutnya dilakukan analisis terhadap data-data itu. Akan tetapi, sebelum itu data di-*indexing* terlebih dahulu. Indexing merupakan proses pengkategorisasian setiap kata dalam data elektronik sehingga menjadi dapat dicari. Tahapan analisis harus dilakukan oleh personel kompeten yang memahami kronologis kejadian perkara, oleh karena itu dibutuhkan koordinasi dengan penyidik yang memahami awal-mula perkara. Melalui analisis itu dapat diketahui pihak yang terlibat, lokasi, rangkaian kejadian, modus, dan sebagainya. Hasil itu selanjutnya disebut sebagai

[103] *Chain of Custody* (CoC) adalah sebuah istilah yang merujuk pada catatan atau jejak audit digital yang menunjukkan histori perpindahan tanggung jawab atas suatu aset digital ataupun fisik dari satu pihak *custodian* ke pihak custodian lainnya.

[104] Rizki Zakariya, *Op.cit.,* hlm 23.

barang bukti elektronik yang harus dapat dipertanggungjawabkan secara teknis keilmiahannya dan secara hukum di depan pengadilan.[105]

4. Tahapan dan Prosedur Pelaporan

Setelah diketahui fakta tertentu terkait tindak pidana melalui analisis digital forensik, kemudian dilakukan pelaporan hasil analisis dalam laporan forensik. Selanjutnya laporan itu diserahkan ke penyidik untuk kepentingan pembuktian tindak pidana. Pelaporan itu juga disertai dengan *chain of custody*, yang berisi catatan rantai tiap tahapan penanganan bukti elektronik yang dilakukan oleh personel.[106]

D. Kepolisian Dalam Penegakan Hukum Pidana

Landasan filosofis Kepolisian dalam melaksanakan tugas adalah berdasarkan ketentuan Pasal 30 Ayat (4) Undang-undang Dasar 1945 yang menyatakan Kepolisian Negara Republik Indonesia sebagai alat negara yang menjaga keamanan dan ketertiban masyarakat bertugas melindungi, mengayomi, melayani masyarakat serta menegakkan hukum. Berdasarkan ketentuan Pasal 30 Ayat (4) UUD 1945 tersebut maka Pemerintah bersama Dewan Perwakilan Rakyat (DPR) membuat peraturan tentang Kepolisian Negara Republik Indonesia dalam Undang-Undang Nomor 2 tahun 2002 sebagai landasan dalam pelaksanaan tugas.

[105] *Ibid*.
[106] *Ibid* hal 24.

Dalam ketentuan Pasal 1 Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian ditentukan bahwa Kepolisian adalah segala hal-ihwal yang berkaitan dengan fungsi dan lembaga polisi sesuai dengan peraturan perundang-undangan. Sedangkan pada Pasal 2 dikatakan bahwa fungsi kepolisian adalah salah satu fungsi pemerintahan negara di bidang pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, perlindungan, pengayoman, dan pelayanan kepada masyarakat. Kepolisian adalah salah satu lembaga yang sangat berperan dalam proses penegakan hukum di Indonesia. Oleh karena itu Kepolisian merupakan salah satu bagian dari sistem peradilan pidana (*criminal justice system*).

Kepolisian dalam pelaksanaan tugas dibidang penegakan hukum seperti penyelidikan dan penyidikan tindak pidana berdasarkan Pasal 1 angka 5 KUHAP “Penyelidikan adalah serangkaian tindakan penyelidik untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyidikan menurut cara yang diatur dalam Undan-Undang ini” sedangkan Penyidikan menurut KUHAP Pasal 1 angka 2 KUHAP disebutkan “Penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam Undang-Undang ini untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan Tersangkanya”. Sementara definisi Penyelidik menurut Pasal 1 angka 4 KUHAP

“Penyelidik adalah Pejabat Polisi Negara Republik Indonesia yang diberi wewenang oleh Undang-Undang ini untuk melakukan penyelidikan” dan penyidik menurut 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” dimana dalam pelaksanaan tugas penegakan hukum selalu menjunjung tinggi HAM berdasarkan ketentuan Pasal 14 huruf g dan i Undang-Undang Nomor 2 Tahun 2002).

Satjipto Rahardjo menyebut Polri sebagai penegak hukum kelas jalanan (dalam konotasi positif, yang langsung bekerja di lapangan), sehingga Polri-lah yang paling banyak berhubungan langsung dengan masyarakat, dibandingkan dengan penegak hukum lainnya. Oleh karena itu, sikap dan keteladanan personil kepolisian menjadi salah satu faktor dihargai atau tidaknya personil kepolisian oleh warga masyarakat, padahal penghargaan atau rasa hormat warga masyarakat terhadap penegak hukum juga cukup berpengaruh terhadap ketaatan mereka. [107]

Dalam pandangan Satjipto Rahardjo, penegakan Hukum dilakukan oleh Instansi yang diberi wewenang untuk itu seperti Polisi, Jaksa dan Pejabat Pemerintahan sudah berlaku sejak hukum itu mengandung perintah dan larangan yang sifatnya memaksa (*Coercion*). Dengan begitu, maka sejak awal hukum tersebut telah membutuhkan bantuan untuk mewujudkan atau menerapkan perintah tersebut jika tidak demikian

[107] Achmad Ali dan Wiwie Heryani, *Menjelajahi Kajian Empiris Terhadap Hukum,* Kencana, Jakarta, 2012, hal 154.

maka tentu saja hukum itu hanya peraturan tertulis yang tidak memiliki makna oleh karena itu dibuatlah ketentuan yang mengatur Lembaga penegak hukum yang diberikan kewenangan oleh Undang-Undang untuk menjalankan hukum tersebut. [108]

E. Penyelidikan dan Penyidikan Dalam Hukum Acara Pidana

1. Penyelidikan

Pasal 1 angka 5 KUHAP mendefinisikan penyelidikan sebagai serangkaian tindakan penyelidik untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyidikan menurut cara yang diatur dalam undang-undang ini. Pasal 1 angka 2 KUHAP menyebutkan bahwa Penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya.

Pada tahap penyelidikan (atau lazim disebut lidik), fungsi penyidik dilakukan penyelidikan hanya bertugas untuk mengetahui dan menentukan peristiwa apa yang sesungguhnya telah terjadi dan bertugas membuat berita acara serta laporannya nantinya merupakan dasar permulaan penyidikan. Penyelidikan dilakukan berdasarkan : a) Informasi atau laporan yang diterima maupun

[108] Satjipto Rahardjo, *Masalah Penegakan Hukum Suatu Tinjauan Sosiologis*, Penerbit Sinar Baru Bandung, 2002, hal 173.

diketahui langsung oleh penyelidik/penyidik; b) Laporan; c) Berita Acara pemeriksaan di TKP; d) Berita Acara pemeriksaan tersangka dan atau saksi.[109] Proses penyelidikan tindak pidana dilakukan untuk:

a. Mencari keterangan-keterangan dan bukti guna menentukan suatu peristiwa yang dilaporkan atau diadukan, apakah merupakan tindak pidana atau bukan.
b. Melengkapi keterangan dan bukti-bukti yang telah diproses agar menjadi jelas sebelum dilakukan penindakan selanjutnya;
c. Persiapan pelaksanaan penindakan dan atau pemeriksaan. Penyelidikan bukanlah fungsi yang berdiri sendiri melainkan hanya merupakan salah satu metode atau sub dari fungsi penyidikan. [110]

M. Yahya Harahap dalam bukunya "Pembahasan Permasalahan dan Penerapan KUHAP: Penyidikan dan Penuntutan", menjelaskan bahwa dari pengertian dalam KUHAP, penyelidikan adalah tindakan tahap pertama permulaan dari penyidikan. Akan tetapi harus diingat, penyelidikan bukan tindakan yang berdiri sendiri terpisah dari fungsi penyidikan. Penyelidikan merupakan bagian yang tak terpisah dari fungsi penyidikan. Kalau dipinjam kata-kata yang digunakan buku petunjuk Pedoman Pelaksanaan KUHAP, penyelidikan merupakan salah satu cara atau metode atau sub daripada fungsi penyidikan

[109] M. Husein Harun, *Penyidik dan Penuntut Dalam Proses Pidana*, PT. Reneka Cipta, Jakarta, 1991, hal. 56

[110] Halpunan Bujuklap, Bujuklap, Bujukmin JAMPIDSUS, *Proses Penyidikan Tindak Pidana*, Kejaksaan RI, Jakarta, 1990, hal 17.

yang mendahului tindakan lain, yaitu penindakan berupa penangkapan, penahanan, penggeledahan, penyitaan, pemeriksaan surat, pemanggilan, tindakan pemeriksaan, dan penyerahan berkas kepada penuntut umum.[111]

Lebih lanjut, M. Yahya Harahap menyatakan sebelum dilakukan tindakan penyidikan, dilakukan dulu penyelidikan oleh pejabat penyelidik, dengan maksud dan tujuan mengumpulkan "bukti permulaan" atau "bukti yang cukup" agar dapat dilakukan tindak lanjut penyidikan. Mungkin penyelidikan dapat disamakan dengan pengertian "tindak pengusutan" sebagai usaha mencari dan menemukan jejak berupa keterangan dan bukti-bukti suatu peristiwa yang diduga merupakan tindak pidana.[112]

Yahya Harahap menambahkan jika diperhatikan dengan seksama, motivasi dan tujuan penyelidikan, merupakan tuntutan tanggung jawab kepada aparat penyidik, untuk tidak melakukan tindakan penegakan hukum yang merendahkan harkat martabat manusia. Sebelum melangkah melakukan pemeriksaan penyidikan seperti penangkapan atau penahanan, harus lebih dulu berusaha mengumpulkan fakta dan bukti, sebagai landasan tindak lanjut penyidikan.[113]

---

[111] Yahya Harahap. *Op.cit*..
[112] *Ibid* hal 102.
[113] *Ibid*.

2. Penyidikan

Kata “Penyidikan” sendiri dipakai sebagai istilah hukum pada Tahun 1961, yaitu sejak dimuatnya dalam Undang-Undang pokok kepolisian No. 13 Tahun 1961. Sebelumnya dipakai istilah pengusutan yang merupakan terjemah dari bahasa Belanda, yaitu “opsporing”. Pasal 1 butir 2 (Kitab Undang-undang Hukum Acara Pidana) KUHAP diuraikan bahwa penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang, mencari dan mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya. Penyidikan ditekankan pada proses pencarian serta pengumpulan bukti tindakan pidananya. Sehingga bisa diketahui siapa tersangka atau pelaku tindak pidana.

Berbicara mengenai penyidikan tidak lain dari membicarakan masalah pengusutan kejahatan atau pelanggaran, orang Inggris lazim menyebutnya dengan istilah ”criminal investigation". Tujuan penyidikan adalah untuk menunjuk siapa yang telah melakukan kejahatan dan memberikan pembuktian-pembuktian mengenai masalah yang telah dilakukannya. Untuk mencapai maksud tersebut maka penyidik akan menghimpun keterangan dengan fakta atau peristiwa-peristiwa tertentu.[114]

Penyidikan dimulai sesudah terjadinya tindak pidana untuk

[114] *Op.cit*., hal 58.

mendapatkan keterangan-keterangan tentang:

a. Tindak pidana apa yang telah dilakukan.
b. Kapan tindak pidana itu dilakukan.
c. Dimana tindak pidana itu dilakukan.
d. Dengan apa tindak pidana itu dilakukan.
e. Bagaimana tindak pidana itu dilakukan.
f. Mengapa tindak pidana itu dilakukan.
g. Siapa pembuatnya.

Dalam proses penyidikan tindak pidana, aspeknya penyidikan meliputi: [115]

a. Penyelidikan;
b. Penindakan, meliputi: pemanggilan, penangkapan, penahanan, penggeledahan, penyitaan.
c. Pemeriksaan, meliputi: pemeriksaan saksi, pemeriksaan ahli dan pemeriksaan tersangka.
d. Penyelesaian dan penyerahan berkas perkara, dengan tahapan; pembuatan resume, penyusunan berkas perkara, dan penyerahan berkas perkara

Sedangkan kegiatan Penyidikan meliputi:

a. Penyidikan berdasarkan informasi atau laporan yang diterima maupun yang diketahui langsung oleh penyidik, laporan polisi,

[115] Halpunan Bujuklap, Bujuklap, Bujukmin JAMPIDSUS, *op.cit.,* hal 24.
M. Husein Harun, *Penyidik dan Penuntut Dalam Proses Pidana, op.cit*.

berita acara pemeriksaan tersangka, dan berita acara pemeriksaan saksi.

b. Penindakan adalah setiap tindakan hukum yang dilakukan oleh penyidik/penyidik pembantu terhadap orang maupun barang yang ada hubungannya dengan tindak pidana yang terjadi. Penindakan hukum tersebut berupa pemanggilan tersangka dan saksi, penangkapan, penahanan, penggeledahan, dan penyitaan.

c. Pemeriksaan adalah merupakan kegiatan untuk mendapatkan keterangan, kejelasan dan keidentikan tersangka dan atau saksi dan atau barang bukti ataupun unsur-unsur tindak pidana yang terjadi sehingga kedudukan dan peranan seseorang maupun barang bukti di dalam tindak pidana menjadi jelas dan dituangkan dalam berita acara pemeriksaan . yang berwenang melakukan pemeriksaan adalah penyidik dan penyidik pembantu.

d. Penyelesaian dan Penyerahan Berkas Perkara, merupakan kegiatan akhir dari proses penyidikan tindak pidana yang dilakukan oleh penyidik dan penyidik pembantu.[116]

Sehingga, fokus utama dari kegiatan penyidikan adalah menemukan tersangkanya sekaligus melengkapi bukti-bukti lain yang telah dikumpulkan sejak tahap penyelidikan. Dengan menemukan

[116] M. Husein Harun,*op.cit*., hal. 89.

tersangkanya, maka akan diketahui motif, modus operandi yang digunakan serta hal-hal lain yang dirasa penting untuk dikembangkan.

F. Tindak Pidana, Unsur Pidana, Pertanggungjawaban Pidana dan Sanksi Pidana

1. Tindak Pidana

Beberapa ahli sering menyebut tindak pidana sebagai "*strafbaar feit*". Pengertian tindak pidana yang dimuat di dalam Kitab Undang-Undang Hukum Pidana (KUHP) oleh pembentuk undang- undang juga sering disebut dengan "*strafbaar feit*". Istilah "*strafbaar feit*" sendiri dalam bahasa Belanda terdiri atas tiga kata, yaitu "*straf*": yang berarti hukuman (pidana), "*baar*" yang berarti dapat (boleh), dan "*feit*" yang berarti tindak, peristiwa, pelanggaran dan perbuatan. Jadi istilah "*strafbaar feit*" adalah peristiwa yang dapat dipidana atau perbuatan yang dapat dipidana.[117]

Simons menyebutkan bahwa "*strafbaar feit*" adalah tindakan melanggar hukum yang telah dilakukan dengan sengaja ataupun tidak dengan sengaja oleh seseorang yang dapat dipertanggungjawabkan atas tindakannya dan oleh undang-undang

[117] *Ibid*.

telah dinyatakan sebagai tindakan hukum.[118] Rumusan demikian karena: [119]

a. Untuk adanya suatu ”strafbaar feit” disyaratkan bahwa disitu terdapat suatu tindakan yang dilarang ataupun yang diwajibkan seperti itu telah dinyatakan sebagai tindakan yang dapat dihukum.
b. Agar suatu tindakan seperti itu dapat dihukum maka tindakan itu harus memenuhi semua unsur dari delik seperti yang dirumuskan dengan undang-undang.
c. Setiap ”*strafbaar feit*” sebagai pelanggaran terhadap suatu larangan atau kewajiban menurut undang-undang itu, pada hakikatnya merupakan tindakan melawan hukum atau suatu *onrechtmatige handeling*. Jadi sifat melawan hukum timbul dari suatu kenyataan bahwa tindakan manusia bertentangan dengan peraturan perundangan-undangan, hingga pada dasarnya sifat tersebut bukan suatu unsur dari delik yang mempunyai arti tersendiri seperti halnya dengan unsur lain.

Menurut Utrecht, ”*strafbaar feit*” adalah peristiwa pidana yang sering juga disebut delik, karena peristiwa itu suatu perbuatan *handeuleum* atau *doen-positif* atau melalaikan *natalen-negatif*, maupun akibatnya (keadaan yang ditimbulkan karena perbuatan

[118] *Ibid*.
[119] P.A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, Citra Aditya Bakti, Bandung, 1997, hal. 34.

atau melalaikan itu). Peristiwa pidana yang merupakan peristiwa hukum (*rechtsfeit*) yaitu peristiwa kemasyarakatan yang membawa akibat yang diatur oleh hukum. Tindakan semua unsur yang disinggung oleh suatu ketentuan pidana dijadikan unsur yang mutlak suatu dari peristiwa pidana, yaitu perilaku manusia yang bertentangan dengan hukum (unsur melawan hukum), oleh sebab itu dapat dijatuhi suatu hukuman dan adanya seorang pembuat dalam arti kata bertanggung jawab.[120]

Sebastian Pompe menjelaskan bahwa secara teoritis ”*strafbaar feit*” dapat dirumuskan sebagai suatu pelanggaran norma atau gangguan terhadap tertib hukum yang dengan sengaja atau tidak sengaja telah dilakukan oleh seorang pelaku, dimana penjatuhan hukuman terhadap pelaku itu adalah penting demi terpeliharanya tertib hukum dan terjaminnya kepentingan umum.”[121] Di sini berlaku ” tiada dipidana tanpa kesalahan ” (*keine strafe ohne schuld* atau *geen straafbaarfeit zonder schuld* atau *nulla poena sine culpa*). Culpa di sini dalam arti luas, meliputi juga kesengajaan.

Hazewinkel Suringa menjelaskan bahwa “*strafbaar feit*” yang bersifat umum yakni suatu perilaku manumur (berdasarkan usia, waktu) yang pada suatu saat tertentu telah ditolak di dalam suatu pergaulan hidup tertentu dan dianggap sebagai perilaku yang harus ditiadakan oleh hukum pidana dengan menggunakan sarana- sarana

[120] *Ibid*.
[121] *Ibid* hal 35.

yang bersifat memaksa yang terdapat di dalam undang-undang".[122] Demikian pula Moeljatno menjelaskan bahwa "*strafbaar feit*" adalah perbuatan yang dilarang oleh suatu aturan hukum, larangan yang mana disertai sanksi berupa pidana tertentu bagi barang siapa yang melanggar aturan tersebut.[123] Sementara P.A.F. Lamintang merumuskan bahwa *strafbaar feit* sebagai suatu perbuatan melakukan atau tidak melakukan sesuatu yang memiliki unsur kesalahan sebagai perbuatan yang dilarang dan diancam dengan hukuman pidana, dimana penjatuhan pidana terhadap pelaku adalah untuk demi tercapainya tertib hukum dan terjaminnya kepentingan umum.[124]

2. Unsur Pidana

Dalam tindak pidana, unsur menjadi penting. Hal ini sesuai salah satu asas dalam hukum pidana, yaitu "*lex certa*", yaitu bahwa setiap tindak pidana harus dijelaskan unsur-unsurnya.[125] P.A.F Lamintang membagi dua unsur dalam sebuah tindak pidana, yaitu unsur obyektif dan unsur subyektif:[126]

[122] *Ibid*.

[123] Tri Andrisman, *Hukum Pidana Asas-Asas Dan Aturan Umum Hukum Pidana Indonesia*, Unila, Banjarmasin, 2009, hal.70.

[124] P. A. F Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, edisi revisi, PT Citra AdityaBakti, Bandung, 2011, hal. 181

[125] Amir Ilyas dan Muh. Nursal, N.S., *Kumpulan Asas-Asas Hukum*, Kencana Prenada Media Group, Jakarta, 2022, hal 61.

[126] P.A.F. Lamintang, *Dasar-dasar Hukum Pidana Indonesia*, Citra Aditya Bakti, Jakarta, 2014, hal. 192

a. Unsur obyektif adalah suatu unsur di luar perbuatan si pelaku dimana unsur-unsur tindakan ini harus dilakukan. Unsur objektif terdiri dari:
    1) Sifat melanggar hukum atau (*wederrechtelijkheid*);
    2) Kualitas dari si pelaku. misalnya “keadaan sebagai seorang pegawai negeri” di dalam kejahatan jabatan menurut Pasal 415 KUHP atau “keadaan sebagai pengurus atau komisaris dari suatu perseroan terbatas” di dalam kejahatan menurut Pasal 398 KUHP;
    3) Kausalitas yaitu hubungan antara suatu tindakan sebagai penyebab dengan suatu kenyataan sebagai akibat.
b. Unsur subjektif adalah suatu unsur yang terdapat atau melekat pada diri si pelaku, atau yang di hubungkan dengan diri si pelaku dan termasuk di dalamnya segala sesuatu yang terkandung di dalam hatinya. Unsur Subjektif terdiri dari:[127]
    1) Kesengajaan atau Ketidaksengajaan (Dolus atau Culpa).
    2) Maksud atau “*Voornemen*” pada suatu percobaan, seperti ditentukan dalam Pasal 53 Ayat 1 KUHP.
    3) Macam-macam maksud atau “*Oogmerk”* seperti terdapat dalam kejahatan, pencurian, penipuan, pemerasan, pemalsuan dan sebagainya.

[127] *Ibid* hal 193.

4) Merencanakan terlebih dahulu atau yang dalam bahasa belanda dikenal dengan *met voorbedachte rade* seperti tercantum dalam pasal 340 KUHP, yaitu pembunuhan yang direncanakan terlebih dahulu.
5) Perasaan takut atau dalam bahasa belanda disebut dengan "vrees" seperti terdapat di dalam Pasal 308 KUHP pembuangan anak sendiri.

Menurut beberapa ahli hukum lain yaitu E,Y Kanter dan S.R. Sianturi berpendapat bahwa unsur - unsur tindak pidana adalah sebagai berikut:[128]

a. Subyek;
b. Kesalahan;
c. Bersifat melawan hukum dari suatu tindakan;
d. Suatu tindakan yang dilarang atau diharuskan oleh undang-undang dan terhadap pelanggarannya diancam dengan pidana;
e. Waktu, tempat, dan keadaan (unsur objektif lainnya).

Sementara itu, rumusan unsur-unsur tindak pidana menurut Simons yaitu:

a. Perbuatan manusia (positif atau negatif, berbuat atau tidak berbuat atau membiarkan);
b. Diancam dengan pidana (*strafbaar gesteld*);

[128] E,Y Kanter dan S.R. Sianturi dalam Amir Ilyas, *Asas-Asas Hukum Pidana,* Rangkang Education & PuKAP – Indonesia, Yogyakarta, 2012, hal.26

c. Melawan hukum (*onrechtmatig*);

d. Dilakukan dengan kesalahan (*met schuld in verband staad*);

e. Oleh orang yang mampu bertanggung jawab (*toerekeningsvatbaar persoon*).

Dari unsur-unsur tindak pidana tersebut Simons membedakan adanya unsur obyektif dan unsur subjektif dari *strafbaarfeit* adalah:

a. Yang dimaksud dengan unsur subyektif ialah : perbuatan orang;

b. Akibat yang kelihatan dari perbuatan itu;

c. Mungkin ada keadaan tertentu yang menyertai perbuatan-perbuatan itu seperti dalam Pasal 281 KUHP sifat ”*openbaar*” atau ”dimuka umum”

Selanjutnya unsur subjektif dari “*strafbaarfeit*” adalah :1) orangnya mampu bertanggung jawab; 2) Adanya kesalahan (dolus atau culpa). Perbuatan harus dilakukan dari perbuatan atau dengan keadaan-keadaan mana perbuatan itu dilakukan

3. Pertanggungjawaban Pidana

Menurut hukum tanggung jawab (*responsibility*) adalah suatu akibat atas konsekuensi kebebasan seseorang tentang perbuatannya yang berkaitan dengan etika atau moral dalam melakukan suatu perbuatan.[129].Dalam hukum pidana dikenal asas “tiada pidana tanpa kesalahan” (*geen straf zonder schuld*), Seseorang hanya dapat

[129] Soekidjo Notoatmodjo, *Etika dan Hukum Kesehatan*, Rineka Cipta, Jakarta, 2010, hal 25.

dihukum atas perbuatannya yang melanggar hukum apabila terhadap dirinya terdapat kesalahan. Kesalahan merupakan unsur yang fundamental dalam hukum pidana. Kesalahan adalah dapat dicelanya pembuat tindak pidana karena dilihat dari segi masyarakat sebenarnya dapat berbuat lain jika tidak ingin melakukan perbuatan tersebut.[130] Orang dapat dikatakan mempunyai kesalahan, jika pada waktu melakukan perbuatan pidana, dilihat dari segi masyarakat dapat dicela karenanya, yaitu kenapa melakukan perbuatan yang merugikan masyarakat padahal mampu untuk mengetahui makna perbuatan tersebut, dan karenanya dapat, bahkan harus menghindari perbuatan demikian.[131]

Pertanggungjawaban pidana (*criminal responsibility*) harus memenuhi unsur *mens rea* dan *actus reus* sehingga terhadap pelakunya dapat dikenakan pemidanaan. *Mens rea* adalah sikap batin (niat jahat) pelaku perbuatan pidana. Berbeda dengan *actus reus* yang menyangkut perbuatan yang melawan hukum (*unlawful act*), *mens rea* mencakup unsur-unsur pembuat tindak pidana yaitu sikap batin yang disebut unsur subyektif suatu tindak pidana atau keadaan psikis pembuat.[132] Utrecht menambahkan bahwa

[130] Roeslan Saleh dalam Mahrus Ali, *Dasar-Dasar Hukum Pidana*, Cetakan Kedua, Sinar Grafika, Jakarta, 2012, hal.157.

[131] Moeljatno dalam Mahrus Ali, 2012, *Ibid.*

[132] E. Utrecht, *Hukum Pidana*, Universitas Gadjah Mada (UGM) Press, Yogyakarta, 1960, hal 257.

pertanggungjawaban pidana atau kesalahan menurut hukum pidana (*schuld in ruime zin*) terdiri atas tiga anasir yaitu:[133]

1. Kemampuan bertanggung jawab (*toerekeningsvatbaarheid*) dari pembuat
2. Suatu sikap psikis pembuat berhubung dengan kelakuannya, yaitu Kelakuan disengaja (anasir sengaja), dan Kelakuan kurang berhati-hati atau lalai (anasir kealpaan) atau culpa (*schuld in enge zin)*.
3. Tidak ada alasan-alasan yang menghapuskan pertanggungjawaban pidana pembuat (anasir *toerekeningsvatbaarheid*).

Dalam konteks hukum publik, pertanggungjawaban atau yang dikenal dengan konsep "*liability*" dalam segi falsafah hukum, Roscoe Pound, seorang ahli berkebangsaan Amerika yang terkenal dengan teori hukum "*law as a tool of social engineering*", menyatakan bahwa: *I..use simple word "liability" for the situation whereby one may exact legally and other is legally subjected to the exception"* pertanggungjawaban pidana diartikan Pound adalah sebagai suatu kewajiban untuk membayar pembalasan yang akan diterima pelaku dari seseorang yang telah dirugikan.[134]

[133] *Ibid*.

[134] Romli Atmasasmita, *Perbandingan Hukum Pidana*, Mandar Maju, Bandung, 2000, hal. 65.

Beberapa ahli seperti Simon Butt dan Sebastian Pompe (keduanya ahli hukum dari Australia) juga mengemukakan pendapatnya tentang pertanggungjawaban pidana. Simons mengatakan kemampuan bertanggungjawab dapat diartikan suatu keadaan psikis sedemikian rupa, sehingga penerapan suatu upaya pemidanaan, baik ditinjau secara umum maupun dari sudut orangnya dapat dibenarkan. Simon menyebut bahwa bahwa seorang pelaku tindak pidana mampu bertanggungjawab apabila: *pertama*, mampu mengetahui/ menyadari bahwa perbuatannya bertentangan dengan hukum. *Kedua*, mampu menentukan kehendaknya sesuai dengan kesadaran tadi.[135] Sebastian Pompe, menyebutkan bahwa pertanggungjawaban pidana dalam batasan unsur-unsur yaitu kemampuan berpikir pada pelaku yang memungkinkan menguasai pikirannya dan menentukan kehendaknya, pelaku dapat mengerti makna dan akibat dari tingkah lakunya serta pelaku dapat menentukan kehendaknya sesuai dengan pendapatnya (tentang makna dan akibat tingkah lakunya).[136]

Van Hamel memberikan pengertian pertanggungjawaban pidana adalah suatu keadaan normal psikis dan kemahiran yang membawa tiga macam kemampuan, yaitu *pertama*, mampu untuk dapat mengerti makna serta akibat sungguh-sungguh dari perbuatan-perbuatan sendiri. *Kedua*, mampu untuk menginsyafi bahwa

[135] Teguh Prasetyo, *Hukum Pidana,* Raja Grafindo Persada, Depok, 2010, hal 85
[136] *Ibid* hal 86.

perbuatan-perbuatan itu bertentangan dengan ketertiban masyarakat. *Ketiga*, mampu untuk menentukan kehendak berbuat.[137]

Untuk istilah ini, Roeslan Saleh menyebutnya sebagai "pertanggung-jawaban pidana".[138] Maksud celaan objektif adalah bahwa perbuatan yang dilakukan oleh seseorang memang merupakan suatu perbuatan yang dilarang. Indikatornya adalah perbuatan tersebut melawan hukum baik dalam arti melawan hukum formil maupun melawan hukum materiil. Sedangkan maksud celaan subjektif menunjuk kepada orang yang melakukan perbuatan yang dilarang tadi. Sekalipun perbuatan yang dilarang telah dilakukan oleh seseorang, namun jika orang tersebut tidak dapat dicela karena pada dirinya tidak terdapat kesalahan, maka pertanggungjawaban pidana tidak mungkin ada.

4. Sanksi Pidana

Kamus *Black's Law Dictionary Henry Campbell Black* memberikan pengertian sanksi pidana sebagai: [139]

> "..*punishment attached to conviction at crimes such fines, probation and sentences"* (suatu pidana yang dijatuhkan untuk menghukum suatu penjahat (kejahatan) seperti dengan pidana denda, pidana pengawasan dan pidana penjara).

---

[137] Eddy O.S. Hiarij, *Prinsip-Prinsip Hukum Pidana,* Cahaya Atma Pustaka, Yogyakarta, 2014, hal 121.

[138] Roeslan Saleh dalam Hanafi Amrani dan Mahrus Ali, *Sistem Pertanggungjawaban pidana Perkembangan dan Penerapan*, PT Rajawali Press, Jakarta, 2015, hal 21.

[139] Mahrus Ali, *Dasar-Dasar Hukum Pidana*, Sinar Grafika, Jakarta, 2015, hal 194.

Sanksi pidana merupakan suatu nestapa atau penderitaan yang ditimpakan kepada seseorang yang bersalah melakukan perbuatan yang dilarang oleh hukum pidana, dengan adanya sanksi tersebut diharapkan orang tidak akan melakukan tindak pidana.[140] Pengertian sanksi pidana sebagai suatu hukuman (*punishment*) juga diperkuat oleh Darwan Prints, bahwa sejatinya pidana adalah "hukuman yang dijatuhi atas diri seseorang yang terbukti secara sah dan menyakinkan melakukan tindak pidana".[141] Soejono juga menegaskan bahwa, hukuman merupakan sanksi atas pelanggaran suatu ketentuan hukum, sedangkan pidana lebih memperjelas pada sanksi yang dijatuhkan terhadap pelanggaran hukum pidana.[142]

J.E.Jonkers dalam Sholehuddin menjelaskan bahwa sanksi pidana dititikberatkan pada pidana yang diterapkan untuk kejahatan yang dilakukan, sedangkan sanksi tindakan mempunyai tujuan yang bersifat sosial".[143] Sedangkan Andi Hamzah mengatakan bahwa sanksi pidana berorientasi pada ide pengenaan sanksi terhadap pelaku suatu perbuatan, sementara sanksi tindakan berorientasi pada ide perlindungan masyarakat".[144]

---

[140] *Ibid* hal 195

[141] Darwan Prints, *Hukum Anak Indonesia*, Citra Aditya Bakti, Bandung, 2001, hal. 23.

[142] Soejono, *Kejahatan dan Penegakan Hukum di Indonesia*, Rineka Cipta, Jakarta, 1996, hal. 35.

[143] Sholehuddin, *Sistem Sanksi Dalam Hukum Pidana, Ide Dasar Double Track System Dan Implementasinya*, Raja Grafindo Persada, Jakarta, 2002, hal. 32.

[144] *Ibid*.

KUHP sebagai induk hukum pidana telah merinci jenis-jenis sanksi pidana, sebagaimana yang dirumuskan dalam Pasal 10 KUHP. Jenis-jenis pidana dibedakan atas pidana pokok dan pidana tambahan, yang terdiri dari:

a. Pidana Pokok terdiri dari: 1) Pidana mati; 2) Pidana penjara; 3) Pidana kurungan; 4) Pidana denda; dan 5) Pidana tutupan.
b. Pidana Tambahan terdiri dari: 1) Pencabutan hak-hak tertentu; 2) Perampasan barang-barang tertentu; 3) Pengumuman putusan hakim.

G. Pengaturan Bukti Elektronik Dalam Hukum Positif

1. Undang-Undang Informasi dan Transaksi Elektronk

Dalam hukum positif,[145] pengaturan tindak pidana siber di Indonesia juga dapat dilihat dalam arti luas dan arti sempit. Secara luas, tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan sistem elektronik. Itu artinya semua tindak pidana konvensional dalam KUHP (lama) dan UU No 1 Tahun 2023 (UU KUHP) sepanjang dengan menggunakan bantuan atau sarana sistem elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas. Demikian juga tindak pidana dalam Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana (UU Transfer Dana) maupun tindak pidana perbankan serta

[145] Hukum positif yang dimaksud adalah UU ITE dan perundang-undangan lain yang secara eksplisit mengatur tindak pidana elektronik.

tindak pidana pencucian uang dalam Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU). Akan tetapi dalam pengertian yang lebih sempit, pengaturan tindak pidana siber diatur dalam UU ITE. Sama halnya dengan *Convention on Cybercrimes*, UU ITE juga tidak memuat definisi mengenai *cybercrime,* tetapi membaginya menjadi beberapa kelompok yang mengacu pada *Convention on Cybercrimes*.[146]

Dalam UU ITE, terdapat sejumlah kualifikasi delik atau tindak pidana yang berhubungan dengan aktivitas illegal, sebagaimana dalam tabel berikut:

Tabel 1; tindak pidana dalam UU ITE

Kategori	Delik	Pasal
Distribusi atau penyebaran, transmisi, dapat diaksesnya konten illegal,	Kesusilaan	Pasal 27 ayat (1)
	Perjudian	Pasal 27 ayat (2)
	penghinaan dan/atau pencemaran nama baik.	Pasal 27 ayat (3)
	Pemerasan dan/atau pengancaman.	Pasal 27 ayat (4)
	Berita bohong yang menyesatkan dan merugikan konsumen.	Pasal 28 ayat (1)
	menimbulkan rasa kebencian berdasarkan SARA.	Pasal 28 ayat (2)
	mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang	Pasal 29

[146] Josua Sitompul. 2012. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*, PT. Tatanusa.

	ditujukan secara pribadi.	
	dengan cara apapun melakukan akses illegal	Pasal 30
	intersepsi atau penyadapan illegal terhadap informasi atau dokumen elektronik dan Sistem Elektronik	Pasal 31
Tindak pidana yang berhubungan dengan gangguan (interferensi), yaitu:	Gangguan terhadap Informasi atau Dokumen Elektronik (*data interference*)	Pasal 32
	Gangguan terhadap Sistem Elektronik (*system interference*)	Pasal 33
	Tindak pidana memfasilitasi perbuatan yang dilarang	Pasal 34
	Tindak pidana tambahan (*accessoir*)	Pasal 36
	Perberatan-perberatan terhadap ancaman pidana	Pasal 52
	Tindak pidana pemalsuan informasi atau dokumen elektronik	Pasal 35

Sumber: Josua Sitompul[147]

Digital forensik menjadi metode untuk membuktikan pelanggaran terhadap pasal-pasal ini, seperti penyusupan ke sistem (*hacking*), pencurian data, dan sabotase digital. Selain mengatur tindak pidana siber materil, UU ITE mengatur tindak pidana siber formil, khususnya dalam bidang penyidikan. Pasal 42 UU ITE mengatur bahwa penyidikan terhadap tindak pidana dalam UU ITE dilakukan berdasarkan ketentuan dalam KUHAP (UU No 8 Tahun 1981) dan ketentuan dalam UU ITE. Artinya, ketentuan penyidikan dalam

[147] Josua Sitompul, "Landasan Hukum Penanganan Cybercrime di Indonesia", https://www.hukumonline.com/klinik/a/landasan-hukum-penanganan-icybercrime-i-di-indonesia-cl5960/ (12/10/2018).

KUHAP tetap berlaku sepanjang tidak diatur lain dalam UU ITE. Kekhususan UU ITE dalam penyidikan antara lain: 1) Penyidik yang menangani tindak pidana siber ialah dari instansi Kepolisian Negara RI atau Pejabat Pegawai Negeri Sipil ("PPNS") Kementerian Komunikasi dan Informatika. 2) Penyidikan dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data. 3) Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan sesuai dengan ketentuan hukum acara pidana; 4) Dalam melakukan penggeledahan dan/atau penyitaan sistem elektronik, penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.[148]

Ketentuan penyidikan dalam UU ITE dan perubahannya berlaku pula terhadap penyidikan tindak pidana siber dalam arti luas. Sebagai contoh, dalam tindak pidana perpajakan, sebelum dilakukan penggeledahan atau penyitaan terhadap server bank, penyidik harus memperhatikan kelancaran layanan publik, dan menjaga terpeliharanya kepentingan pelayanan umum sebagaimana diatur dalam UU ITE dan perubahannya. Apabila dengan mematikan server bank akan mengganggu pelayanan publik, tindakan tersebut tidak boleh dilakukan.[149]

[148] Pasal 43 ayat (1), ayat (2), ayat (3), ayat (4), dan ayat (5) UU ITE.
[149] Josua Sitompul, *Op.cit*.

2. Undang-Undang Tindak Pidana Pencucian Uang

Pencucian Uang dalam Undang-Undang Nomor 8 Tahun 2010 (UU TPPU) adalah segala perbuatan yang memenuhi unsur-unsur tindak pidana sesuai dengan ketentuan dalam Undang-Undang ini.[150] Secara materil, perbuatan yang disebut TPPU adalah; menempatkan, mentransfer, mengalihkan, membelanjakan, membayarkan, menghibahkan, menitipkan, membawa ke luar negeri, mengubah bentuk, menukarkan dengan mata uang atau surat berharga atau perbuatan lain atas Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1)[151] dengan tujuan menyembunyikan atau menyamarkan asal usul Harta Kekayaan.[152]

Pencucian uang atau *money laundering* secara sederhana diartikan sebagai suatu suatu proses menjadikan hasil kejahatan (*proceed of crimes*) atau disebut sebagai uang kotor (*dirty money*) misalnya hasil dari obat bius, korupsi, penggelapan pajak, judi,

[150] Pasal 1 angka 1 UU TPPU.

[151] Pasal 2 ayat (1): Hasil tindak pidana adalah Harta Kekayaan yang diperoleh dari tindak pidana: a. korupsi; b. penyuapan; c. narkotika; d. psikotropika; e. penyelundupan tenaga kerja; f. penyelundupan migran; g. di bidang perbankan; h. di bidang pasar modal; i. di bidang perasuransian; j. kepabeanan; k. cukai; l. perdagangan orang; m. perdagangan senjata gelap; n. terorisme; o. penculikan; p. pencurian; q. penggelapan; r. penipuan; s. pemalsuan uang; t. perjudian; u. prostitusi; v. di bidang perpajakan; w. di bidang kehutanan; x. di bidang lingkungan hidup; y. di bidang kelautan dan perikanan; atau z. tindak pidana lain yang diancam dengan pidana penjara 4 (empat) tahun atau lebih,

[152] Pasal 3 UU TPPU.

penyelundupan dan lain-lain yang dikonversi atau diubah ke dalam bentuk yang tampak sah agar dapat digunakan dengan aman.[153]

Dalam laporan kajian berjudul “Penilaian Risiko Sektoral Tindak Pidana Pencucian Uang Dan Tindak Pidana Pendanaan Terorisme Pada Tindak Pidana Siber”,[154] PPATK memetakan Penilaian Resiko Sektoral atau “*Sectoral Risk Assessment* (SRA)” dari Tindak Pidana Pendanaan Terrorisme (TPPS) pada Tindak Pidana Siber (TPS), beberapa pemetaan tersebut menghaslkan temuan diantaranya, berdasarkan jenis TP Siber, penipuan dalam jaringan (*online fraud*) dan perjudian online (*online gambling*) dinilai berisiko tinggi TPPU. Hasil TP Siber cenderung dilakukan pencucian uang oleh pelaku TP Siber sendiri. Berdasarkan tipologi TPPU, yang dinilai berisiko tinggi adalah penggunaan mata uang virtual dan perjudian online. Berdasarkan pola transaksi, yang dinilai berisiko tinggi adalah transfer dan tarik/setor tunai.[155]

UU TPPU mengakui bukti elektronik dalam Pasal 73, bahwa alat bukti yang sah dalam pembuktian tindak pidana pencucian uang ialah: a. alat bukti sebagaimana dimaksud dalam Hukum Acara Pidana; dan/atau b. alat bukti lain berupa informasi yang diucapkan,

[153]Yenti Garnasih, 2017, *Penegakan Hukum Anti Pencucian Uang dan Permasalahannya di Indonesia*, Edisi 1, Cetakan 4, Rajawali Pers, Depok, hlm. 15

[154] “Penilaian Risiko Sektoral Tindak Pidana Pencucian Uang Dan Tindak Pidana Pendanaan Terorisme Pada Tindak Pidana Siber”, Pusat Pelaporan dan Analisis Transaksi Keuangan, Jakarta, 2025.

[155] PPAT,*ibid*, hlm vi-vii

dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau alat yang serupa optik dan Dokumen.

3. Undang-Undang Tindak Pidana Korupsi

Dalam konteks penegakan hukum di Indonesia, tindak pidana korupsi sering kali melibatkan modus operandi yang canggih, termasuk penggunaan teknologi informasi. Oleh karena itu, alat bukti elektronik menjadi relevan dan penting dalam membuktikan perkara korupsi. Dalam perkara korupsi, alat bukti elektronik sering kali digunakan untuk melacak aliran dana, mengidentifikasi komunikasi, atau mengungkap pola kejahatan. Misalnya, rekaman percakapan elektronik atau transaksi perbankan dapat menjadi bukti kuat yang mendukung dakwaan terhadap terdakwa.

Dalam UU Tipikor, bukti elektronik diatur dalam Pasal 26A sebagai perluasan alat bukti petunjuk, bahwa alat bukti yang sah dalam bentuk petunjuk sebagaimana dimaksud dalam Pasal 188 ayat (2) Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana, khusus untuk tindak pidana korupsi juga dapat diperoleh dari: a. alat bukti lain yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan b. dokumen, yakni setiap rekaman data atau informasi yang dapat dilihat, dibaca, dan atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, maupun

yang terekam secara elektronik, yang berupa tulisan, suara, gambar, peta, rancangan, foto, huruf, tanda, angka, atau perforasi yang memiliki makna.

Dalam penjelasan umum UU Tipikor, diterangkan bahwa ketentuan perluasan mengenai sumber perolehan alat bukti yang sah yang berupa petunjuk, dirumuskan bahwa mengenai "petunjuk" selain diperoleh dari keterangan saksi, surat, dan keterangan terdakwa, juga diperoleh dari alat bukti lain yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu tetapi tidak terbatas pada data penghubung elektronik (*electronic data interchange*), surat elektronik (*e-mail*), telegram, teleks, dan faksimili, dan dari dokumen, yakni setiap rekaman data atau informasi yang dapat dilihat, dibaca dan atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, maupun yang terekam secara elektronik, yang berupa tulisan, suara, gambar, peta, rancangan, foto, huruf, tanda, angka, atau perforasi yang memiliki makna.

4. Undang-Undang Pemberantasan Tindak Pidana Terrorisme

Terorisme dalam Undang-Undang Nomor 15 Tahun 2003 (UU Terorisme)[156] adalah perbuatan yang menggunakan kekerasan atau

[156] Sebagaimana telah diubah dengan Undang-Undang Nomor 5 Tahun 2018 Tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 Tentang Penetapan

ancaman kekerasan yang menimbulkan suasana teror atau rasa takut secara meluas, yang dapat menimbulkan korban yang bersifat massal, dan/atau menimbulkan kerusakan atau kehancuran terhadap objek vital yang strategis, lingkungan hidup, fasilitas publik, atau fasilitas internasional dengan motif ideologi, politik, atau gangguan keamanan.[157] Tindak pidana terorisme sendiri didefinisikan sebagai segala perbuatan yang memenuhi unsur-unsur tindak pidana sesuai dengan ketentuan dalam Undang-Undang ini.[158] Pada konteks modernitas dan kemajuan internet, narasi menjadi komoditas pengaruh yang substansial dan cukup kuat. Dalam perspektif kejahatan terorisme, di satu sisi, internet dan media sosial cukup efektif sebagai propaganda narasi oleh pelaku terorisme.[159]

Mengenai lingkup pemanfaatan internet untuk tujuan terorisme, Conway membuat suatu klasifikasi perbandingan mengenai bentuk pemanfaatan internet untuk tujuan terorisme, yang berasal dari pendapat ahli, diantaranya;[160] menurut Furnell dan Warren, yaitu: propaganda dan publikasi; pendanaan; penyebaran informasi; dan komunikasi yang aman. Menurut Cohen, yaitu: perencanaan; pendanaan; operasi dan koordinasi ; aksi politik; dan propaganda.

Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang

[157] Pasal 1 angka 2 UU Terorisme

[158] Pasal 1 angka 1 UU Terorisme

[159] Topan Yuniarto, “Relasi Internet, Media Sosial, dan Narasi Terorisme”, Kompas.id (27/04/2022) pukul 03:00 WIB.

[160] Golose, Petrus Reinhard, (2015). *Invasi Terorisme Ke Cyberspace*. Jakarta: Yayasan Pengembangan Kajian Ilmu Kepolisian, hlm. 23

Menurut Thomas, yaitu: pembuatan profil; propaganda; anonymous atau komunikasi rahasia; menciptakan suasana rasa takut melalui cyberspace; pendanaan; komando dan pengendalian; perekrutan dan pengerahan anggota; pengumpulan informasi; meminimalisasi resiko; pencurian atau manipulasi data; dan serangan dengan menggunakan informasi yang tidak benar (*misinformation*).[161]

Mengingat UU Terorisme merupakan undang-undang khusus (*lex specialis*) dimana secara khusus juga mengukur tentang alat bukti sebagaimana diatur dalam Pasal 27, alat bukti pemeriksaan tindak pidana terorisme meliputi: 1. Alat bukti sebagaiamana dimaksud dalam Hukum Acara Pidana; 2. Alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima atau disimpan secara elektronik dengan alat optik atau yang sesuai dengan itu; 3. Data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik ataupun selain kertas, atau yang terrekam secara elektronik, termasuk tetapi tidak terbatas pada: a. Tulisan, suara, atau gambar; b. Peta, rancangan,foto, atau sejenisnya; c. Huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya. Berdasarkan Pasal 27 tersebut, pengaturan mengenai alat bukti pemeriksaan perkara pidana

[161] Weldi Rozika, (2017), *Propaganda dan Penyebaran Ideologi Terorisme Melalui Media Internet (Studi Kasus Pelaku Cyber Terorisme oleh Bahrun Naim)*, Jurnal Ilmu Kepolisian, edisi 089, Agustus-Oktober 2017.

terorisme lebih luas daripada alat bukti sebagaimana diatur dalam Pasal 184 ayat (1) KUHAP, perluasan alat bukti dalam Pasal 27 ini dapat diperhatikan bunyi ketentuan dalam Pasal 27 huruf b dan huruf c yang menyebutkan alat bukti elektronik.

5. Undang-Undang Transfer Dana

Dalam Undang-Undang Nomor 3 Tahun 2011 Tentang Transfer Dana (UU Transfer Dana), Transfer Dana adalah rangkaian kegiatan yang dimulai dengan perintah dari Pengirim Asal yang bertujuan memindahkan sejumlah Dana kepada Penerima yang disebutkan dalam Perintah Transfer Dana sampai dengan diterimanya Dana oleh Penerima.[162]Transfer dana yang dahulu hanya dapat dilakukan secara konvensional dengan mengantri di bank dan prosesnya masih *paper based* sekarang sudah dapat dilakukan secara instan melalui sistem elektronik yang telah dikembangkan sedemikian rupa guna mengakomodir pelayanan nasabah secara jarak jauh. Pengoperasiannya yang didasari oleh jejaring elektronik memudahkan oknum untuk dapat mengakses data nasabah dengan tujuan diubah maupun dimanipulasikan seolah olah data yang otentik untuk meraup keuntungan bagi dirinya sendiri.[163]

UU Transfer Dana mengakui kedudukan bukti elektronik dalam Pasal 76 (1), bahwa Informasi elektronik, dokumen elektronik,

[162] Pasal 1 angka 1 UU Transfer Dana

[163] Qanita Fakhira dkk, 2024, *Analisis Penerapan Pasal 81 Undang-Undang Transfer Dana pada Putusan Nomor 78/Pid.Sus/2022/PN YYK Berdasarkan Asas Lex Specialis Sistematis*, Demokrasi: Jurnal Riset Ilmu Hukum, Sosial dan Politik Vol. 1, No.4.

dan/atau hasil cetaknya dalam kegiatan Transfer Dana merupakan alat bukti hukum yang sah. (2) Informasi elektronik, dokumen elektronik, dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku. Pasal 77 Tanda tangan elektronik dalam kegiatan Transfer Dana memiliki kekuatan hukum yang sah.

6. Undang-Undang Narkotika

Dalam Undang-Undang Nomor 35 Tahun 2009 Tentang Narkotika (UU Narkotika), Narkotika adalah zat atau obat yang berasal dari tanaman atau bukan tanaman, baik sintetis maupun semisintetis, yang dapat menyebabkan penurunan atau perubahan kesadaran, hilangnya rasa, mengurangi sampai menghilangkan rasa nyeri, dan dapat menimbulkan ketergantungan, yang dibedakan ke dalam golongan-golongan sebagaimana terlampir dalam Undang-Undang ini.[164]

Pada saat yang sama, perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam modus operandi tindak pidana narkotika. Kejahatan narkoba kini semakin canggih dengan memanfaatkan platform digital dan media sosial untuk transaksi ilegal.[165] Fenomena ini menimbulkan tantangan baru bagi penegak

[164] Pasal 1 angka 1 UU Narkotika

[165] Muh. Akbar Fhad Syahril, *Hukum Informasi dan Transaksi Elektronik*. Eureka Media Aksara, 2023.

hukum dalam upaya pemberantasan peredaran gelap narkotika. Pada tahun 2023, tercatat lebih dari 60% transaksi narkoba dilakukan melalui platform digital, meningkat tajam dari 35% pada tahun 2020.[166] Hal ini mengindikasikan pergeseran pola peredaran narkoba dari metode konvensional ke metode berbasis teknologi. Pada Maret 2024, BNN mengungkap jaringan narkoba internasional yang memanfaatkan aplikasi pesan terenkripsi untuk koordinasi pengiriman sabu-sabu seberat 100 kg dari Malaysia ke Indonesia. Kasus ini menunjukkan bahwa sindikat narkoba telah mengadopsi teknologi canggih untuk menghindari deteksi aparat.[167]

Kedudukan alat bukti elektronik dalam UU Narkotika diatur dalam Pasal 86, bahwa Penyidik dapat memperoleh alat bukti selain sebagaimana dimaksud dalam Undang-Undang tentang Hukum Acara Pidana.[168] Alat bukti sebagaimana dimaksud pada ayat (1) berupa: a. informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan b. data rekaman atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana baik yang tertuang di atas kertas, benda fisik apa pun selain kertas maupun yang terekam secara elektronik, termasuk tetapi tidak terbatas pada: 1. tulisan, suara, dan/atau

[166] Muh.Natsir dkk, (2024), *Urgensi Reformasi UU Narkotika dan UU ITE Menghadapi Ancaman Narkoba di Era Digital*, Jurnal Litigasi AMSIR, Vol. 11. No. 4.
[167] *Ibid* hlm 2.
[168] Pasal 86 ayat (1)

gambar; 2. peta, rancangan, foto atau sejenisnya; atau 3. huruf, tanda, angka, simbol, sandi, atau perforasi yang memiliki makna dapat dipahami oleh orang yang mampu membaca atau memahaminya.[169]

Salah satu cara mendapatkan alat bukti elektronik dalam tindak pidana narkotika adalah melalui penyadapan.[170] Penjelasan Pasal 75 huruf I UU Narkotika menerangkan bahwa yang dimaksud dengan "penyadapan" adalah kegiatan atau serangkaian kegiatan penyelidikan dan/atau penyidikan yang dilakukan oleh penyidik BNN atau Penyidik Kepolisian Negara Republik Indonesia dengan cara menggunakan alat-alat elektronik sesuai dengan kemajuan teknologi terhadap pembicaraan dan/atau pengiriman pesan melalui telepon atau alat komunikasi elektronik lainnya.

7. Undang-Undang Tindak Pidana Perdagangan Orang

Dalam Undang-Undang Nomor 21 Tahun 2007 Tentang Pemberantasan Tindak Pidana Perdagangan Orang (UU TPPO), Perdagangan Orang adalah tindakan perekrutan, pengangkutan, penampungan, pengiriman, pemindahan, atau penerimaan seseorang dengan ancaman kekerasan, penggunaan kekerasan, penculikan, penyekapan, pemalsuan, penipuan, penyalahgunaan

[169] Pasal 86 ayat (2)

[170] Pasal 1 angka 19 UU Narkotika: Penyadapan adalah kegiatan atau serangkaian kegiatan penyelidikan atau penyidikan dengan cara menyadap pembicaraan, pesan, informasi, dan/atau jaringan komunikasi yang dilakukan melalui telepon dan/atau alat komunikasi elektronik lainnya.

kekuasaan atau posisi rentan, penjeratan utang atau memberi bayaran atau manfaat, sehingga memperoleh persetujuan dari orang yang memegang kendali atas orang lain tersebut, baik yang dilakukan di dalam negara maupun antar negara, untuk tujuan eksploitasi atau mengakibatkan orang tereksploitasi.[171]

Dalam era digital yang semakin maju, media elektronik, terutama media sosial, telah menjadi sarana yang digunakan oleh para pelaku kejahatan untuk mengeksploitasi masyarakat dan memfasilitasi praktik perdagangan manusia. Media sosial memungkinkan pelaku kejahatan untuk dengan cepat dan secara anonim mencapai potensi korban di berbagai negara. Mereka dapat mengumpulkan data pribadi tentang calon korban, memantau aktivitas mereka, dan menargetkan mereka dengan efisiensi yang tinggi. Selain itu, media sosial memfasilitasi perdagangan manusia untuk tujuan eksploitasi seksual dan pekerjaan paksa dengan memungkinkan penyebaran konten merugikan, seperti gambar dan video pornografi anak-anak. Dengan demikian, media sosial telah secara signifikan memperluas lingkup dan intensitas praktik perdagangan manusia lintas negara.[172]

Kedudukan alat bukti elektronik dalam UU TPPO terdapat dalam Pasal 29, bahwa alat bukti selain sebagaimana ditentukan dalam Undang-Undang Hukum Acara Pidana, dapat pula berupa: a.

[171] Pasal 1 angka 1 UU TPPO.

[172] Andi Aina Ilmih, 2024, *Penggunaan Media Elektronik Dalam Perdagangan Manusia Lintas Negara*, ALADALAH : Jurnal Politik, Sosial, Hukum dan Humaniora Volume. 2 No. 4 Oktober, hlm 2.

informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan b. data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apa pun selain kertas, atau yang terekam secara elektronik, termasuk tidak terbatas pada: 1) tulisan, suara, atau gambar; 2) peta, rancangan, foto, atau sejenisnya; atau 3) huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.

Penjelasan pasal tersebut menerangkan bahwa yang dimaksud dengan “data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apa pun selain kertas, atau yang terekam secara elektronik” dalam ketentuan ini misalnya: data yang tersimpan di komputer, telepon, atau peralatan elektronik lainnya, atau catatan lainnya seperti: a. catatan rekening bank, catatan usaha, catatan keuangan, catatan kredit atau utang, atau catatan transaksi yang terkait dengan seseorang atau korporasi yang diduga terlibat di dalam perkara tindak pidana perdagangan orang; b. catatan pergerakan, perjalanan, atau komunikasi oleh seseorang atau organisasi yang diduga terlibat di dalam tindak pidana menurut Undang-Undang ini; atau c.

dokumen, pernyataan tersumpah atau bukti-bukti lainnya yang didapat dari negara asing, yang mana Indonesia memiliki kerja sama dengan pihak-pihak berwenang negara tersebut sesuai dengan ketentuan dalam undang-undang yang berkaitan dengan bantuan hukum timbal balik dalam masalah pidana.

8. Undang-Undang Perlindungan Data Pribadi

Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (UU PDP), Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.[173]. Perlindungan Data Pribadi adalah keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional subjek Data Pribadi.[174]

Kejadian pelanggaran privasi yang melibatkan bocornya informasi pribadi sering terjadi di Indonesia.[175] Dalam sektor perbankan, informasi pribadi dapat terungkap dalam berbagai kegiatan seperti pertukaran data pribadi antara lembaga keuangan, penyaluran informasi kepada pihak ketiga terkait transaksi keuangan, atau melalui penyedia jasa pihak ketiga yang mengelola data transaksi. Di

[173] Pasal 1 angka 1 UU Perlindungan Data Pribadi.
[174] Pasal 1 angka 2.
[175] Disemadi, H. S., (2021). *Legal Aspects Of 'Gali Lubang Tutup Lubang'in Fintech P2p Lending Business During Covid-19*. Tadulako Law Review, 6(2), 237–256.

bidang medis, data pasien sering kali tersedia untuk tujuan asuransi atau program dukungan pemerintah tanpa persetujuan langsung dari pasien dan kadang-kadang dapat disalahgunakan untuk kepentingan yang tidak sah. Pada platform jual beli online, informasi pribadi seperti preferensi belanja dan riwayat transaksi sering kali diambil secara tidak sah menggunakan cookies yang dapat membahayakan privasi konsumen dan digunakan untuk kepentingan yang tidak diinginkan. Dalam platform transportasi online, penggunaan nomor telepon konsumen dapat disalahgunakan untuk tujuan yang tidak terkait dengan layanan, seperti mengirim pesan tidak relevan atau mengancam konsumen atas ulasan negatif.[176]

Pada tanggal 12 Mei 2021, Indonesia mengalami kasus serius terkait kebocoran informasi atau data pribadi yang melibatkan sekitar 279 juta data warga. Informasi yang tersedia mencakup detail seperti nama lengkap sesuai Kartu Tanda Penduduk (KTP), nomor telepon, alamat email, Nomor Identitas (NIK), lokasi tinggal, serta perkiraan pendapatan. Lebih dari 20 juta data juga dilengkapi dengan foto pribadi penduduk. Akun Kotz menawarkan sampel data gratis kepada pengguna dengan menyediakan 1 juta sampel dan memperkenalkan 3 tautan yang membutuhkan kata sandi untuk mengaksesnya. Kasus

[176] Yuniarti, S. (2019). *Perlindungan hukum data pribadi di Indonesia*. Business Economic, Communication, and Social Sciences Journal (BECOSS), 1(1), 147–154.

ini menimbulkan keprihatinan serius terhadap privasi data dan keamanan informasi pribadi masyarakat.[177]

Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (UU PDP), alat bukti elektronik diatur dalam Pasal 64 ayat (3) bahwa alat bukti yang sah dalam Undang-Undang ini meliputi: a. alat bukti sebagaimana dimaksud dalam hukum acara; dan b. alat bukti lain berupa informasi elektronik dan/atau dokumen elektronik sesuai dengan ketentuan peraturan perundang-undangan.

H. Kerangka Teori

1. Teori Pembuktian

Secara *gramatikal* pembuktian berasal dari kata dasar "bukti" yang berarti sesuatu yang menyatakan kebenaran suatu peristiwa, sedangkan membuktikan yakni memperlihatkan bukti atau meyakinkan dengan bukti sedangkan pembuktian merupakan proses, cara perbuatan membuktikan atau usaha menunjukkan benar atau salahnya si terdakwa dalam sidang pengadilan.[178]

Sedangkan dari perspektif yuridis, pembuktian itu sendiri menurut M. Yahya Harahap adalah ketentuan-ketentuan yang berisi penggarisan dan pedoman tentang cara-cara yang dibenarkan

[177] Luthiya, A. N., Irawan, B., & Yulia, R, (2021), *Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi*. Jurnal Hukum Pidana Dan Kriminologi, 2(2), 14–29.

[178].Kamus Besar Bahasa Indonesia, dari Departemen Pendidikan Nasional, Edisi Ketiga, Balai Pustaka, Jakarta, 2007, hal.172 s/d 173.

undang-undang membuktikan kesalahan yang didakwakan kepada Terdakwa. Pembuktian juga merupakan ketentuan yang mengatur alat-alat bukti yang dibenarkan oleh undang-undang yang boleh dipergunakan Hakim membuktikan kesalahan yang didakwakan. Persidangan pengadilan tidak boleh sesuka hati dan semena-mena membuktikan kesalahan Terdakwa.[179]

Selain itu, Munir Fuady memberikan pandangannya bahwa pembuktian dalam ilmu hukum adalah suatu proses, baik dalam acara perdata, acara pidana, maupun acara-acara lainnya, dimana dengan menggunakan alat-alat bukti yang sah, dilakukan tindakan dengan prosedur khusus, untuk mengetahui apakah suatu fakta atau pernyataan, khususnya fakta atau pernyataan yang dipersengketakan di Pengadilan, yang diajukan dan dinyatakan oleh salah satu pihak dalam proses pengadilan itu benar atau tidak seperti yang dinyatakan itu.[180] Sementara Suharto mengatakan bahwa pembuktian di muka sidang pengadilan adalah suatu usaha Penuntut Umum dalam mengajukan alat-alat bukti yang sah menurut undang-undang di muka sidang Pengadilan untuk membuktikan kesalahan Terdakwa.[181]

---

[179]. M. Yahya Harahap, *Pembahasan Permasalahan dan Penerapan KUHAP, Pemeriksaan Sidang Pengadilan, Banding, Kasasi dan Peninjauan Kembali,* Edisi Kedua, Sinar Grafika, Jakarta, 1985, hal. 273.

[180].Munir Fuady, *Teori Pembuktian (Pidana dan Perdata)*, Citra Aditya Bakti, Bandung, 2006, hal. 1 s/d 2.

[181].Suharto RM, *Penuntutan Dalam Praktek Peradilan*, Sinar Grafika, Jakarta, 1997, hal.135 s/d 136.

Pada hakekatnya pembuktian dimulai sejak adanya suatu peristiwa hukum.[182] Menurut Adami Chazawi, pada dasarnya seluruh kegiatan dalam proses hukum penyelesaian perkara pidana, sejak penyelidikan sampai putusan akhir diucapkan di muka persidangan oleh majelis hakim adalah berupa kegiatan yang berhubungan dengan pembuktian atau kegiatan untuk membuktikan.[183] Ilmu pengetahuan hukum mengenal 4 (empat) sistem pembuktian, yaitu:

1. Pembuktian Berdasarkan Keyakinan Hakim Belaka (*Conviction in Time*). Menurut sistem ini, hakim dapat menyatakan telah terbukti kesalahan terdakwa melakukan tindak pidana yang didakwakan dengan berdasarkan keyakinannya saja, dan tidak perlu mempertimbangkan dari mana (alat bukti) dia memperoleh dan alasan-alasan yang dipergunakan serta bagaimana caranya dalam membentuk keyakinannya tersebut. Juga tidak perlu mempertimbangkan apakah logis ataukah tidak logis. Bekerjanya sistem ini benar-benar bergantung kepada hati nurani hakim. Sehingga pembuktian ini sangatlah subyektif, seseorang bisa dinyatakan bersalah tanpa bukti apa-apa yang mendukungnya, sebaliknya pembuktian sistem ini bisa membebaskan seseorang dari

[182] Pandoe Pramoe Kartika, (2019), *Data Elektronik Sebagai Alat Bukti Yang Sah Dalam Pembuktian Tindak Pidana Pencucian Uang*, Indonesia Journal of Criminal Law (IJoCL), Vol.1.No.1. : https://doi.org/10.31960/ijocl.v1i1.146.

[183] A. Chazawi, A, 2008, *Hukum Pembuktian Tindak Pidana Korupsi*, PT Alumni, Bandung, hlm 13.

perbuatan yang dilakukannya.[184] Wirjono Prodjodikoro mengatakanbahwa system pembuktian ini pernah dianut di Indonesia, yaitu pada pengadilan distrik dan kabupaten, Sistem ini memungkinkan hakim menyebur apa saja yang menjadi dasar keyakinannya, misalkan keterangan dukun.[185]

2. Sistem Pembuktian Berdasarkan Undang-Undang Secara Positif (*Positief Wettelijk Bewijstheorie*). Dikatakan secara positif, karena hanya didasarkan kepada undang-undang, yang artinya jika telah terbukti suatu perbuatan sesuai dengan alat-alat bukti yang disebut oleh undang-undang, maka keyakinan hakim tidak diperlukan sama sekali. Sistem ini disebut juga teori pembuktian formal (*formele bewijstheorie*).[186] Menurut D. Simons, sistem atau teori pembuktian berdasar undang-undang secara positif (*positief wettelijk*) ini berusaha untuk menyingkirkan semua pertimbangan subjektif hakim dan mengikat hakim secara ketat menurut peraturan- peraturan pembuktian yang keras.[187] Teori pembuktian ini sekarang tidak mendapat penganut lagi. Teori ini terlalu banyak

[184] Irman. S.Tb. (2006), *Hukum Pembuktian Pencucian Uang*, MQS Publishing, Jakarta, hlm 136.

[185] Makarao, Mohammad Taufik, dan Suhasril, 2010, *Hukum Acara Pidana Dalam Teori dan Praktek*, Ghalia Indonesia, Bogor, 2010.

[186] A. Hamzah, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta, 2010, hlm 251.

[187] *Ibid*.

mengandalkan kekuatan pembuktian yang disebut oleh undang-undang.[188]

3. Sistem Pembuktian Berdasarkan Keyakian Hakim Dengan Alasan Yang Logis (*La Conviction Raisonee*). Menurut sistem pembuktian ini, hakim dapat menghukum seseorang terdakwa apabila ia telah meyakini bahwa perbuatan yang berssangkutan terbukti kebenarannya dengan keyakinan tersebut harus disertai dengan alasan-alasan yang berdasarkan atas suatu rangkaian pemikiran (logika), hakim wajib menguraikan dan menjelaskan alasan-alasan yang menjadi dasar keyakinannya atas kesalahan terdakwa. Sistem atau teori pembuktian ini disebut juga pembuktian bebas karena hakim bebas menyebut alasan-alasan keyakinannya (*vrije bewijstheorie*).[189]
4. Sistem Pembuktian Berdasarkan Undang-Undang Secara Negatif (*Negatief Wettelijk*). Sistem pembuktian ini merupakan gabungan antara sistem pembuktian menurut undang-undang secara positif dengan sistem pembuktian berdasarkan keyakinan hakim semata. Hasil penggabungan ini dapat dirumuskan “salah tidaknya seseorang terdakwa ditentukan oleh hakim yang didasarkan kepada cara dan dengan alat-alat bukti yang sah menurut undang-undang.” “sistem pembuktian

[188] *Ibid* hlm 250.
[189] *Ibid*.

menurut undangundang secara negative ini merupakan suatu keseimbangan antara sistem yang saling bertolak belakang secara ekstrim.[190] Dalam sistem atau teori pembuktian yang berdasarkan undang-undang secara negatif ini, pemidanaan didasarkan kepada pembuktian yang berganda, yaitu pada peraturan perundangundangan dan pada keyakinan hakim, dan menurut undang-undang, dasar keyakinan hakim ini bersumber pada peraturan undang-undang.[191]

Teori hukum pembuktian tersebut tentunya akan terkait dengan pihak-pihak yang akan dibebani untuk membuktikan menyangkut tindak pidana yang telah di dakwakan oleh Penuntut Umum di Persidangan. A. Djoko Sumaryanto menyebutkan dikaji dari perspektif ilmu pengetahuan hukum pidana dikenal ada 3 (tiga) tentang beban pembuktian. secara universal ketiga teori tentang beban pembuktian tersebut hakikatnya terdapat di negara Indonesia, maupun di beberapa Negara seperti Malaysia, Inggris, Hongkong, maupun di Singapura, yaitu ; (a) beban pembuktian pada penuntut umum, (b) beban pembuktian pada terdakwa dan (c) beban pembuktian berimbang. [192]

---

[190] M. Yahya Harahap, *Pembahasan Permasalahan dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali*, Sinar Grafika, Jakarta, 2012, hlm 278.

[191] Hamzah, *Op.cit*., hlm 250.

[192].A. Djoko Sumaryanto, *Pembalikan beban Pembuktian Tindak Pidana Korupsi Dalam rangka Pengembalian Kerugian Keuangan Negara*, Jakarta: Prestasi Pustaka Raya, Jakarta, 2009, hal. 89 s/d 90.

Selain itu, ada juga yang dinamakan “pembuktian terbalik” atau “pembalikan beban pembuktian”. Dari sisi bahasa dikenal sebagai “*Omkering van het Bewijslast”* atau *“Reversal Burden of Proof”* yang bila secara bebas diterjemahkan menjadi “Pembalikan Beban Pembuktian”.[193] Sebaliknya jika ia tidak bisa membuktikan asal usul harta/objek sita itu, maka ia bisa dikenakan pemberatan dalam tuntutan dan dalam vonis. Karena telah melakukan kebohongan dihadapan sidang yang dimuliakan. Sidang adalah sebuah proses yang sakral dimana setiap pihak didengar kesaksiannya dalam sumpah.

Pada dasarnya, dalam sistem hukum pidana formil di Indonesia, beban untuk membuktikan ada atau tidaknya pidana terletak pada Jaksa Penuntut Umum, bukan pada terdakwa. Ketentuan Pasal 66 KUHAPidana bahwa tersangka atau terdakwa tidak dibebani kewajiban pembuktian. Dalam penjelasan Pasal 66 KUHAP, dikatakan bahwa ketentuan ini adalah penjelmaan asas “praduga tak bersalah”. M. Yahya Harahap, dalam bukunya berjudul “Pembahasan Permasalahan dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali”,[194] menyatakan bahwa ditinjau dari segi hukum acara pidana, penuntut umum bertindak sebagai aparat yang diberi wewenang untuk

[193] Akil Mochtar, *Pembalikan Beban Pembuktian Tindak Pidana Korupsi*. Sekretariat Jenderal dan Kepaniteraan Mahkamah Konstitusi, Jakarta, 2009, hal 129.

[194] M. Yahya Harahap, *op.cit.,* hal 274.

mengajukan segala daya upaya membuktikan kesalahan yang didakwakan kepada terdakwa.

a. Barang Bukti

Kitab Undang-undang Hukum Acara Pidana memang tidak menyebutkan secara jelas tentang apa yang dimaksud dengan barang bukti. Namun dalam Pasal 39 ayat (1) KUHAP disebutkan mengenai apa-apa saja yang dapat disita, yaitu:[195]

a. benda atau tagihan tersangka atau terdakwa yang seluruh atau sebagian diduga diperoleh dari tindakan pidana atau sebagai hasil dari tindak pidana;
b. benda yang telah dipergunakan secara langsung untuk melakukan tindak pidana atau untuk mempersiapkannya;
c. benda yang digunakan untuk menghalang-halangi penyelidikan tindak pidana;
d. benda yang khusus dibuat atau diperuntukkan melakukan tindak pidana;
e. benda lain yang mempunyai hubungan langsung dengan tindak pidana yang dilakukan.

Dalam *Hertzienne inLandsch Reglement* (HIR) terdapat perihal barang bukti. Dalam Pasal 42 HIR disebutkan bahwa para pegawai, pejabat atau pun orang-orang berwenang diharuskan mencari kejahatan dan pelanggaran kemudian selanjutnya

[195] Ratna Nurul Afiah, *Barang Bukti dalam Proses Pidana*, Sinar Grafika, Jakarta, 1988.

mencari dan merampas barang-barang yang dipakai untuk melakukan suatu kejahatan serta barang-barang yang didapatkan dari sebuah kejahatan. Penjelasan Pasal 42 HIR menyebutkan barang-barang yang perlu di-*beslag* di antaranya:

1. Barang-barang yang menjadi sasaran tindak pidana (*corpora delicti*);
2. Barang-barang yang terjadi sebagai hasil dari tindak pidana (*corpora delicti*);
3. Barang-barang yang dipergunakan untuk melakukan tindak pidana (*instrumental delicti*);
4. Barang-barang yang pada umumnya dapat dipergunakan untuk memberatkan atau meringankan kesalahan terdakwa (*corpora delicti*).

Selain dari pengertian-pengertian yang disebutkan oleh kitab undang-undang di atas, pengertian mengenai barang bukti juga dikemukakan dengan doktrin oleh beberapa Sarjana Hukum. Andi Hamzah mengatakan, barang bukti dalam perkara pidana adalah barang bukti mengenai mana delik tersebut dilakukan (objek delik) dan barang dengan mana delik dilakukan (alat yang dipakai untuk melakukan delik), termasuk juga barang yang merupakan

hasil dari suatu delik.[196] Ciri-ciri benda yang dapat menjadi barang bukti:

1. Merupakan objek materiil.
2. Berbicara untuk diri sendiri.
3. Sarana pembuktian yang paling bernilai dibandingkan sarana pembuktian lainnya.
4. Harus diidentifikasi dengan keterangan saksi dan keterangan terdakwa.

Menurut Martiman Prodjohamidjojo, barang bukti atau *corpus delicti* adalah barang bukti kejahatan. Dalam Pasal 181 KUHAP majelis hakim wajib memperlihatkan kepada terdakwa segala barang bukti dan menanyakan kepadanya apakah ia mengenali barang bukti tersebut. Jika dianggap perlu, hakim sidang memperlihatkan barang bukti tersebut.[197] Ansori Hasibuan berpendapat barang bukti ialah barang yang digunakan oleh terdakwa untuk melakukan suatu delik atau sebagai hasil suatu delik, disita oleh penyidik untuk digunakan sebagai barang bukti pengadilan.[198]

Dari pendapat beberapa Sarjana Hukum di atas dapat disimpulkan bahwa yang disebut dengan barang bukti adalah:

---

[196] Andi Hamzah, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta, 2017, hal. 254.

[197] Martiman Prodjohamidjojo, *Memahami Dasar-Dasar Hukum Pidana Indonesia*, PT. Pradnya Paramita, Jakarta, 1997.

[198] Ansori Hasibuan, dan Ruben Ahmad, *Hukum Acara Pidana*, Angkasa, Bandung, 1990.

1. Barang yang dipergunakan untuk melakukan tindak pidana.
2. Barang yang dipergunakan untuk membantu melakukan suatu tindak pidana.
3. Benda yang menjadi tujuan dari dilakukannya suatu tindak pidana.
4. Benda yang dihasilkan dari suatu tindak pidana.
5. Benda tersebut dapat memberikan suatu keterangan bagi penyelidikan tindak pidana tersebut, baik berupa gambar ataupun berupa rekaman suara.
6. Barang bukti yang merupakan penunjang alat bukti mempunyai kedudukan yang sangat penting dalam suatu perkara pidana. Tetapi kehadiran suatu barang bukti tidak mutlak dalam suatu perkara pidana, karena ada beberapa tindak pidana yang dalam proses pembuktiannya tidak memerlukan barang bukti, seperti tindak pidana penghinaan secara lisan (Pasal 310 ayat [1] KUHP).[199]

Jadi, dapat disimpulkan bahwa fungsi barang bukti dalam sidang pengadilan adalah sebagai berikut:

1. Menguatkan kedudukan alat bukti yang sah (Pasal 184 ayat [1] KUHAP);

[199] Ratna Nurul Afiah, *op.cit.*

2. Mencari dan menemukan kebenaran materiil atas perkara sidang yang ditangani;
3. Setelah barang bukti menjadi penunjang alat bukti yang sah maka barang bukti tersebut dapat menguatkan keyakinan hakim atas kesalahan yang didakwakan JPU

b. Alat Bukti

Alat Bukti adalah segala sesuatu yang ada hubungannya dengan suatu perbuatan, dimana dengan alat - alat bukti tersebut, dapat dipergunakan sebagai bahan pembuktian guna menimbulkan keyakinan hakim atas kebenaran adanya suatu tindak pidana yang telah dilakukan oleh terdakwa.

Pasal 184 ayat (1) Kitab Undang-Undang Hukum Acara Pidana disebutkan bahwa alat bukti yang sah adalah: keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa. Dalam sistem pembuktian hukum acara pidana yang menganut *stelsel negatief wettelijk*, hanya alat-alat bukti yang sah menurut undang-undang yang dapat dipergunakan untuk pembuktian.[200] Hal ini berarti bahwa di luar dari ketentuan tersebut tidak dapat dipergunakan sebagai alat bukti yang sah.

Pengajuan alat bukti yang sah menurut undang-undang di dalam persidangan dilakukan oleh: a). Penuntut umum dengan tujuan untuk membuktikan dakwaan nya; b). Terdakwa atau

[200] Martiman Prodjoharmijo, *Sistem Pembuktian dan Alat-Alat Bukti (seri pemerataan keadilan 10)*, Ghalia Indonesia, Jakarta, 1983, hal 19.

penasehat hukum , jika ada alat bukti yang bersifat meringankan , atau membebaskan terdakwa dari segala tuntutan hukum. Pada dasarnya yang mengajukan alat bukti dalam persidangan adalah penuntut umum (alat bukti yang memberatkan/*acharge*). Terdakwa tidak dibebani kewajiban pembuktian. Hal ini merupakan jelmaan asas praduga tak bersalah (Pasal 66 KUHAP). Jadi pada prinsipnya yang membuktikan kesalahan terdakwa adalah penuntut umum.[201]

c. Bukti Elektronik Sebagai Perluasan Alat Bukti KUHAP

Sebelum berlakunya UU ITE, para ahli hukum berbeda pandangan soal keberadaan dan kekuatan bukti elektronik (*digital evidence*): apakah dianggap sebagai alat bukti atau barang bukti. Esensinya, alat bukti adalah segala sesuatu yang digunakan dalam rangka pembuktian. Keberadaannya menimbulkan keyakinan hakim atas suatu tindak pidana yang dituduhkan terhadap terdakwa. Di sisi lain, barang bukti bertujuan untuk mendukung pembuktian dan menerangkan suatu kejadian.[202]

Sejak UU ITE berlaku, informasi elektronik, dokumen elektronik, dan/atau hasil cetaknya (bukti elektronik) dianggap sebagai perluasan dari alat bukti yang sah dalam hukum acara pidana. Hal ini sebagaimana dimaksud dalam Pasal 5 ayat (1)

[201] Alfitra, *Hukum Pembuktian Dalam Beracara Pidana , Perdata, dan Korupsi di Indonesia* , edisi revisi, Penebar Swadaya Group, Jakarta, 2011, hal 21-25

[202] Eddy, O.S Hiariej, *Teori dan Hukum Pembuktian*, Erlangga: Jakarta, 2012.

dan (2) UU ITE. Alat bukti elektronik termasuk sebagai alat bukti selain yang diatur terbatas dalam Pasal 184 ayat (1) KUHAP serta undang-undang pidana khusus lainnya.[203] Ketentuan secara khusus mengenai alat bukti yang sah dan perluasan dari Pasal 184 KUHAP termuat dalam Pasal 5 ayat (1) dan ayat (2), serta Pasal 44 huruf b UU ITE. Pengaturan secara khusus tersebut seharusnya diberlakukan kepada kejahatan-kejahatan yang menggunakan sarana elektronik karena norma serta rumusan pidananya terpisah dari KUHAP.[204]

Pandangan bukti elektronik hanya dianggap sebagai barang bukti atau alat bukti surat atau petunjuk dalam hal terdapat kesesuaian fakta dan peristiwa pidana atas dasar alasan berikut. Pertama, tindak pidana yang didakwakan hanya merujuk pada hukum acara pidana dalam KUHAP. Tindak pidana yang dimaksud sebagian besar diatur dalam KUHP - seperti pembunuhan, penganiayaan, pencurian, dan sebagainya - atau di luar KUHP yang tidak secara khusus mengatur pembuktian atau alat bukti selain penjelasan KUHAP. Kedua, bukti elektronik hanya dianggap alat bukti karena dinyatakan secara tegas dalam UU ITE serta undang-undang lain yang mengaturnya secara khusus sebagai alat bukti. Pasal 44 UU ITE termasuk dalam

[203] UU Khusus yang dimaksud seperti: Pasal 26A Undang-Undang tentang Pemberantasan Tindak Pidana Korupsi (UU Tipikor), Pasal 86 ayat (2) Undang-Undang tentang Narkotika (UU Narkotika), Pasal 29 Undang-Undang tentang Pemberantasan Tindak Pidana Perdagangan Orang (UU TPPO), dan undang-undang lainnya.

[204] Putusan Nomor: 20/PUU-XIV/2016, hlm 48.

bagian penyidikan dalam tindak pidana informasi dan transaksi elektronik. Harus dimaknai bahwa alat bukti dalam penyidikan, penuntutan, hingga pemeriksaan di sidang pengadilan dalam tindak pidana ITE meliputi alat bukti dalam KUHAP serta bukti elektronik.[205]

Dalam UU ITE, alat bukti mengalami perluasan, yang mana alat bukti tersebut selain yang terdapat dalam Pasal 184 ayat (1) KUHAP, juga termasuk alat bukti elektronik ataupun dokumen elektronik. Menurut UU ITE, Pasal 5 ayat (1) dan ayat (2) juncto Pasal 44 huruf b, alat bukti elektronik, informasi elektronik, atau dokumen elektronik merupakan alat bukti hukum yang sah. Jadi secara substantif UU ITE pada hakikatnya menempatkan dan mengkualifikasi "informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya" sebagai alat bukti yang sah menurut hukum yang berlaku di Indonesia, sehingga dapat dipergunakan untuk membuktikan perbuatan seseorang yang dikategori sebagai tindak pidana.[206]

Dengan diberlakukannya UU ITE, maka secara yuridis terciptalah suatu dasar hukum bagi transaksi-transaksi elektronik

[205] Jefferson Hakim dan Nael Yehezkiel, "Mempertanyakan Bukti Elektronik sebagai Alat Bukti dalam Kasus Pidana", Hukumonline.com (26/6/2024). https://www.hukumonline.com/berita/a/mempertanyakan-bukti-elektronik-sebagai-alat-bukti-dalam-kasus-pidana-lt667b57ba9f459/. Data akses 17 Juli 2024 pukul 23.15 WIT.

[206] Putusan Nomor 20/PUU-XIV/2016, hlm 8.

dan informasi yang terjadi di wilayah hukum Indonesia.[207] Keberadaan bukti elektronik secara materiil memang telah diakui keberadaannya, namun dalam tataran hukum acara (formil) masih belum terakomodir sepenuhnya. Berdasarkan ketentuan Pasal 5 ayat 3 UU ITE bahwa informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan suatu sistem elektronik sesuai dengan ketentuan yang ada di dalam UU ITE. Hal ini sesuai dengan Pasal 6 UU ITE, yang menentukan bahwa dokumen elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan, sehingga menerangkan suatu keadaan. Di samping itu, kedudukan dokumen elektronik dapat disetarakan dengan dokumen yang dibuat di atas kertas.[208]

Perluasan alat bukti sebagaimana dimaksud dalam ketentuan Pasal 5 ayat (2) UU ITE, dimaksudkan oleh pembentuk undang-undang sebagai upaya preventif dan represif bagi perbuatan hukum baru dalam tindak pidana *cyber*. Selain itu, perluasan alat bukti dalam ketentuan *a quo* juga dapat dipergunakan Aparat Penegak Hukum (APH) dalam menindak pelaku tindak pidana

[207] Moh. Nafri, *Dokumen Elektronik Sebagai Alat Bukti Dalam Hukum Acara Perdata di Indonesia*, Maleo Law Journal, vol. 3, No. 1 (2019), hlm. 42.
[208] Penjelasan umum UU No 11 Tahun 2008 tentang ITE pasal 6

dan/atau pelaku perbuatan melawan hukum lainnya yang memanfaatkan teknologi informasi dalam sistem elektronik.[209]

d. Prinsip Pendekatan Kesetaraan Fungsional Informasi/Dokumen Elektronik

Dalam pemahaman kekuatan pembuktian yang paling lemah, suatu informasi elektronik adalah bernilai secara hukum karena secara fungsional keberadaannya adalah sepadan atau setara dengan suatu informasi yang tertulis diatas kertas, sebagaimana telah diamanahkan dalam UNCITRAL[210] tentang nilai hukum dari suatu rekaman elektronik (*legal value of electronic records*) karena memenuhi unsur-unsur tertulis (*writing*), bertandatangan (*signed*), dan asli (*original*). Menindaklanjuti hal tersebut dengan keberlakuan UU ITE, suatu informasi elektronik di Indonesia juga telah diterima sebagai alat bukti sebagaimana telah diakomodir dalam Pasal 5 UU ITE, sehingga kehadirannya tidak dapat ditolak hanya karena bentuknya yang elektronik.[211]

Berbeda dengan ketentuan dalam UNCITRAL yang memasangkan satu per satu kesetaraan fungsional antara informasi tertulis dengan informasi elektronik terlebih dahulu (melalui kejelasan syarat pemenuhan unsur tertulis, bertandatangan, dan asli), sementara Pasal 5 dan Pasal 6 UU

---

209 Putusan Nomor 20/PUU-XIV/2016, hlm 56.
210 https://uncitral.un.org/
211 Edmon Makarim, *Loc.cit*., hlm 29-30.

ITE lebih merangkumkan semua unsur tersebut secara kumulatif, sehingga akan lebih fleksibel dalam penerapannya. Mencermati rumusan tersebut, jelas ditentukan bahwa suatu informasi elektronik (IE) dan/atau dokumen elektronik (DE) telah diakui keberadaannya sebagai alat bukti hukum yang sah baik dalam bentuk originalnya yang elektronik maupun hasil cetaknya. Namun timbul pertanyaan berikutnya, yaitu bahwa apakah ia hanya sekedar alat bukti yang merupakan perluasan dari yang telah ada ataukah ia berdiri sendiri diluar kategorisasi alat bukti yang berdasarkan hukum acara yang telah berlaku, baik yang dikenal dalam hukum acara perdata maupun pidana.[212]

Beberapa ahli hukum berbeda pendapat dalam memandang Pasal 5 UU ITE, kebanyakan ahli hukum positivistic akan menyatakan bahwa UU ITE secara jelas menyatakan IE/DE hanyalah merupakan perluasan alat bukti saja sebagaimana dinyatakan pada ayat (2), padahal IE/DE selayaknya juga menjadi alat bukti tersendiri sebagai konsekuensi dari perumusan pada ayat (1) yang mengakui IE/DE dalam bentuk originalnya yang elektronik, dan perumusan pada ayat (3) yang menyatakan bahwa keberadaannya baru dianggap sah jika memenuhi ketentuan yang diatur dalam UU ITE.

[212] *Ibid* hlm 31.

Berdasarkan sejarah dan perdebatannya, sesungguhnya perumusan Pasal 5 yang seperti itu merupakan hasil perumusan jalan tengah dari perbedaan perumusan yang ada pada beberapa UU yang lain, dimana pada satu UU tertentu hanya dinyatakan sebagai perluasan alat bukti petunjuk saja (contoh UU TPK), namun pada UU lainnya dinyatakan sebagai alat bukti lain diluar kategorisasi alat bukti dalam hukum acara pidana dan acara perdata yang berlaku (contoh UU TPPU). Kedua perumusan yang berbeda dari beberapa UU lain tersebut adalah refleksi adanya perbedaan pemikiran terhadap eksistensi informasi elektronik itu sendiri. Hal tersebut tidak perlu terjadi karena keduanya memang ada nilai kebenarannya, yakni; 1) IE/DE dalam konteks tertentu memang dapat hadir dan memenuhi kriteria sebagai satu alat bukti yang telah dikenal dalam hukum acara yang berlaku sehingga keberadaannya merupakan perluasan dari alat bukti yang telah ada (contoh: petunjuk), dan; 2) IE/DE dapat berdiri sendiri jika memenuhi ketentuan UU yang berlaku (contoh: sistem telah diaudit dan terakreditasi sehingga mampu menjamin keautentikannya). Keduanya tergantung pada karakteristik teknis yang melekat pada informasi elektronik itu sendiri dan tergantung kepada cara bagaimana para pihak ingin menghadirkannya di muka persidangan.[213]

[213] *Ibid* hlm 32.

Secara teknis berdasarkan muatannya, suatu IE/DE dapat dikategorikan menjadi dua, yakni; 1) suatu informasi elektronik yang secara lahiriah hanya memperlihatkan suatu fakta peristiwa hukum saja sehingga dengan sendirinya ia hanya dapat berfungsi sebagai petunjuk semata karena validitasnya harus dirangkaikan pertemuannya dengan informasi yang lain (contoh: foto yang hanya merekam suatu keadaan secara diam); dan 2) suatu informasi elektronik yang secara lahiriah tidak hanya memperlihatkan suatu fakta peristiwa hukum saja, melainkan juga dapat menjelaskan dan merujuk kepada suatu subjek hukum yang bertanggung jawab daripadanya (contoh: rekaman video penarikan uang tunai berikut orangnya pada Anjungan Tunai Mandiri/ATM).[214]

2. Teori Tujuan Hukum

Sudikno Mertokusumo menjelaskan bahwa kepastian hukum merupakan sebuah jaminan bahwa, hukum tersebut harus dijalankan dengan cara yang baik. Kepastian hukum menghendaki adanya upaya pengaturan hukum dalam perundang-undangan yang dibuat oleh pihak yang berwenang dan berwibawa, sehingga aturan-aturan itu memiliki aspek yuridis yang dapat menjamin adanya kepastian

214

bahwa, hukum berfungsi sebagai suatu peraturan yang harus ditaati.[215]

Kepastian adalah perihal (keadaan) yang pasti, ketentuan atau ketetapan. Hukum secara hakiki harus pasti dan adil. Pasti sebagai pedoman kelakukan dan adil karena pedoman kelakuan itu harus menunjang suatu tatanan yang di nilai wajar. Hanya karena bersifat adil dan dilaksanakan dengan pasti hukum dapat menjalankan fungsinya. Kepastian hukum merupakan pertanyaan yang hanya bisa dijawab secara normatif, bukan sosiologi.[216]

Kepastian hukum secara normatif adalah ketika suatu peraturan dibuat dan diundangkan secara pasti karena mengatur secara jelas dan logis. Jelas dalam artian tidak menimbulkan keragu-raguan (multi tafsir) dan logis. Jelas dalam artian ia menjadi suatu sistem norma dengan norma lain sehingga tidak berbenturan atau menimbulkan konflik norma. Kepastian hukum menunjuk kepada pemberlakuan hukum yang jelas, tetap, konsisten dan konsekuen yang pelaksanaannya tidak dapat dipengaruhi oleh keadaan-keadaan yang sifatnya subjektif. Kepastian dan keadilan bukanlah sekedar tuntutan moral, melainkan secara faktual mencirikan hukum. Suatu

[215] Asikin Zainal, *Pengantar Tata Hukum Indonesia*, Rajawali Press: Jakarta, 2012.

[216] Dominikus Rato, *Filsafat Hukum Mencari: Memahami dan Memahami Hukum*, Laksbang Pressindo: Yogyakarta, 2010, hlm 59.

hukum yang tidak pasti dan tidak mau adil bukan sekedar hukum yang buruk.[217]

Menurut Utrecht, kepastian hukum mengandung dua pengertian, yaitu pertama, adanya aturan yang bersifat umum membuat individu mengetahui perbuatan apa yang boleh atau tidak boleh dilakukan, dan kedua, berupa keamanan hukum bagi individu dari kesewenangan pemerintah karena dengan adanya aturan yang bersifat umum itu individu dapat mengetahui apa saja yang boleh dibebankan atau dilakukan oleh Negara terhadap individu.[218]

Kepastian hukum diartikan sebagai kejelasan norma sehingga dapat dijadikan pedoman bagi masyarakat yang dikenakan peraturan ini.[219] Pengertian kepastian tersebut dapat dimaknai bahwa, ada kejelasan dan ketegasan terhadap berlakunya hukum di dalam masyarakat. Hal ini agar tidak menimbulkan banyak salah tafsir. Menurut Van Apeldoorn, "kepastian hukum dapat juga berarti hal yang dapat ditentukan oleh hukum dalam hal-hal yang konkret".[220] Kepastian hukum adalah jaminan bahwa, hukum dijalankan, oleh, yang berhak menurut hukum dapat memperoleh haknya dan bahwa, putusan dapat dilaksanakan. Kepastian hukum merupakan

---

[217] Cst Kansil, Christine, S.T Kansil, Engelien R, Palandeng dan Godlieb N Mamahit, *Kamus Istilah Hukum*, Jala Permata Aksara: Jakarta, 2009, hlm. 385.

[218] Riduan Syahrani, *Rangkuman Intisari Ilmu Hukum*, PT Citra Aditya Bakti: Bandung, 1999, hlm.23.

[219] Tata Wijayanta, (2014). *Asas Kepastian Hukum, Keadilan dan Kemanfaatan Dalam Kaitannya Dengan Putusan Kepailitan Pengadilan Niaga"*, Fakultas Hukum Universitas Gadjah Mada Yogyakarta, Jurnal Dinamika Hukum Vol. 14 No. 2, hlm.219

[220] Van Apeldoorn, *Pengantar Ilmu Hukum*, Cet XXIV, terj, Pradnya Paramita: Jakarta, 1990, hlm 24-25.

perlindungan *yustisiabel* terhadap tindakan sewenang-wenang yang berarti bahwa, seseorang akan dapat memperoleh sesuatu yang diharapkan dalam keadaan tertentu.[221]

3. TeorI Sistem Hukum

Lawrence M. Friedman mengemukakan bahwa sistem hukum terdiri dari tiga sub bagian, yaitu : (1) Struktur Hukum; (2) Substansi Hukum; dan (3) Kultur hukum yang disebut sebagai "*Three Elements of Legal Systems*".[222] Struktur Hukum mencakupi berbagai kelembagaan yang berfungsi menjalankan dan menegakkan ketentuan hukum materiil. Dalam pengertian ini adalah aparat penegak hukum itu sendiri; kepolisian, kejaksaan, hakim, advokat/pengacara, lembaga pemasyarakatan. Mereka ini sebagai sistem struktural yang menentukan bisa atau tidaknya hukum itu dilaksanakan dengan baik.

Substansi hukum adalah setiap peraturan hukum yang berlaku dan memiliki kekuatan mengikat bagi setiap subyek hukum yang ada. Substansi hukum dalam hal ini adalah UU ITE dan KUHAP. Substansi juga mencakup hukum yang hidup (*living law*), bukan

---

[221] R. Tony Prayogo, {2016). *Penerapan Asas Kepastian Hukum Dalam Peraturan Mahkamah Agung Nomor 1 Tahun 2011 Tentang Hak Uji Materiil dan Dalam Peraturan Mahkamah Konstitusi Nomor 06/pmk/2005 Tentang Pedoman Beracara Dalam Pengujian Undang-Undang,* Jurnal Legislasi Indonesia, Vol. 13 No. 02, hlm 194.

[222] Lawrence M. Friedman, *Teori dan Filsafat hukum: Telaah kritis atasi Teori-Teori Hukum* (susunan I), judul asli "Legal Theory", penerjemah: Mohammad Arifin, Cetakan kedua, (Jakarta,PT Raja Grafindo Persada 1993), hlm 31. Lihat juga Lawrence M. Friedman, 2009, *System Hukum Dalam Perspektif Ilmu Sosial* (*The Legal System: A Social Science Perspective*), (Bandung: Nusa Media, 2009), hlm 16. Diterjemahkan dalam buku Lawrence M. Friedman, "The Legal System: A Social Science Perspective", (New York: Russell Sage Foundation, 1999).

hanya aturan yang ada dalam kitab undang-undang (*law books*). Sebagai negara yang masih menganut sistem *Civil Law System* atau sistem Eropa Kontinental (meski sebagian peraturan perundang-undangan juga telah menganut *Common Law System* atau *Anglo Saxon* dikatakan hukum adalah peraturan-peraturan yang tertulis sedangkan peraturan-peraturan yang tidak tertulis bukan dinyatakan hukum. Sistem ini mempengaruhi sistem hukum di Indonesia. Salah satu pengaruhnya adalah adanya asas Legalitas dalam KUHP. Dalam Pasal 1 KUHP disebutkan *"*tidak ada suatu perbuatan pidana yang dapat dihukum jika tidak ada aturan yang mengaturnya*"*. Sehingga bisa atau tidaknya suatu perbuatan dikenakan sanksi hukum apabila perbuatan tersebut telah mendapatkan pengaturannya dalam peraturan perundang-undangan.

Sedangkan kultur hukum mencakupi suatu proses pelaksanaan hukum yang menggambarkan tingkah laku hukum (*legal behavior*) dalam praktek yang terjadi.[223] Dalam kaitan dengan budaya hukum ini, Friedman selanjutnya mengartikannya sebagai suasana pikiran sosial dan kekuatan sosial yang menentukan bagaimana hukum digunakan, dihindari atau disalahgunakan. Tanpa budaya hukum, sistem itu sendiri tidak akan berdaya [224]

[223] Juajir Sumardi, *Aspek-Aspek Hukum Franchise dan Perusahaan Transnasional)*, (Bandung: Citra Aditya Bakti, 1995), hlm 23, mengutip Lawrence M Friedman, ibid.

[224] Lawrence M Friedman, op.cit, hlm 8.

Menurut Friedman budaya hukum diterjemahkan sebagai sikap-sikap dan nilai-nilai yang berhubungan dengan hukum dan lembaganya, baik secara positif, maupun negatif. Jika masyarakat mempunyai nilai nilai yang positif, maka hukum akan diterima dengan baik, sebaliknya jika negatif, masyarakat akan menentang dan menjauhi hukum dan bahkan menganggap hukum tidak ada. Membentuk undang-undang memang merupakan budaya hukum, tetapi mengandalkan undang-undang untuk membangun budaya hukum yang berkarakter tunduk, patuh dan terikat pada norma hukum adalah jalan pikiran yang setengah sesat. Budaya hukum bukanlah hukum. Budaya hukum secara konseptual adalah soal-soal yang ada di luar hukum.[225] bahkan Friedman menempatkan budaya hukum sebagai sebagai sumber hukum,[226] nilai yang terkandung dalam ide, opini, dan perilaku masyarakat sejatinya akan membentuk norma hukum, dan norma itulah yang akan menentukan perubahan dalam masyarakat, termasuk kepatuhan sekaligus pembentukan hukum.

Friedman mengibaratkan struktur hukum seperti mesin. Substansi adalah apa yang dihasilkan atau dikerjakan oleh mesin itu. Budaya hukum adalah apa saja atau siapa saja yang memutuskan untuk

[225] Mardjono Reksodiputro, *Sistem Peradilan Pidana Indonesia, Melihat Kejahatan dan Penegakan Hukum dalam Batas-Batas Tolerans, loc.cit*, hlm 81.

[226] Jo. Carrillo, "Links And Choices: Popular Legal Culture In The Work Of Lawrence M. Friedman," Southern California Interdisciplinary Law Journal 17 (2007): 1–22. Disadur dari Izzy Al Kautsar, Danang Wahyu Muhammad, (2022), "Sistem Hukum Modern Lawrence M. Friedman: Budaya Hukum dan Perubahan Sosial Masyarakat Dari Industri Ke Digital", Jurnal Sapientia et Virtus | Volume 7 Nomor 2, 2022, hal 89.

menghidupkan dan mematikan mesin itu serta memutuskan bagaimana mesin itu digunakan. Sedangkan Achmad Ali, membagi sistem hukum itu menjadi 5 sub sistem hukum yaitu: struktur, substansi, kultur hukum, profesionalisme dan komitmen.[227]

Achmad Ali menambahkan bahwa struktur mencakup berbagai kelembagaan yang berfungsi menjalankan dan menegakkan ketentuan hukum materil; Substansi adalah setiap peraturan hukum yang berlaku dan memiliki kekuatan mengingat bagi setiap subjek hukum yang ada. Kultur hukum mencakup suatu proses pelaksanaan hukum yang menggambarkan tingkah laku hukum (*legal behavior*) dalam praktik yang terjadi. Profesionalisme, yaitu pemahaman wawasan hukum yang mendalam tentang kemahiran teknis, maupun pemahaman dan kemampuan menganalisis situasi konkret yang harus ditangani oleh setiap penegak hukum dalam mengembang kewenangannya di bidang penegakan hukum, baik sebagai polisi, advokat, jaksa, hakim dan lainnya. Komitmen adalah tekad yang optimal untuk benar-benar melaksanakan tugas profesional yang diamanatkan kepada setiap penegak hukum, untuk tidak sekadar menegakkan hukum, tetapi juga di dalam penegakan hukum senantiasa mewujudkan keadilan, baik keadilan prosedural maupun keadilan substansial.[228]

---

[227] Achmad Ali, 2009. *Menguak Teori Hukum (Legal Theory) dan Teori Peradilan (Judicial Prudence),* Kencana Prenada Media Group, Jakarta.

[228] Achmad Ali, *"Sumbangan Pemikiran tentang Upaya Pembangunan Hukum di Indonesia"*. Makalah pada seminar Revitalisasi Nilai-Nilai Kejuangan Membangun

Soerjono Soekanto menyatakan bahwa efektif atau tidaknya suatu penegakan hukum ditentukan oleh 5 (lima) faktor, yaitu:[229]

1. Faktor undang-undang. Undang-undang dalam arti material adalah peraturan tertulis yang berlaku umum dan dibuat oleh Penguasa Pusat maupun Daerah yang sah. Mengenai berlakunya Undang-undang tersebut, terdapat beberapa asas yang tujuannya adalah agar Undang-undang tersebut mempunyai dampak yang positif. Asas-asas tersebut antara lain:
    1) Undang-undang tidak berlaku surut.
    2) Undang-undang yang dibuat oleh penguasa yang lebih tinggi, mempunyai kedudukan yang lebih tinggi pula.
    3) Undang-undang yang bersifat khusus menyampingkan Undang-undang
    4) yang bersifat umum, apabila pembuatnya sama.
    5) Undang-undang yang berlaku belakangan, membatalkan Undang-undang yang berlaku terdahulu.
    6) Undang-undang tidak dapat diganggu gugat.
    7) Undang-undang merupakan suatu sarana untuk mencapai kesejahteraan spiritual dan material bagi masyarakat maupun pribadi, melalui pelestarian ataupun pembaharuan

Indonesia yang Maju, Sejahtera dan Berkarakter, (Bandung pada tanggal 21 Juni 2008), h. 2.

[229] Soerjono Soekanto, *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum*, (Jakarta, Raja Grafindo Persada, 2008), hlm 23.

(inovasi).

2. Faktor Penegak Hukum. Penegak hukum merupakan golongan panutan dalam masyarakat, yang hendaknya mempunyai kemampuan-kemampuan tertentu sesuai dengan aspirasi masyarakat. Mereka harus dapat berkomunikasi dan mendapat pengertian dari golongan sasaran, di samping mampu menjalankan atau membawakan peranan yang dapat diterima oleh mereka. Ada tiga faktor elemen penting yang mempengaruhi kinerja aparat penegak hukum dalam menjalankan tugas-tugasnya, yaitu:
   1) Institusi penegak hukum beserta berbagai perangkat sarana dan prasarana pendukung dan mekanisme kerja kelembagaannya;
   2) Budaya kerja yang terkait dengan aparatnya, termasuk mengenai kesejahteraan aparatnya, dan
   3) Perangkat peraturan yang mendukung baik kinerja kelembagaannya maupun yang mengatur materi hukum yang dijadikan standar kerja, baik hukum materilnya maupun hukum acaranya.
3. Faktor Sarana dan Fasilitas. Tanpa adanya sarana atau fasilitas tertentu, maka tidak mungkin penegakan hukum akan berjalan dengan lancar. Sarana atau fasilitas tersebut antara lain, mencakup tenaga manusia yang berpendidikan dan terampil,

organisasi yang baik, peralatan yang memadai, keuangan yang cukup, dan seterusnya. Sarana atau fasilitas mempunyai peran yang sangat penting dalam penegakan hukum. Tanpa adanya sarana atau fasilitas tersebut, tidak akan mungkin penegak hukum menyerasikan peranan yang seharusnya dengan peranan yang aktual.

4. Faktor Masyarakat. Penegakan hukum berasal dari masyarakat, dan bertujuan untuk mencapai kedamaian dalam masyarakat. Oleh karena itu, dipandang dari sisi tertentu, maka masyarakat dapat mempengaruhi penegakan hukum tersebut. Masyarakat Indonesia mempunyai kecenderungan yang besar untuk mengartikan hukum dan bahkan mengidentifikasikannya dengan petugas (dalam hal ini penegak hukum sebagai pribadi). Salah satu akibatnya adalah, bahwa baik buruknya hukum senantiasa dikaitkan dengan pola perilaku penegak hukum.
5. Faktor Kebudayaan. Kebudayaan/sistem hukum pada dasarnya mencakup nilai-nilai yang mendasari hukum yang berlaku, nilai-nilai yang merupakan konsepsi abstrak mengenai apa yang dianggap baik sehingga dianut dan apa yang dianggap buruk sehingga dihindari. Pasangan nilai yang berperan dalam hukum, adalah:

   1) Nilai ketertiban dan nilai ketentraman.

2) Nilai jasmani/kebendaan dan nilai rohani/keakhlakan.

3) Nilai kelanggengan atau konservatisme dan nilai kebaruan/ inovatisme.

4. Teori *Locus Delicti*

Penegakan hukum TPE tidak mudah dalam menentukan "*locus delicti*" pada *cybercrime* sangat penting karena berpengaruh pada kompetensi relatif dalam penerapan hukum acara pidana, selain itu kita ketahui juga bahwa kejahatan *cybercrime* ini tidak terbatas oleh ruang dan waktu, mengenai hal tersebut juga menjadi masalah besar dalam proses penegakan hukum pada tindak pidana *cybercrime* ini. *Locus delicti* adalah tempat terjadinya peristiwa pidana, berasal dari kosakata Latin "locus" yang artinya "tempat" atau "lokasi" dan "delicti" yang artinya "delik" atau "tindak pidana". Mengenai pengertian *locus delicti*, ada beberapa pendapat dari ahli mengenai *locus delicti* itu sendiri. Menurut Van Hattum, pemerintah berpendapat bahwa yang harus dipandang sebagai *locus delicti* itu adalah seorang pelaku telah melakukan kejahatannya, dan bukan tempat kejahatan itu telah menimbulkan akibat. Sedangkan menurut Van Bemmelen berpendapat bahwa yang harus dipandang sebagai *locus delicti* itu pada dasarnya adalah tempat seseorang pelaku telah melakukan perbuatannya secara material.[230]

[230] P. Lamintang, *KUHAP dengan Pembahasan Secara Yuridis Menurut Yurisprudensi dan Ilmu Pengetahuan Hukum Pidana*, Sinar Baru: Bandung, 1984.

Terdapat empat teori dalam menentukan tempat terjadinya peristiwa pidana atau *locus delicti*. Beberapa di antaranya adalah sebagai berikut.[231]

a. Teori perbuatan materiil (*leer van de lichamelijke daad).* Teori ini didasarkan pada perbuatan fisik, sehingga teori ini menjelaskan terkait dianggap sebagai tempat terjadinya tindak pidana adalah tempat di mana perbuatan tersebut dilakukan.
b. Teori alat (*leer van het instrument*). Teori ini didasarkan terhadap fungsinya suatu alat digunakan dalam perbuatan pidana. Teori ini menegaskan bahwa dianggap tempat terjadinya tindak pidana adalah tempat di mana alat digunakan dalam tindak pidana bereaksi.
c. Teori akibat (*leer van het gevolg*). Teori ini menjelaskan mengenai akibat dari suatu tindak pidana. Hal ini menjelaskan bahwa locus delicti adalah tempat di mana akibat dari pada tindak pidana tersebut timbul.
d. Teori beberapa tempat (*leer van de lichamelijke daad*). Teori ini menjelaskan mengenai tempat terjadinya tindak pidana mengenai tempat-tempat perbuatan tersebut secara fisik terjadi, tempat di mana alat digunakan bereaksi, serta tempat adanya akibat dari tindak pidana tersebut timbul.

231

I. Kerangka Pikir Penelitian

Pentingnya kerangka pikir atau kerangka teori karena setiap penelitian haruslah selalu disertai dengan pemikiran-pemikiran teoritis. Hal ini disebabkan karena adanya hubungan timbal balik antara teori dengan kegiatan-kegiatan pengumpulan data, konstruksi data, pengolahan data dan analisis data.[232] Menurut Polancik, kerangka pemikiran adalah suatu diagram yang menjelaskan secara garis besar alur logika berjalannya sebuah penelitian. Kerangka pemikiran dibuat berdasarkan pertanyaan penelitian (*research question*), dan merepresentasikan suatu himpunan dari beberapa konsep serta hubungan diantara konsep-konsep tersebut.[233]

Di dalam penelitian ini, peneliti menetapkan 3 (tiga) variabel penelitiannya berdasarkan 3 (tiga) rumusan masalah, yaitu: 1) urgensi digital forensik; 2) proses pengumpulan bukti melalui digital forensik; dan 3) formulasi ideal. Untuk variabel pertama, menggunakan 2 (dua) indikator; (i) membuat terang peristiwa pidana, dan (ii) mengumpulkan bukti. Untuk variabel kedua, menggunakan 4 (empat) indikator: (i) penindakan TPE oleh Polri; (ii) proses pengumpulan bukti menggunakan digital forensic; (iii) kendala dalam penerapan digital forensic; dan (iv) perbandingan Negara. Untuk variabel ketiga, menggunakan 3 (tiga) indikator; (i) penguatan pembuktian alat bukti elektronik; (ii) penguatan

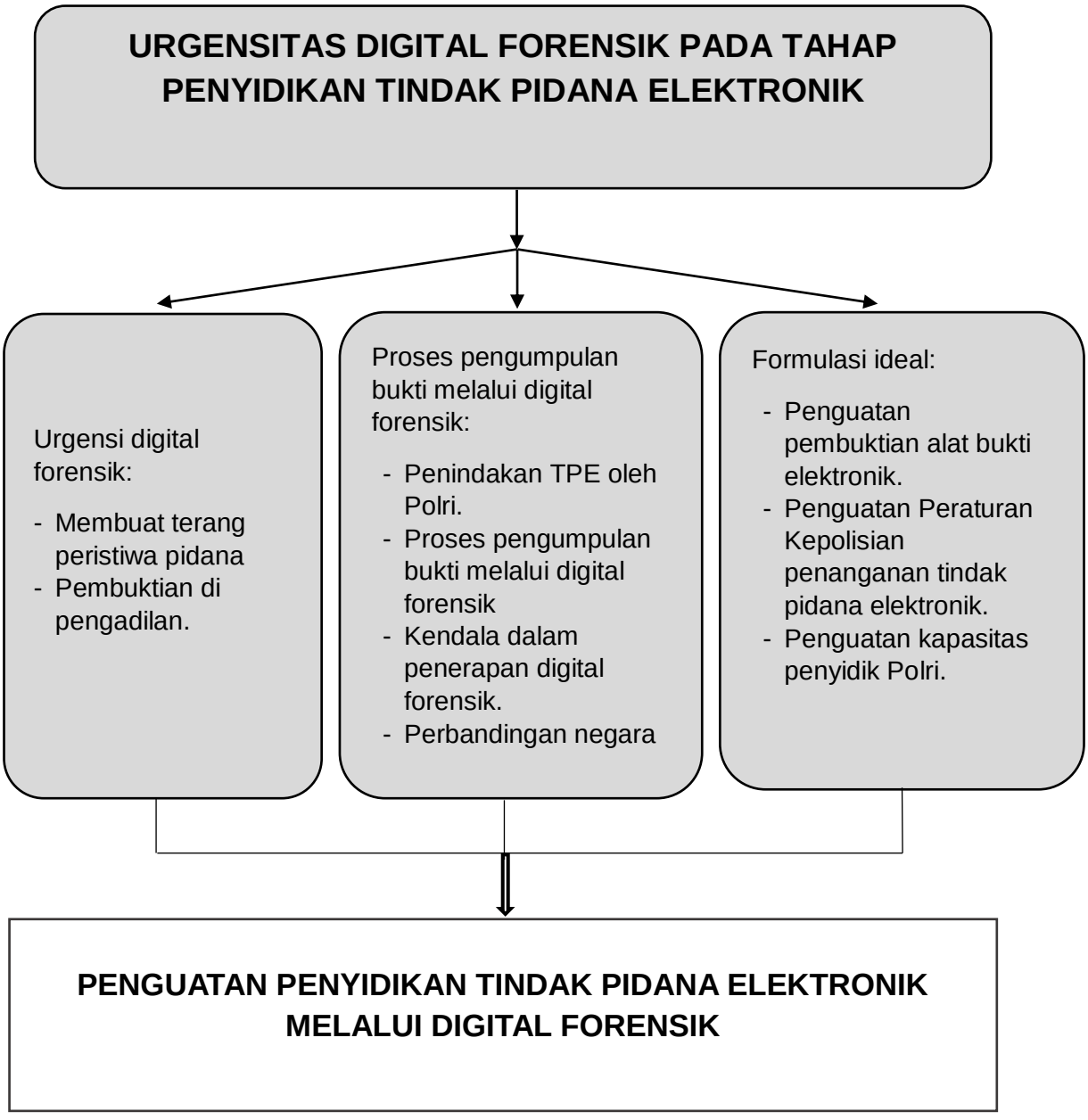
[232] Ronny Hanitijo Soemitro, *Metodologi Penelitian Hukum dan Jurimetri*, Ghalia Indonesia, Jakarta, 1990, hal. 41.

[233] Gregor Polancik, *"Empirical Research Method Poster"*. Jakarta, 2009).

peraturan Kepolisian penanganan tindak pidana elektronik, dan (iii) penguatan kapasitas penyidik Polri.

Untuk lebih jelasnya, variabel dan indikator masalah penelitian dapat digambarkan dalam bagan kerangka pikir berikut:

J. BAGAN KERANGKA PIKIR



K. Definisi Operasional

1. Urgensitas adalah urgensi digital forensik pada tahap penyidikan tindak pidana elektronik.
2. Tindak pidana adalah tindak pidana elektronik.
3. Penyidikan adalah penyidikan tindak pidana elektronik oleh Kepolisian
4. Digital forensik adalah bidang ilmu pengetahuan dan teknologi komputer yang digunakan dalam kepentingan pembuktian hukum (*pro justice*), untuk melakukan pembuktian kejahatan dengan menggunakan teknologi atau komputer secara ilmiah hingga mendapatkan bukti digital yang digunakan untuk menjerat pelaku kejahatan.
5. Membuat terang peristiwa pidana adalah kegiatan pengidentifikasian melalui digital forensik akan membuat terang suatu peristiwa pidana elektronik yang memiliki karakteristik khusus.
6. Pembuktian di pengadilan adalah digital forensik sebagai cara pembuktian bukti elektronik sebagai alat bukti di pengadilan.
7. Proses pengumpulan bukti adalah proses pengumpulan bukti elektronik melalui digital forensik.
8. Penindakan adalah penindakan tindak pidana elektronik oleh POLRI.

9. Proses pengumpulan bukti adalah proses pengumpulan bukti elektronik melalui digital forensic.
10. Hambatan dan kendala adalah hambatan dan kendala dalam penggunaan digital forensik dalam kegiatan penyidikan tindak pidana elektronik di Kepolisian.
11. Perbandingan Negara adalah perbandingan penggunaan digital forensic dalam penyidikan tindak pidana elektronik di beberapa negara.
12. Formulasi ideal adalah gagasan hukum yang ideal penggunaan digital forensik dalam kegiatan penyidikan tindak pidana elektronik.
13. Penguatan pembuktian adalah penguatan pembuktian alat bukti elektronik dalam UU ITE dan tindak pidana dengan predikat *serious crime*.
14. Peraturan Kepolisian penanganan tindak pidana elektronik peraturan yang diterbitkan oleh Kepolisian Republik Indonesia dalam penanganan tindak pidana elektronik yang memiliki tingkat kerumitan dan karakteristik khusus.
15. Penguatan kapasitas penyidik Polri adalah penguatan kapasitas penyidik Polri dalam penanganan tindak pidana elektronik dan digital forensik.