ISSN:3031-3422
Sumenep, 5-6 Desember 2023

MEKANISME PENYIDIKAN DAN PENUNTUTAN TINDAK PIDANA CYBERCRIME: TINJAUAN HUKUM INDONESIA

Siti Hailatul Umami[1], Abshoril Fithry[2*]
[1,2]Universitas Wiraraja, Madura

abshorilfithry@wiraraja.ac.id

ABSTRAK

Perkembangan teknologi informasi dan telekomunikasi dalam era globalisasi menciptakan media internet sebagai jaringan mendunia. Transformasi ini memengaruhi cara bertransaksi, membuka peluang baru, dan mengubah perilaku masyarakat. Meskipun memberikan kemudahan, teknologi informasi juga melahirkan kejahatan siber yang canggih, termasuk di Indonesia. Ancaman ini menciptakan ketidakamanan di masyarakat, mengingat informasi pribadi dan keuangan rentan jatuh ke tangan yang salah. Di tengah dinamika teknologi, penanganan cybercrime perlu merujuk pada semangat UUD 1945 dan nilai-nilai Pancasila. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menjadi upaya hukum untuk mengatasi kekosongan dalam menghadapi kejahatan di dunia maya. Namun, penerapan undang-undang ini menghadapi persepsi yang berbeda, mengancam kepastian hukum. Pembuktian tindak pidana siber menantang karena locus delicti berada di ruang siber. Bagaimana alat bukti dalam Kitab Undang-Undang Hukum Acara Pidana berkaitan dengan Undang-Undang ITE menjadi fokus perdebatan. Kendati Undang-Undang ITE mencoba mengatasi permasalahan tersebut, Keberlanjutan nilai-nilai Pancasila dalam menghadapi dinamika teknologi menjadi pokok perdebatan. Ketiadaan undang-undang yang memadai mengakibatkan pelaku kejahatan sulit diadili. Oleh karena itu, perlu upaya cepat untuk menyusun regulasi yang efektif, menegakkan hukum, dan memberikan perlindungan adekuat di era digital.

Kata kunci : kejahatan dunia maya , globalisasi, nilai-nilai pancasila, locus delicti.

ABSTRACT

The development of information and telecommunications technology in the era of globalization has created internet media as a global network. This transformation influences the way of transactions, opens up new opportunities and changes people's behavior. Even though it provides convenience, information technology has also given rise to sophisticated cyber crimes, including in Indonesia. This threat creates insecurity in society, considering that personal and financial information is vulnerable to falling into the wrong hands. In the midst of technological dynamics, handling cybercrime needs to refer to the spirit of the 1945 Constitution and the values of Pancasila. Law Number 11 of 2008 concerning Information and Electronic Transactions is a legal effort to overcome the gaps in dealing with crime in cyberspace. However, the implementation of this law faces different perceptions, threatening legal certainty. Proving cyber crimes is challenging because the locus of delicti is in cyberspace. How the evidence in the Criminal Procedure Code relates to the ITE Law is the focus of debate. Even though the ITE Law tries to overcome this problem, the sustainability of Pancasila values in the face of technological dynamics is the subject of debate. The absence of adequate laws makes it difficult for criminals to be prosecuted. Therefore, immediate efforts are needed to formulate effective regulations, enforce the law, and provide adequate protection in the digital era.

Keywords : cybercrime, globalization, Pancasila values, locus delicti.

PENDAHULUAN

Saat ini istilah Cyber Law telah digunakan secara internasional untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Hukum siber atau cyber law, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika. Istilah lain yang juga digunakan adalah hukum teknologi informasi (law of information technology), hukum dunia maya (virtual world law), dan hukum mayantara (Ahmad Ramli, 2006). Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global (Internet), memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual. Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.

Sistem elektronik adalah sistem komputer dalam arti luas, yang tidak hanya mencakup perangkat keras dan perangkat lunak komputer, tetapi juga mencakup jaringan telekomunikasi dan/atau sistem komunikasi elektronik. Perangkat lunak atau program komputer adalah sekumpulan instruksi yang diwujudkan dalam bentuk bahasa, kode, skema, ataupun bentuk lain, yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat computer bekerja untuk melakukan fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang instruksi tersebut. Sistem elektronik juga digunakan untuk menjelaskan keberadaan sistem informasi yang merupakan penerapan teknologi informasi yang berbasis jaringan telekomunikasi dan media elektronik, yang berfungsi merancang, memproses, menganalisis, menampilkan, dan mengirimkan atau menyebarkan informasi elektronik. Sistem informasi secara teknis dan manajemen sebenarnya adalah perwujudan penerapan produk teknologi informasi ke dalam suatu bentuk organisasi dan manajemen sesuai dengan karakteristik kebutuhan pada organisasi tersebut dan sesuai dengan tujuan peruntukannya. Pada sisi yang lain, sistem informasi secara teknis dan fungsional adalah keterpaduan sistem antara manusia dan mesin yang mencakup komponen perangkat keras, perangkat lunak, prosedur, sumber daya manusia, dan substansi informasi yang dalam pemanfaatannya mencakup fungsi input, process, output, storage, dan communication

Dalam era digital yang semakin berkembang, Indonesia tidak luput dari ancaman kejahatan cybercrime yang dapat merugikan individu, perusahaan, dan bahkan keamanan nasional. Pentingnya mekanisme penyidikan dan penuntutan dalam menanggulangi tindak pidana ini menjadi fokus utama hukum Indonesia. Menyoroti pergeseran dramatis dalam kehidupan sehari-hari masyarakat Indonesia, yang semakin terhubung dalam ekosistem digital. Di tengah kemajuan teknologi, tindak pidana cybercrime memunculkan tantangan serius terhadap keamanan dan privasi individu. Situasi ini membutuhkan pemahaman mendalam tentang bagaimana sistem hukum dapat merespons secara efektif terhadap ancaman ini.

Secara sosiologis, kita melihat bagaimana masyarakat menghadapi dampak tindak pidana cybercrime dalam kehidupan sehari-hari, menciptakan kekhawatiran dan ketidakamanan. Dari perspektif filosofis, penting untuk menjelajahi relevansi nilai-nilai UUD 45 dalam menanggapi tantangan hukum yang berasal dari dunia digital yang terus berkembang. Secara yuridis, pergeseran paradigma kejahatan digital menuntut pemahaman mendalam tentang bagaimana undang-undang yang ada, terutama KUHAP, dapat beradaptasi untuk efektif menegakkan hukum dalam konteks tindak pidana cybercrime. Pergeseran masyarakat Indonesia ke ranah digital telah membuka pintu bagi kehadiran tindak pidana cybercrime yang semakin beragam dan berbahaya. Sosiologisnya, kita perlu meresapi bagaimana masyarakat bersentuhan dengan ancaman cybercrime, apakah itu dalam kehidupan sehari-hari atau dalam dunia maya yang semakin kompleks. Filosofisnya, perlu dilakukan refleksi mendalam terhadap kesesuaian nilai-nilai UUD 45 dalam membimbing

penegakan hukum terkait cybercrime. Dari segi yuridis, kita akan menyelidiki apakah KUHAP, sebagai kerangka hukum utama, telah mampu menyesuaikan diri dengan dinamika tindak pidana cyber. Apakah diperlukan amendemen atau regulasi tambahan untuk memastikan penyidikan dan penuntutan cybercrime dapat dilakukan secara efektif dan adil.

METODE PENELITIAN

Penelitian ini merupakan suatu penelitian hukum normatif, yaitu penelitian dengan terutama melihat hukum sebagai seperangkat norma (a set of rules), di mana penelitian ini dikenal juga dengan nama penelitian kepustakaan (library research). Pendekatan yang digunakan dalam penelitian ini adalah: statuta approach dan conseptual approach. Teknik analisis yang digunakan adalah penalaran dan argumentasi hukum untuk menjawab isu-isu penelitian yang diajukan sesuai dengan pendekatan yang digunakan.

HASIL DAN PEMBAHASAN

A. Hukum Tindak Pidana Cybercrime

Perkembangan ilmu pengetahuan dan teknologi saat ini tidak hanya mampu memberikan dampak yang positif saja namun perkembangan tersebut ternyata disalahgunakan sebagai sarana kejahatan. Hal tersebut sangat penting untuk di antisipasi bagaimana kebijakan hukumnya, sehingga cyber crime yang terjadi dapat dilakukan upaya penanggulangannya dengan hukum pidana, termasuk dalam hal ini adalah mengenai sistem penegakannya. Indonesia sendiri sudah memiliki aturan hukum cyber crime yang tertuang dalam Undang-Undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik yaitu atas perubahan undang-undang nomor 11 tahun 2008 (Arisandy, 2021).

Mekanisme penyidikan tindak pidana cybercrime diatur dalam UU ITE dan beberapa peraturan pelaksanaannya. Polisi memiliki peran utama dalam penyidikan, mulai dari penerimaan laporan, pengumpulan bukti digital, hingga identifikasi dan penangkapan pelaku. Pasal 30 ayat 1, ayat 2, dan atau ayat 3 UU No 11/2008 tentang Informasi dan Transaksi Elektronik (ITE), berbunyi (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apa pun. (2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik. Dan, (3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

B. Penyidikan dan Penuntutan Perkara Tindak Pidana Cybercrime

Penyidik adalah pejabat polisi negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh undang-undang. Menurut ketentuan Pasal 7 KUHAP wewenang penyidik yaitu (Wulandari, 2021):

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

j. Mengadakan tindakan lain menurut hukum yang bertanggung jawab.

Berdasarkan ketentuan Pasal 15, Peraturan Kepala Kepolisian Negara Republik Indonesia No. 14 Tahun 2012, kegiatan penyidikan dilaksanakan secara bertahap meliputi: penyelidikan; pengiriman SPDP; upaya paksa; pemeriksaan; gelar perkara; penyelesaian berkas perkara; penyerahan berkas perkara ke penuntut umum; penyerahan tersangka dan barang bukti; dan penghentian penyidikan. Secararinci kegiatan tersebut terjabar dalam uraian berikut:

1. PenyelidikanBerdasarkan ketentuan Pasal 1 angka 5 KUHAP, pengertian penyelidikan adalah serangkaian tindakan penyelidik untuk mencari dan menemukan peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyidikan menurut cara yang diatur dalam undang-undang ini. Merujuk pada ketentuan Pasal 1 angka 4 KUHAP, maka penyelidikan perbuatan yang diduga cybercrime dilakukan pejabat Polridan PNS sebagaimana yang diatur dalam undang-undang.
2. Pengiriman Surat Pemberitahuan Dimulainya Penyidikan(SPDP)
   Pasal 109 ayat (1) KUHAP mengatur bahwa dalam hal penyidik telah memulai melakukan penyidikan suatu peristiwa yang merupakan tindak pidana, penyidik memberitahukan hal itu kepadapenuntut umum. Karena itu, berdasarkan Perkap No 14 tahun 2012 Pasal 1 angka 17, ditentukan bahwa Surat Pemberitahuan Dimulainya Penyidikan adalah surat pemberitahuan kepada Kepala kejaksaan tentang dimulainya penyidikan yang dilakukan oleh penyidik Polri.
3. Upaya PaksaMerujuk pada ketentuan Pasal 26 Perkap No 14 Tahun2012, upaya paksa meliputi:
   a. pemanggilan;
   b. penangkapan;
   c. penahanan;
   d. penggeledahan;
   e. penyitaan, dan
   f. pemeriksaan surat.

   Berdasarkan ketentuan Pasal 43 ayat (6) diatur bahwa dalam hal melakukan penangkapan dan penahanan, penyidik melalui penuntut umum wajib meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam.

   Selanjutnya menurutketentuan Pasal 43 ayat (3) UU ITE, diatur bahwa Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat. Sedangkan dalam ayat (4) diatur bahwa dalam melakukan penggeledahan dan/atau penyitaan, penyidik wajib menjagaterpeliharanya kepentingan pelayanan umum.
4. Pemeriksaan Pasal 63 Perkap No 14 Tahun 2012, bahwa pemeriksaan dilakukan oleh penyidikatau penyidik pembantu terhadap saksi, ahli, dan tersangka yang dituangkan dalam berita acara pemeriksaan yang ditandatangani oleh penyidik/penyidik pembantu yang melakukan pemeriksaan dan orang yang diperiksa. Tujuannya untuk mendapatkan keterangan saksi, ahli dan tersangka yang dituangkan dalam berita acara pemeriksaan, guna membuat terang perkara sehingga peran seseorang maupun barang bukti dalam peristiwa pidana yang terjadi dapat diketahui secara jelas (Idy, 2013).

Berkaitan dengan proses pemeriksaan barang bukti digital baik pada saat penyidikan maupun pemeriksaan di pengadilan, perlu ada kemampuan yang memadai dari penegak hukum. Dalam penanganan data elektronik diperlukan langkah-langkah khusus agar bukti digitalnya tidak berubah. Karena itu, penyidik harus memahami penanganan awal barang bukti elektronik pada komputer di tempat kejadian perkara, penggandaan secara Physicalsektor per sektor (forensic imaging), analisis sistem file (file system) dari Program Microsoft

Windows,mencari dan memunculkan file walaupun sudah dihapus dan diformat, atau data yang tidak pernah disimpan dan hanya di print (files recovery), analisis telepon seluler (mobile forensic), analisis rekaman suara (audio forensic), analisis rekaman video (video forensic), dan analisis gambar digital (image forensic).

Perkara cybercrime merupakan perkara khusus yang cara penyidikannya dapat berbeda sebagaimana penyidikan dalam perkara umum. Dalam melaksanakan tugas dan peranannya maka fungsi reserse khususnya satuan cybercrime mendasarkan pada beberapa undang-undang yang terkait dengan tindak pidana cybercrime yang terjadi. Salah satunya sebagai pedoman alat bukti yaitu ketentuan dalam Pasal 184 KUHAP, dimana yang dimaksud alat-alat bukti adalah keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Selain itu penyidik dapat menggunakan penyidik cybercrime menggunakan alat bukti yaitu Informasi Elektronik dan atau Dokumen Elektronik dan/atau hasil cetaknya. Namun informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam UU ITE. Selain itu informasi elektronik dan/atau dokumen elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk surat yang menurut undangundang harus dibuat dalam bentuk tertulis. Demikian pula dengan surat beserta dokumennya yang menurut undang-undang harus dibuat dalam bentuk akta notaris atau akta yang dibuat oleh pejabat pembuat akta.

Selanjutnya Menurut ketentuan Pasal 6 UU No.11 tahun 2008, diatur pula bahwa dalam hal terdapat ketentuan lain yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, informasi elektronik dan/atau dokumen elektronik, maka akan dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan. Dalam ketentuan Pasal 44 UU ITE diatur bahwa, alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan undangundang ini adalah sebagai berikut: a. alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3). Berdasarkan ketentuan tersebut, maka alat bukti dalam cybercrime adalah sebagai berikut :

a. Informasi Elektronik yaitu 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. Hal ini sesuai dengan ketentuan Pasal 1 angka 1 UU No.11 Tahun 2008.
b. 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. Hal ini didasarkan pada ketentuan Pasal 1 angka 4 UU No.11 Tahun 2008.

Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Informasi Elektronik dan/atau Dokumen Elektronik ataupun hasil cetaknya merupakan bentuk perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia. Namun demikian, hasil cetak dokumen elektronik tidak berlaku untuk: a). surat yang menurut UndangUndang harus dibuat dalam bentuk tertulis; dan b). surat beserta dokumennya yang menurut UndangUndang harus dalam bentuk akta notaris atau akta yang dibuat oleh pejabat pembuat akta. Dalam hal terdapat ketentuan lain yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah

sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

5. Penyerahan Berkas Perkara Ke Penuntut Umum

   Sesuai dengan ketentuan Pasal 110 KUHAP diatur bahwa dalam hal penyidik telah selesai melakukan penyidikan, penyidik wajib segera menyerahkan berkas perkara itu kepada penuntut umum. Dalam hal penuntut umum berpendapat bahwa hasil penyidikan tersebut ternyata masih kurang lengkap, maka penuntut umum segera mengembalikan berkas perkara itu kepada penyidik disertai petunjuk untuk dilengkapi.

   Dalam hal penuntut umum mengembalikan hasil penyidikan untuk dilengkapi, penyidik wajib segera melakukan penyidikan tambahan sesuai dengan petunjuk dari penuntut umum. Penyidik dianggap telah selesai apabila dalam waktu empat belas hari penuntut umum tidak mengembalikan hasil penyidikan atau apabila sebelum batas waktu tersebut berakhir telah ada pemberitahuan tentang hal itu dari penuntut umum kepada penyidik.

   Penipuan secara online masuk dalam kategori perkara pidana biasa. Bilamana terjadi tindak pidana penipuan yang dilakukan secara online, maka pihak korban dapat melaporkannya kepada Aparat Penegak Hukum disertai bukti awal berupa data/informasi elektronik dan/atau hasil cetaknya. Jika kasus tersebut ditindaklanjuti oleh kepolisian dalam suatu proses penyelidikan/penyidikan, maka pihak kepolisian akan menelusuri sumber dokumen elektronik tersebut. Dalam praktek, biasanya yang pertama-tama dilacak adalah keberadaan pelaku dengan menelusuri alamat Internet Protocol (IP Address) pelaku berdasarkan log IP Address yang tersimpan dalam server pengelola web site/homepage yang dijadikan sarana pelaku dalam melakukan penipuan. Namun demikian, permasalahan yang sering kali timbul adalah, pihak kepolisian akan menemui kesulitan jika web site/homepage tersebut pemiliknya berada di luar wilayah yurisdiksi Indonesia. Meskipun saat ini Aparat Penegak Hukum (polisi maupun Penyidik Pegawai Negeri Sipil/PPNS Kementerian Komunikasi dan Informatika) telah bekerja sama dengan beberapa pengelola website/homepage di luar wilayah Indonesia, dalam prakteknya tidak mudah untuk mendapatkan IP address seorang pelaku yang diduga melakukan tindak pidana dengan menggunakan layanan web site/homepage tertentu. Hal ini disebabkan oleh adanya perbedaan prosedur hukum antar negara. Meskipun pemerintah melalui aparat penegak hukum telah membuat perjanjian Mutual Legal Asistance atau perjanjian bantuan hukum timbal balik, pada kenyataannya MLA tidak serta merta berlaku dalam setiap kasus yang melibatkan antar negara. Permasalahan yurisdiksi inilah yang seringkali menjadi penyebab tidak dapat diprosesnya atau tertundanya penyelidikan/penyidikan kasus-kasus cyber crime. Oleh karena itu, pemerintah dan lembaga lain yang terkait perlu melakukan langkahlangkah tertentu untuk dapat mengatasi hambatan-hambatan yang dihadapi dalam penegakan hukum, khususnya terhadap tindak kejahatan yang dilakukan melalui media internet.

   Terkait dengan subjek pelaku tindak pidana, maka pertanggungjawaban pidana dalam Undang-Undang ITE dapat dijatuhkan kepada individu dan korporasi. Hal ini terlihat dari subjek tindak pidana yang terkandung dalam ketentuan pidananya, yaitu setiap orang. Pengertian orang dalam Ketentuan Umum Pasal 1 ayat (21) adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum. Bahkan secara eksplisit, pertanggungjawaban korporasi dalam tindak pidana UU ITE disebutkan secara tegas dalam Pasal 52 ayat(4).

Dalam Undang-Undang ITE, korporasi juga merupakan subjek tindak pidana. Maka seharusnya diatur pula sistem pertanggungjawaban korporasi yang jelas dan terperinci, khususnya berkaitan dengan kapan korporasi dikatakan melakukan tindak pidana, siapa yang bertanggung jawab dan sanksi pidana yang dapat dijatuhkan. Namun dalam undang-undang ini justru tidak diatur mengenai tiga hal pokok tersebut. Terkait sanksi pidana misalnya, hanya disebutkan pidana

pokoknya ditambah dua pertiga. Tidak diatur jenis sanksi lain yang lebih tepat bagi korporasi, seperti tindakan tata tertib penutupan sementara atau selamanya.

KESIMPULAN

Kesimpulan Sebagaimana yang telah diuraikan sebelumnya pada bagian pembahasan, maka dapat dibuat kesimpulan bahwa pengaturan mengenai tindak pidana penipuan yang dilakukan secara online pada prinsipnya sama dengan penipuan konvensional, yang membedakan hanyalah pada sarana perbuatannya yakni menggunakan Sistem Elektronik (komputer, internet, perangkat telekomunikasi). Sehingga secara hukum, penipuan secara online dapat diperlakukan sama sebagaimana delik konvensional yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP). Dengan demikian dalam proses penanganan perkaranya, aparat penegak hukum dapat menerapkan ketentuan-ketentuan hukum, baik yangterdapat dalam KUHP maupun ketentuan-ketentuan hukum yang terdapat dalam UU No. 11 Tahun 2008. Demikian pula dengan prosedur beracaranya, penipuan secara online secara formal akan diproses dan ditangani oleh penyidik, sesuai dengan ketentuan yang diatur dalam KUHAP. Hal ini juga sesuai dengan ketentuan Pasal 42 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

UCAPAN TERIMAKASIH

Pertama-tama saya ucapkan syukur kepada Tuhan Yang Maha Esa telah memberikan rahmat dan barokahnya sehingga saya dapat menulis penelitian ini dengan penuh semangat dan kelancaran. Yang kedua saya ucapkan terimakasih kepada dosen mata kuliah metode penilitian bapak Abshoril Fithry, S.H., M.H. yang telah membimbing, menuntun, dan memberikan kesempatan kepada saya untuk mengikuti Seminar Nasional ini serta menjadi pembicara pada seminar ini. Tak lupa pula saya ucapkan terimakasih kepada penyelenggara Seminar Nasional Penelitian dan Pengabdian kepada Masyarakat 2 Tahun 2023 dengan tema “Inovasi Penelitian dan Pengbdian Kepada Masyarakat Menuju Indonesia Emas 2045” dan juga kepada rekan-rekan sekalian yang saya banggakan

DAFTAR PUSTAKA

Ahmad Ramli. (2006). *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia*.

Arisandy, Y. O. (2021). Penegakan Hukum terhadap Cyber Crime Hacker. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, *1*(3), 162–169. https://doi.org/10.18196/ijclc.v1i3.11264

Idy, M. Y. (2013). *Mekanisme Hukum Penanganan Tindak Pidana Penipuan Yang Dilakukan Melalui Internet*. *1193*, 49–61.

Wulandari, S. (2021). Mekanisme Penyidikan Tindak Pidana Penipuan Yang Menggunakan Media Transaksi Elektronik. *Spektrum Hukum*, *18*(1). https://doi.org/10.35973/sh.v18i1.2388