Website : http://um-tapsel.ac.id email : justitia@um-tapsel.ac.id
JURNAL JUSTITIA : Jurnal Ilmu Hukum dan Humaniora
P- ISSN: 2356 - 9033
E -ISSN: 2579 - 9398
Fakultas Hukum

Pelaksanaan Penyidikan Dalam Pengungkapan Kasus Tindak Pidana Penipuan Online di Wilayah Hukum Polres Karawang

Mochammad Khafiddin Muharam [1)], Ilyas [2)], Aryo Fadlian [3)]

Fakultas Hukum Universitas Singaperbangsa Karawang

Khafidinmuharam30@gmail.com [1)]
ilyas.unsika@gmail.com [2)]
aryo.fadlian@fh.unsika.ac.id [3)]

Abstrak

Penyidikan merupakan tahapan penting dalam peradilan pidana yang bertujuan mengumpulkan bukti dan mengidentifikasi pelaku. Dalam kasus penipuan online, polisi menghadapi kendala melacak pelaku dan memperoleh bukti digital yang memerlukan ilmu IT Forensik. Penelitian ini bertujuan menganalisis pelaksanaan penyidikan tindak pidana penipuan online, mengidentifikasi hambatan yang dihadapi penyidik, dan mengetahui upaya penanganannya dari kendala yang ditemui. Penelitian ini menggunakan metode yuridis normatif dengan menggunakan data sekunder dari kepustakaan, wawancara, dan studi lapangan, serta analisis kualitatif. Penyidikan penipuan online di Polres Karawang mengikuti UU ITE dan KUHAP, perbedaan utamanya terletak pada alat bukti yang diatur dalam UU ITE. Kendala terbesar adalah identifikasi pelaku terhambat oleh bank dan provider telekomunikasi yang tidak bisa membuka data nasabah atau pelanggan. Upaya penyidik yaitu dengan *profiling* akun media sosial yang digunakan oleh pelaku penipuan.

Kata kunci: Kepolisian, Penyidikan, Tindak Pidana Penipuan Online

Abstract

Investigation is an important stage in criminal justice that aims to collect evidence and identify perpetrators. In online fraud cases, the police face obstacles to tracking perpetrators and obtaining digital evidence that requires Forensic IT knowledge. This study aims to analyze the implementation of online fraud investigations, identify the obstacles faced by investigators, and find out how to handle them from the obstacles encountered. This study uses a normative juridical method using secondary data from literature, interviews, and field studies, as well as qualitative analysis. The investigation of online fraud at the Karawang Regional Police follows the ITE Law and the Criminal Procedure Code, the main difference lies in the evidence provided for in the ITE Law. The biggest obstacle is the identification of perpetrators is hampered by banks and telecommunications providers who cannot open customer or subscriber data. Investigators' efforts involve profiling social media accounts used by fraud perpetrators.

***Key words**: Police, Investigations, Online Fraud Crimes*

PENDAHULUAN

Konsep Negara Indonesia sebagai negara hukum merupakan konsep yang dibangun oleh para pendirinya sebagai bagian dari mengatur setiap regulasi tanpa adanya kesewenang-wenangan. Artinya, semua keputusan dan tindakan pemerintah harus didasarkan pada hukum yang berlaku, dan tidak boleh ada diskriminasi atau penyalahgunaan kekuasaan dalam proses pembuatan kebijakan. Prinsip ini menempatkan hukum sebagai landasan utama dalam menjalankan negara dan

melindungi hak-hak warga negara. Oleh karena itu, dengan kemajuan teknologi yang beragam, diharapkan hukum akan mampu mengikuti perkembangan tersebut sehingga tidak ada kelompok yang merasa dirugikan. Pada dasarnya, negara memiliki tanggung jawab untuk memberikan kesejahteraan dan kemakmuran kepada warganya, tidak hanya terbatas pada pengelolaan sumber daya alam, tetapi juga dalam memberikan jaminan keamanan.[1]

Peningkatan teknologi informasi dan komunikasi dewasa ini telah menyebabkan kemudahan bagi masyarakat dalam menyampaikan dan menerima informasi. Dengan adanya teknologi ini, komunikasi antar masyarakat menjadi tak terbatas jarak, ruang, dan waktu. Namun, bersamaan dengan perkembangan teknologi yang pesat, masyarakat juga dihadapkan pada tantangan guna terus mengikuti perkembangan tersebut. Pengembangan teknologi hingga kini bukan terbatas berfungsi guna keperluan komunikasi serta interaksi sosial semata, tetapi juga melibatkan aspek lainnya.

Hal ini menyebabkan banyak perubahan dalam tuntutan kehidupan masyarakat, baik dari segi ekonomi maupun sosial. Perkembangan teknologi informasi juga menyebabkan munculnya kejahatan baru yang disebut *cybercrime*. Cybercrime didefinisikan sebagai Kejahatan umum yang tereksekusi oleh individu-individu yang memiliki keahlian dalam mengendalikan teknologi informasi seperti internet dan ponsel. Kejahatan di dunia maya sangat beragam, contohnya termasuk penipuan kartu kredit, penipuan online, penipuan perbankan, penipuan di bursa efek, pornografi anak, perdagangan narkoba, terorisme, dan lainnya. Selain itu, ada juga kejahatan yang mengincar teknologi informasi itu sendiri, seperti serangan virus (*hacking*), pelanggaran *privasi, phising, spamming*, dan lain sejenisnya.

Contoh kejahatan yang dilakukan melalui media Internet ialah penipuan. Penipuan secara *online* adalah tindakan kriminal yang memanfaatkan fasilitas teknologi dalam pelaksanaannya. Prinsip yang digunakan dalam penipuan online mirip dengan penipuan biasa atau konvensional, di mana terdapat orang yang mengalami kerugian dan pada sisi lain terdapat entitas yang tidak sah yang mendapatkan keuntungan. Perbedaan dasar antara penipuan daring dan penipuan tradisional terletak pada pemanfaatan sistem elektronik seperti perangkat telekomunikasi, internet, dan komputer dalam pelaksanaannya. Dari perspektif hukum, penipuan online maupun konvensional bisa dianggap sebagai delik konvensional yang telah dimuat pada Kitab Undang-Undang Hukum Pidana (KUHP).

Pada garis besarnya, aturan dan ketentuan mengenai tindak pidana penipuan dapat diidentifikasi dalam Pasal 378 KUHP. Pada Pasal tersebut tidak secara khusus mengatur penipuan pada konteks *online*, tetapi mencakup penipuan secara umum (dalam bentuk pokok). Pasal 378 KUHP memberikan pengaturan mengenai tindakan yang bertujuan guna memperoleh keuntungan bagi dirinya sendiri atau orang lain dengan menggunakan nama palsu, kedudukan palsu, tipu muslihat, atau kebohongan untuk memperoleh sesuatu yang memiliki nilai, maka akan dikenai hukuman penjara paling lama 4 (empat) tahun karena melakukan tindak pidana penipuan. Secara spesifik tindak pidana kejahatan yang menyangkut mengenai Informasi dan Transaksi Elektronik telah diatur melalui Undang-undang (UU) Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang selanjutnya UU ini diubah dengan Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Tahun 2008

[1] Roni Sulistyanto Luhukay. Karakteristik Tanggung Gugat Perusahaan Terhadap Lingkungan Dalam Menciptakan Kesejahteraan Rakyat, Jurnal Meta Yuridis (2)2 (2019): 13-34

tentang Informasi dan Transaksi Elektronik yang kemudian disebut Perubahan UU ITE. Dalam UU tersebut, tidak terdapat penguraian yang secara khusus menyebutkan tentang "penipuan," yang dapat diperhatikan dari ketiadaan kata "penipuan" dalam pasal-pasalnya. Namun, ketentuan yang melarang penyebaran berita bohong yang dapat merugikan konsumen termasuk dalam Pasal 28 ayat (1), yang memiliki kesamaan signifikan dengan aspek tindak pidana penipuan dan perlindungan konsumen.[2]

Penyidikan merupakan proses atau Tindakan yang dijalankan oleh petugas penyidik terhadap individu yang dicurigai telah melakukan tindak pidana.. Seseorang dapat dianggap sebagai tersangka ketika ada dugaan bahwa dia terlibat dalam suatu tindak pidana. Dalam Kitab Undang-undang Hukum Acara Pidana (KUHAP) Pasal 1 dan 2, penyidikan merujuk pada serangkaian tindakan yang diambil oleh penyidik sesuai dengan ketentuan undang-undang untuk mencari serta mengumpulkan bukti guna mengungkap fakta tentang tindak pidana yang terjadi dan mencari tersangka yang terlibat. Setelah penyidikan selesai, penyidik akan membuat laporan yang disebut Berita Acara Pemeriksaan (BAP) berdasarkan hasil penyelidikan yang telah dilakukan. Langkah awal dalam penyidikan adalah mencari dan mengamankan barang-barang bukti terkait dengan tindak pidana, yang bisa ditemukan di lokasi kejadian kasus atau tertinggal setelah terjadinya kejahatan.

Penanganan perkara penipuan online pada tingkat penyidikan menjadi sangat penting karena tahap ini menjadi krusial dalam mengungkap pelaku dan membawa mereka ke pengadilan. Namun, kepolisian menghadapi berbagai kendala dalam menangani kasus penipuan online, salah satunya adalah kurangnya pengetahuan dan keterampilan petugas dalam melakukan penyidikan kasus penipuan online.

Selain itu, terdapat kendala-kendala lain yang harus dihadapi, karena dalam proses pembuktian dalam mendapatkan barang bukti, dibutuhkan pengetahuan dalam bidang teknologi informasi (IT) Forensik untuk mengumpulkan bukti-bukti siber yang dapat digunakan pada persidangan. Selain itu, fasilitas dan alat-alat yang mendukung teknologi IT juga menjadi hal penting. Beberapa kasus penipuan online seringkali menyebar di berbagai wilayah dan bahkan luar negeri, sehingga membutuhkan kerja sama dengan kepolisian dari berbagai daerah dan negara. Kendala-kendala ini memerlukan penanganan yang tepat dan strategi yang efektif agar kasus penipuan online dapat diatasi secara efektif. Selain itu, dibutuhkan langkah preventif dan represif guna meminimalisir terjadinya tindak pidana penipuan online.

Perbuatan melawan hukum yang dieksekusi pada media internet atau kejahatan di dunia maya disebut sebagai *Cyber Crime*. Permasalahan yang terkait dengan *cybercrime* selalu menarik perhatian karena beberapa alasan. Pertama, masalah ini masih tergolong baru dan terus berkembang seiring dengan perkembangan teknologi. Kedua, kejahatan di dunia maya sering terkait dengan teknologi yang hanya dimengerti oleh beberapa orang tertentu. Ketiga, lingkup hukum terbatas dalam mengantisipasi dan menangani cybercrime. Masalah-masalah ini menjadi tantangan yang perlu diatasi secara efektif. Di Indonesia, penanganan masalah ini masih dilakukan secara sporadis serta tidak mendapat perhatian serius, padahal jika tidak ditangani dengan serius,

[2] Anton Hendrik Samudra. Modus Operandi dan Problematika Penanggulangan Tindak Pidana Penipuan Daring. Mimbar Hukum: Jurnal Berkala Fakultas Hukum Universitas Gadjah Mada (31)1 (2019): 59-74.

akan berdampak negatif pada kepercayaan terhadap dunia usaha di Indonesia.[3]

Berdasarkan latar belakang masalah tersebut, maka penulis akan membahas mengenai bagaimana pelaksanaan penyidikan dalam pengungkapan kasus tindak pidana penipuan online, apa saja kendala yang dihadapi oleh penyidik dalam pelaksanaan penyidikan kasus tindak pidana penipuan *online,* dan bagaimana upaya yang dilakukanoleh penyidik dalam mengatasi kendala yang dihadapi dalam pelaksaanan peyidikan kasus tindak pidana penipuan *online*

METODE

Penelitian ini menggunakan pendekatan yuridis normatif, yaitu pendekatan penelitian dengan cara meneliti dan mengkaji objek penelitian melalui asas-asas hukum, perundang-undangan untuk lebih mempertajam analisis data penelitian yang bertujuan untuk mengetahui dasar-dasar pemikiran, sejarah, latar belakang hukum dan peraturan perundang-undangan yang berhubungan dengan penyidikan tindak pidana penipuan online. Jenis data yang digunakan adalah data sekunder dengan teknk pengumpulan data kepustakaan dan wawancara atau studi lapangan. Dan dengan analisis data kualitatif.

HASIL DAN PEMBAHASAN

Pelaksanaan Penyidikan Dalam Pengungkapan Kasus Tindak Pidana Penipuan Online

Prinsip dasar penerapan hukum pidana yang telah dikodifikasi adalah bahwa hukum pidana yang telah dikodifikasi berlaku bagi semua jenis pelanggaran pidana, baik yang diatur di dalam kode tersebut maupun yang tidak, kecuali apabila ada penentuan dan pengaturan khusus yang terdapat di luar kode. Prinsip yang sama berlaku bagi hukum acara pidana dalam konteks Informasi dan Teknologi Elektronik (ITE), di mana pada dasarnya hukum acara pidana yang termuat dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP) tetap berlaku. Namun, disamping itu, terdapat pula ketentuan khusus mengenai proses penyidikan dalam Bab X Undang-Undang ITE. Berdasarkan prinsip lex specialis derogat legi generali, maka yang diberlakukan adalah peraturan yang bersifat khusus dalam hal ini.

Dalam proses penyelidikan kejahatan di bidang ITE, tidak hanya diberlakukan semua peraturan terkait penyelidikan yang tercantum dalam undang-undang acara hukum (Bab IV Bagian kesatu dan Kedua KUHAP), tetapi juga berlaku peraturan yang bersifat spesifik mengenai penyelidikan yang dijelaskan dalam Bab X Pasal 42 hingga 44 UU ITE. Dalam tiga pasal ini, hanya diatur dua hal yang memiliki sifat khusus, yakni:

1. Tentang penyidik dan hak atau kewenangannya serta prosedur yang harus dipenuhi dalam hal melaksanakan kewenangan melakukan penyidikan tersebut (Pasal 43);
2. Tentang alat bukti yang dapat digunakan dalam hal penyidikan, penuntutan dan dalam siding pengadilan perkara tindak pidana ITE (Pasal 44).

Berdasarkan hasil wawancara dengan Brigpol Tomy Noordiansyah S.H. penyidik Unit III Tipiter Satuan Reserse Kriminal (Satreskrim) Kepolisian Resor Karawang (Polres Karawang) Untuk perbedaan penyidikan selain dengan kasus tindak pidana

[3] Sally Carmelia Azis, Annie Myranika, Erialdy. Penerapan Penyidikan Tindak Pidana Penipuan Melalui Media Elektronik Whatsapp Oleh Direktorat Tindak Pidana Siber Bareskrim Polri. Jurnal Pemandhu (3)3 (2022): 206-212

penipuan online yaitu seperti dari barang buktinya, yaitu disebut dengan Alat Bukti elektronik yaitu sperti contohnya *screenshoot chatting* antara korban dan pelaku tindak pidana penipuan, bukti struk transfer *Automated Teller Machine* (ATM) atau juga dengan menggunakan bukti transfer dari mobile *banking*, *internet banking*, dan SMS banking, *Short Message Service* (SMS) verifikasi pemesanan barang, dan lain lain rekam data penipuan harus dijamin keutuhan atau keasliannya untuk diajukan sebagai alat bukti. selebihnya pelaksanaan penyidikannya sesuai dengan tahapan yang ada di KUHAP dan di UU ITE. Jika misalnya terdapat petunjuk saksi untuk selanjutnya tahapannya melakukan undangan klarifikasi dari proses lidik lalu apabila ditemukan alat bukti serta saksi-saksi mencukupi lalu masuk ke tahap penyidikan. Pada tahap penyidikan diperiksa Kembali dari saksi hingga lainnya. Setelah itu penetapan tersngka jika benar-benar bukti sudah tercukupi.

Pada prinsipnya, wewenang untuk melakukan penyidikan terhadap kejahatan di bidang ITE diberikan kepada pejabat penyelidik dari Kepolisian Negara Republik Indonesia. Namun, dalam situasi tertentu, Penyidikan terhadap tindak pidana ITE juga memiliki kemungkinan dilakukan oleh petugas penyidik yang berwenang. yang memiliki tanggung jawab di dalam ranah teknologi informasi dan transaksi elektronik. Salah satu contohnya Merupakan penyidik yang berasal dari Kementerian Komunikasi dan Informatika (KOMINFO).

Dalam Pasal 5 Undang-Undang ITE, tidak ada penjelasan serupa seperti yang terdapat dalam Pasal 26A dari Undang-Undang Nomor 31 Tahun 1999 yang telah mengalami perubahan melalui Undang-Undang Nomor 20 Tahun 2001. Yaitu Kedua jenis alat bukti yang diuraikan dalam Pasal 26A secara tegas dijelaskan yakni elemen yang bisa dijadikan dasar dalam membentuk alat bukti petunjuk. Ini menyiratkan bahwa kedua jenis alat bukti ini memiliki posisi dan peran yang setara dengan alat bukti lainnya seperti kesaksian saksi, keterangan dari terdakwa, dan dokumen, dalam membentuk dasar bagi alat bukti petunjuk Meskipun begitu, karakteristik Informasi Elektronik dan Dokumen Elektronik, sebagaimana dijelaskan dalam Pasal 1 angka 1 dan angka 4 Undang-Undang ITE, memiliki kesamaan dengan ciri-ciri alat bukti surat. Kemiripan ini terletak pada aspek visual seperti tulisan dan/atau gambar yang bisa dilihat dan dibaca serta memiliki makna tertentu. Oleh karena itu, frasa "merupakan perluasan" dalam kalimat Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil pencetakannya sebagaimana yang dijelaskan dalam ayat (1), Dapat dimaknai sebagai ekspansi dari kategori alat bukti yang sah sesuai dengan aturan-aturan Prosedur Hukum yang berlaku di Indonesia, dengan fokus pada perluasan dalam bentuk bukti berupa tulisan, dan hal ini mengacu pada perluasan alat bukti yang berupa dokumen

Oleh sebab itu, terkait dengan alat bukti petunjuk, alat bukti Informasi Elektronik dan Dokumen Elektronik, yang merupakan perluasan dari alat bukti surat atau memiliki kedudukan dan peran yang setara dengan alat bukti surat, juga memiliki posisi dan peran yang serupa dengan alat bukti surat saat digunakan sebagai komponen dalam membentuk alat bukti petunjuk.

Jadi Informasi Elektronik dan Dokumen Elektronik dalam hukum acara pidana ITE mempunyai kedududkan yang sama dengan alat bukti surat, yang sekaligus sebagai alat bukti yang dapat digunakan hakim untuk membentuk alat bukti petunjuk. Oleh karena itu pula mempunyai nilai yang sama dengan alat bukti surat dalam hal untuk membentuk keyakinan hakim tentang kesalahan terdakwa menurut Pasal 183 KUHAP.

Walaupun posisi dan peran alat bukti Informasi Elektronik dan Dokumen

Elektronik sejajar dengan alat bukti surat, terdapat pembatasan dalam penggunaannya. Diatur dalam Pasal 5 Ayat (4) Undang-Undang ITE bahwa Aturan mengenai Informasi Elektronik dan/atau Dokumen Elektronik seperti yang dijelaskan pada ayat (1), tidak berlaku untuk:

1. Surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan
2. Surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

Untuk surat yang diwajibkan oleh undang-undang untuk dihasilkan dalam bentuk tertulis, seperti yang disebutkan dalam poin a, penjelasan tambahannya adalah sebagai berikut: "Surat yang diwajibkan oleh undang-undang untuk diwujudkan dalam bentuk tertulis mencakup, namun tidak terbatas pada, surat-surat berharga, instrumen berharga, dan surat-surat yang diterapkan dalam proses penegakan hukum di bidang acara perdata, pidana, serta administrasi negara". Mengamankan integritas dokumen elektronik sebagai bukti yang sah menjadi esensial, karena melalui dokumen ini akan dijelaskan dengan rinci kronologi terjadinya tindak pidana. Dengan memastikan keaslian dan keutuhan dokumen elektronik, kita dapat membangun landasan yang kuat untuk memahami dan mengungkap kasus kejahatan tersebut.[4]

Kendala Yang Dihadapi Oleh Penyidik Dalam Pelaksanaan Penyidikan Kasus Tindak Pidana Penipuan Online

Pelaksanaan penyidikan di indonesia terkait kasus tindak pidana penipuan *online* disinyalir mengalami kendala atau kesulitan. Karena pelaku penipuan online kebanyakan menggunakan data atau identitas palsu serta penipuan tindakan yang dijalankan oleh pelaku yang berlokasi di negara asing membuat semakin sulit dalam hal penanganan kasus tersebut.

Berdasarkan wawancara dengan Brigpol Tomy Menyebutkan bahwa tingkat kesulitan dalam penaganan perkara tebagi menjadi tiga yaitu tingkatan mudah, sedang dan sulit. Saat ini penangan perkara penipuan *online* merupakan penaganan perkara yang sulit karena yang pertama saksinya minim, yang kedua sulitnya berkoordinasi dengan pihak bank dan *provider* nomor telepon itu mereka tidak bisa membuka data atau memberikan data nasabah atau pelanggannya. Lebih lengkapnya Brigpol Tomy menjelasakan bahwa hambatan yang ditemui dalam penyidikan tindak pidana penipuan *online* yaitu dari pihak bank yang tidak mau membuka data rekening pelaku. Seperti contohnya Ketika dari pihak kepolisian mengirim surat ke bank untuk dimintakan membuka data rekening pelaku, dari pihak bank justru mengirimi balik surat ke kepolisian yang menjelaskan bahwa untuk membuka data rekening harus dengan surat kuasa yang dibuat oleh pemilik rekening tersebut dalam hal ini pemilik rekening tersebut ialah pelakunya, sangat tidak logis jawaban dari pihak bank untuk meminta surat kuasa dari pemilik rekening pelaku meskipun ini untuk kepentingan penyidikan di kepolisian, serta juga ada pihak bank yang tidak membalas surat dari kepolisian. lalu dari pihak *provider* juga kurang lebih sama seperti pihak bank yaitu dia menjelaskan bahwa *provider* membalas surat ke kepolisian yang menyatakan bahwa tidak bisa membuka data pelanggannya karena ancaman pidananya kurang dari lima tahun sedangkan tindak pidana penipuan dalam pasal 378 KUHP dengan ancaman paling lama empat tahun penjara.

[4] Monika Elisabet Lamtiur Butar-Butar, Nyoman Serikat Putra Jaya, Bambang Dwi Baskoro."Pembuktian Tindak Pidana Penipuan Melalui Media OnlineDilihat Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Informasi Dan Transaksi Elektronik." Diponegoro Law Review 5 no.2 (2016): 1–14, Hal. 6-7

Lebih lanjut Brigpol Tommy menyatakan bahwa dalam menagani perkara di Satreskrim Polres Karawang untuk penipuan *online* secara umum masih menerapkan pasal 378 KUHP, memang tidak menutup kemungkinan menerapkan pasal 28 ayat (1) UU ITE, tetapi pada kenyataan dilapangannya atau praktiknya masih menerapkan pasal 378. Karena umumnya penipuan *online* tidak masuk dalam frasa konsumen pada UU ITE Pasal 28 ayat 1.

Sumadi menuliskan dalam artikelnya bahwa Kendala dalam penegakan hukum ini muncul karena minimnya pemahaman aparat penegak hukum mengenai aspek teknologi informasi (internet), keterbatasan fasilitas serta infrastruktur, dan rendahnya kesadaran masyarakat akan aspek hukum dalam mengatasi tindak pidana teknologi informasi.[5] Selanjutnya, disebutkan bahwa situasi ini juga mencakup kurangnya kesiapan aparat penegak hukum di wilayah-wilayah, di mana mereka belum memadai dalam menghadapi peningkatan kasus tindak kejahatan ini disebabkan oleh adanya banyak aparat penegak hukum yang memiliki keterbatasan pengetahuan dalam bidang teknologi (kurang paham teknologi atau gaptek), yang diakibatkan karena kurangnya institusi hukum di wilayah tersebut yang belum dilengkapi dengan akses internet.[6]

Di sisi lain, Tumalun menguraikan dalam tulisannya tentang faktor-faktor yang menghalangi upaya penanggulangan kejahatan komputer dan/atau sistem elektronik, yang meliputi:[7]

1. Terbatasnya personil Tenaga Ahli;

Terbatasnya jumlah personil tenaga ahli antara Negara Indonesia dan China sangatlah berbeda jauh dalam jumlah personilnya. Lebih ironis lagi laporan tingkat kejahatan siber di Indoensia semakin meningkat, dengan keterbatasan personil dan tenaga ahli di pihak kepolisisan Indonesia maka penyelesaian kasus tersebut tidak bisa diselesaikan dengan cepat. Akibatnya dirasakan langsung oleh pihak korban atau kejahatan siber. Kualitas fasilitas teknologi informasi di Indonesia memang sudah cukup baik, namun tidak sebanding dengan jaminan keamanan oleh para pengguna. Barda Nawawi dalam Tumalun mengatakan bahwa "Keterbatasan tenaga ahli pada pihak kepolisian memang merupakan faktor yang sangat besar, dengan jumlah anggota ahli yang terbatas ini pengungkapan dan penyidikan kasus kejahatan dunia maya tidak bisa diselesaikan dengan waktu yang cepat, sehingga akan membuat para pelaku lebih leluasa dalam beraksi".

2. Lemahnya pengawasan Pemerintah; dan

Lemahnya pengawasan penggunaan internet berpotensi besar akan menciptakan peluang terjadinya kejahatan *cybercrime* (dunia maya). Karena kejahatan dengan menggunakan teknologi terjadi jika ada akses internet yang cukup memadai. Saat ini fasilitas internet di sejumlah kota besar di Indonesia bisa dikatakan sudah memadai baik dari segi kecepatan akses dan kemudahan pemasangan jaringan akses internet. Namun dengan tidak adanya kebijakan dan langkah preventif yang menjadi faktor utama, para pengguna bisa dengan bebas mengakses data-data tertentu yang mana bisa disalahgunakan oleh pengguna yang tidak bertanggung jawab.

3. Kendala Prosedural Hukum UU ITE

[5] Hendy Sumadi, "Kendala Dalam Menanggulangi Tindak Pidana Penipuan Transaksi Elektronik Di Indonesia," Jurnal Wawasan Hukum 33, no. 2 (2015): 175–203. Hal. 197.
[6] Ibid hal. 197
[7] Brisilia Tumalun, "Upaya Penanggulangan Kejahatan Komputer Dalam Sistem Elektronik Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008," Lex Et Societatis 6, no. 2 (2018): 24–31. Hal. 27

Lemahnya perangkat hukum UU ITE dapat terlihat pada Pasal 27 dan 37 mengenai perbuatan yang dilarang dimana para aparat penegak hukum itu sendiri masih banyak yang belum memahami makna dari pasal tersebut.

Lebih lanjut Brigpol Tommy juga menyebutkan untuk membuka data nomor rekening juga bisa dilakukan tetapi banyak sekali tahapan dalam birokrasi yang sulit yaitu kapolres harus bersurat ke kapolda lalu kapolda bersurat ke kapolri lalu kapolri bersurat ke gubernur bank Indonesia, lalu gubernur bank Indonesia melihat data untuk dibuat keputusan apakah disetujui atau tidak untuk membuka data nasabah, jika disetujui oleh Gubernur Bank Indonesia lalu bersurat lagi dari kapolri hingga ke tingkat kapolres.

Dalam penanganan kasus tindak pidana penipuan *online* di polres karawang ini hingga saat ini belum ada yang naik ke tingkat kejaksaan. Yang mana dari laporan tindak pidana penipuan online yang masuk akhirnya terhenti di penyelidikan akibat dari hambatan-hambatan yang ditemui seperti yang sudah dijelasakan diatas. Brigpol Tommy juga yakin jika dari pihak bank dan provider telekomunikasi mempermudah dalam hal membuka data akan membuat angka penipuan online turun

Upaya Yang Dilakukan Oleh Penyidik Dalam Mengatasi Kendala Yang Dihadapi Dalam Pelaksanaan Penyidikan Kasus Tindak Pidana Penipuan *Online*

Hambatan-hambatan yang tergambarkan sebelumnya setidaknya harus dapat diminimalisir dengan segera karena berbicara mengenai perkembangan teknologi saat ini juga disinyalir sangat cepat sehingga perlu ada aturan hukum yang lebih progresif lagi untuk mengatasi hambatan-hambatan tersebut

Penanggulangan kejahatan di dunia maya tidak terlepas dari kebijakan penanggulangan kejahatan atau yang biasa dikenal dengan istilah politik kriminal, menurut Sudarto politik kriminal merupakan suatu usaha yang rasional dari masyarakat dalam menanggulangi kejahatan.[8] Oleh karena itu tujuan pembuatan UU ITE tidak terlepas dari tujuan politik kriminal yaitu sebagai upaya untuk kesejahteraan sosial (*social welfare*) dan untuk perlindungan masyarakat (*social defence*). Evaluasi terhadap kebijakan di dunia mayantara tetap diperlukan sekiranya ada kelemahan kebijakan formulasi dalam perundang-undangan tersebut. Menurut Barda Nawawi Arief, evaluasi atau kajian ulang ini perlu dilakukan, karena ada keterkaitan erat antara kebijakan formulasi perundang-undangan (*legaslative policy*) dengan kebijakan penegakan hukum (*law enforcement policy*) dan kebijakan pemberantasan/ penanggulangan kejahatan (*criminal policy*). Kelemahan kebijakan formulasi hukum pidana, akan berpengaruh pada kebijakan penegakan hukum pidana dan kebijakan penanggulangan kejahatan.[9]

Brigpol Tomy menyebutkan juga upaya untuk mengatasi hambatan-hambatan yang ditemui yaitu mencoba untuk terus berkomunikasi pihak bank dengan komunikasi yang baik tapi tetap saja nihil, karena mereka juga punya aturan sendiri dan jika mereka melanggar ada sanksi pidananya, lalu upaya lainnya yaitu dengan upaya *profiling* secara pribadi seperti misalnya jika melalui media facebook memerika apakah akun yang digunakan oleh pelaku merupakan asli atau palsu, jika akunnya adalah palsu maka proses yang dijalani menemui jalan yang buntu, lalu jika akun tersebut asli bisa mendapatkan petunjuk lain selain dari nomor rekening atau nomor handphone.

[8] Sudarto, Hukum dan Hukum Pidana, Alumni, Bandung, 1977, hlm. 38
[9] Barda Nawawi Arief, Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Jakarta, 2007, hlm. 214-215

Dalam Seminar *Cybercrime* dan *Cyber Porn* dalam Perspektif Hukum Teknologi dan Hukum Pidana, Barda Nawawi Arief dalam Ginting mengatakan bahwa upaya Peningkatan Efektifitas dan Pembaharuan Orientasi (Reformasi/ Rekonstruksi) Penegakan Hukum Pidana Menghadapi *Cybercrime* perlu kiranya ditempuh beberapa langkah (upaya) antara lain sebagai berikut:[10]

1. Meningkatkan komitmen strategi/prioritas nasional dalam penanggulangan kejahatan di bidang kesusilaan, yang seyogyanya disejajarkan dengan upaya penanggulangan tindak pidana korupsi, narkoba, terorisme dan sebagainya;
2. Melakukan pembaharuan pemikiran/ konstruksi juridis (juridical construction reform), antara lain:
   a. rekonstruksi penegakan hukum (pemikiran hukum) dalam konteks kebijakan pembaharuan sistem hukum dan pembangunan nasional;
   b. melakukan konstruksi hukum yang konseptual/substansial (*substansial legal construction*) dalam menghadapi kendala juridis;
   c. meningkatkan budaya/orientasi keilmuan (*scientific culture/scientific approach*) dalam proses pembuatan dan penegakan hukum pidana.
3. Upaya melakukan pembaharuan/ rekonstruksi pemikiran yuridis (butir nomor 2 di atas) seyogyanya dilakukan untuk semua bidang penegakan hukum pidana. Namun terutama diperlukan dalam menghadapi masalah cybercrime (CC) karena CC tidak dapat disamakan dengan tindak pidana konvensional, sehingga tidak bisa dihadapi dengan penegakan hukum dan pemikiran/ konstruksi hukum yang konvensional.

Untuk kemahiran para penyidik di Unit Tipiter Satreskrim Polres Karawang dalam mempermudah pengungkapan kasus penipuan online hanya beberapa penyidik saja yang mahir dan sudah mendapat pelatihan. Meskipun tidak semua karena setiap penyidik punya keahlian nya masing-masing dalam mengurus perkara yang masuk di Unit Tipiter, Karena unit tipiter tidak hanya mengurus tindak pidana siber saja khususnya penipuan online, tetapi juga menangani tindak pidana di luar KUHP lainnya. Jika berkaca pada Unit Tindak Pidana korupsi (Tipikor) yang menangani perkara korupsi yang merupakan delik di luar KUHP, maka karena banyaknya kasus tindak pidana siber di unit Tipiter mungkin saja bisa dibentuk Unit baru yang khusus menangani tindak pidana siber yang semakin berkembang. Tetapi memang membuat unit baru perlu biaya yang sangat besar dan terlebih harus dibarengi dengan fasilitas-fasilitas yang mumpuni sebagai penunjang dalam pengungkapan kasus tindak pidana siber.

Dalam menangani kasus-kasus *cybercrime* khususnya tindak pidana penipuan transaksi elektronik, Indonesia sangat membutuhkan aparat penegak hukum yang mumpuni, yang terorganisasi dan terstruktur untuk menyatukan komunitas-komunitas spesialisasi dalam penanganan segala jenis tindak pidana *cyber*. Tanpa adanya penegakan hukum yang terorganisasi dan terstruktur di bidang teknologi informasi, maka akan sulit menjerat penjahat-penjahat *cyber* oleh karena kejahatan *cyber* ini *locos delicti*-nya bisa lintas negara. Dalam hal menangani kasus *cybercrime* khususnya tindak pidana penipuan transaksi elektronik diperlukan spesialisasi aparat penyidik yang dapat dipertimbangkan sebagai salah satu cara untuk melaksanakan upaya penegakan hukum terhadap *cybercrime*. Spesialisasi tersebut dimulai dari adanya pendidikan yang diarahkan untuk menguasai teknis serta dasar-dasar

[10] Philemon Ginting, Thesis tentang "Kebijakan Penanggulangan Tindak Pidana Teknologi Informasi Melalui Hukum Pidana", Universitas Diponegoro, 2008. Hal. 229

pengetahuan di bidang teknologi komputer. Pasal 43 UU ITE, menerangkan selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu dilingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-Undang tentang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik.

Faktor sarana prasarana juga dirasakan masih menjadi salah satu faktor lemahnya penegakan hukum terhadap tindak pidana penipuan tersebut. Sebagai contoh fasilitas komputer yang tersedia saat ini hanya berfungsi sebatas kegiatan administratif, sementara kejahatan melalui internet dilakukan dengan menggunakan komputer yang berjaringan dan berkapasitas teknologi yang tinggi dan rumit sehingga pihak aparat penegak hukum masih sulit untuk melacak, mendeteksi ataupun mengimbangi kegiatan para pelaku kejahatan tersebut. Hal senada juga dapat terlihat pada kurangnya kemampuan dan keterampilan aparat penegak hukum di bidang komputer yang mengakibatkan taktis, teknis penyelidikan, penuntutan dan pemeriksaan di pengadilan tidak dikuasai karena menyangkut sistem yang ada didalam komputer.

Bagaimana bisa melaksanakan tugas dan tanggung jawabnya sebagai penyidik di bidang teknologi informasi dan transaksi elektronik, apabila tanpa adanya sarana atau fasilitas tertentu, maka tidak mungkin penegakan hukum akan berlangsung dengan lancar. Sarana atau fasilitas tersebut antara lain, mencakup tenaga manusia yang berpendidikan dan trampil, organisasi yang baik, peralatan yang memadai, keuangan yang cukup, dan seterusnya. Menurut Strecher (1971:59- 66) penegakan hukum bukanlah suatu yang bisa dilihat sebagai berdiri sendiri, melainkan senantiasa bertukar kegiatan dengan masyarakat yang melayaninya, atau yang dengan mengutip Parsons kita sebut sebagai relational. Dengan demikian kiranya bila diterima, bahwa perubahanperubahan dalam masyarakat yang disebabkan oleh penggunaan teknologi modern, terutama yang berupa peliputan dalam kecepatan dan daya merusak, akan memberikan pengaruhnya sendiri terhadap penegakan hukum dalam masyarakat. Khususnya dalam hubungan dengan pekerjaan penegakan hukum yang dalam hal ini banyak dipusatkan pada pekerjaan kepolisian.[11]

Terakhir Brigpol Tommy mengatakan bahwa ada program atau kegiatan khusus dilakukan polres karawang Bersama satreskrim untuk pencegahan dan penanggulangan kasus penipuan online yaitu Polres karawang sudah membentuk tim dari humas yang anggotanya sudah mendapatkan pelatihan dari Polda yaitu tim *cybercrime* yang melakukan patroli siber untuk melihat akun-akun media sosial yang diduga melakukan tindak pidana penipuan dan bisa juga berdasarkan laporan-laporan dari masyarakat. Untuk pencegahan yang dilakukan yaitu memberikan arahan Ketika ada yang konsultasi ke polres seperti jangan mudah transfer ke orang lain yang tidak dikenal.

SIMPULAN DAN SARAN

Simpulan

Pelaksanaan penyidikan dalam penanganan kasus tindak pidana penipuan online di wilayah hukum polres karawang seseuai dengan yang ada di UU ITE dan

[11] Satjipto Rahardjo, Masalah Penegakan Hukum Suatu Tinjauan Sosiologis, Sinar Baru, Bandung, 2005, hlm. 125-126

Kuhap, yang membedakannya dengan dengan penanganan tindak pidan alai yaitu pada alat buktinya yaitu informasi elektronik dan/atau dokumen digital misalnya berupa chatting antara korban dan pelaku tindak pidana penipuan, bukti struk transfer Automated Teller Machine (ATM), Short Message Service (SMS) verifikasi pemesanan barang, dan lain lain rekam data penipuan harus dijamin keutuhan atau keasliannya untuk diajukan sebagai alat bukti.

Saat ini penanganan perkara penipuan *online* masih sangat sulit karena jika dilihat dari hambatan-hambatannya terutama dari pihak bank dan pihak provider telekomunikasi yang tidak mau membuka data nasabah atau pelangggan, dari pihak bank justru mensyaratkan untuk meminta surat kuasa dari pemilik rekening jika ingin membuka data sedangkan pemilik rekening tersebut merupakan pelakunya yang tidak diketahui keberadaannya, dan juga pada pihak provider telekomunikasi menolak memberikan data pelanggannya karena perkara tersebut ancaman penjaranya kurang dari 5 tahun. padahal dengan diberikannya informasi mengenai data pelanggan atau nasabahnya yang dalam hal ini ialah identitas pelaku maka dapat mempermudah pihak kepolisian untuk mencari dan menangkap pelaku tindak pidana penipuan online.

Upaya yang bisa dilakukan para penyidik untuk mengatasi kendala tersbut hanya sebatas terus berkomunikasi dengan pihak bank dan pihak provider telekomunikasi, tetapi hasilnya pun tetap nihil karena dari mereka juga punya aturan sendiri terkait membuka data nasabah atau pelanggan dan jika melanggar ada sanksi pidananya. Dan juga upaya lainnya ialah seperti *profiling* akun media sosial yang digunakan untuk melakukan tindak pidana penipuan online.

Saran

Perlunya dibuat lagi aturan khusus yang bisa mempermudah berkoordinasi dengan pihak diluar kepolisisan seperti bank dan provider telekomunikasi, walaupun sudah ada aturan pengecualian untuk pihak bank atau provider telekomunikasi untuk membuka data dalam upaya penagangan perkara tindak pidana, tetapi pada kenyataannya di lapangan masih banyak penolakan-penolakan yang dilakukan oleh pihak bank dan provider telekomunikasi.

UCAPAN TERIMAKASIH

Puji syukur kehadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan artikel ilmiah ini. Serta juga penulis sampaikan terima kasih sebesar-besarnya kepada pembimbing dalam penulisan skripsi penulis yaitu, Bapak Dr. Ilyas, S.H, M.H. dan Bapak Aryo Fadlian, S.H, M.H. dan yang utama ialah keluarga di rumah yang selalu mendoakan dan menjadikan motivasi terbesar penulis dalam menyelesaikan karya ilmiah ini. Serta kepada seluruh teman-teman penulis di Unsika yang sudah banyak memberikan saran dan arahan dalam penulisan karya ilmiah ini

DAFTAR PUSTAKA

Anton Hendrik Samudra. “Modus Operandi dan Problematika Penanggulangan Tindak Pidana Penipuan Daring”. Mimbar Hukum: Jurnal Berkala Fakultas Hukum Universitas Gadjah Mada, Vol.31 No.1 (2019).

Barda Nawawi Arief, (2007). Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan. Jakarta: Kencana

Brisilia Tumalun, “Upaya Penanggulangan Kejahatan Komputer Dalam Sistem Elektronik Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008,” Lex Et

Societatis Vol. 6, No. 2 (2018).

Hendy Sumadi, "Kendala Dalam Menanggulangi Tindak Pidana Penipuan Transaksi Elektronik Di Indonesia," Jurnal Wawasan Hukum Vol. 33, No. 2 (2015).

Monika Elisabet Lamtiur Butar-Butar, Nyoman Serikat Putra Jaya, Bambang Dwi Baskoro, "Pembuktian Tindak Pidana Penipuan Melalui Media OnlineDilihat Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Informasi Dan Transaksi Elektronik". Diponegoro Law Review, Vol.5 No.2 (2016)

Philemon Ginting, Thesis tentang "Kebijakan Penanggulangan Tindak Pidana Teknologi Informasi Melalui Hukum Pidana", Universitas Diponegoro, 2008.

Roni Sulistyanto Luhukay. Karakteristik Tanggung Gugat Perusahaan Terhadap Lingkungan Dalam Menciptakan Kesejahteraan Rakyat, Jurnal Meta Yuridis Vol. 2 No. 2 (2019).

Sally Carmelia Azis, Annie Myranika, Erialdy. Penerapan Penyidikan Tindak Pidana Penipuan Melalui Media Elektronik Whatsapp Oleh Direktorat Tindak Pidana Siber Bareskrim Polri. Jurnal Pemandhu (3)3 (2022).

Sudarto. (1977). *Hukum dan Hukum Pidana*. Bandung: Alumni\