MASALAH-MASALAH HUKUM
p-ISSN : 2086-2695 e-ISSN : 2527-4716
Diterbitkan oleh Fakultas Hukum Universitas Diponegoro Semarang

JURNAL MASALAH-MASALAH HUKUM
Tersedia online di https://ejournal.undip.ac.id/index.php/mmh/
Volume 51, Nomor 4, Oktober 2022

HAMBATAN TEKNIS PENYIDIKAN TINDAK PIDANA MANIPULASI INFORMASI ELEKTRONIK PADA POLDA SUMATERA BARAT[1]

Fitriati*, Iyah Faniyah, Nisep Rahmad
Magister Ilmu Hukum, Universitas Ekasakti Padang
Jl. Veteran Dalam, Padang Pasir, Kec. Padang Bar., Kota Padang, Sumatera Barat
fitriatif08@gmail.com

Abstract

This study aims to discuss technical barriers in investigating criminal acts of manipulation of electronic information and/or electronic documents by investigators. This study uses a normative juridical research method using secondary legal data. Based on the results of the study, it was concluded that the technical obstacles that occurred during the examination of witnesses and victims during the investigation process were because the witness only found out after the incident took place because he received the impact of the attack that was launched. The attack data in the server log has been deleted, usually in the case of defacement, so investigators have difficulty finding statistical logs on the server because usually the server automatically deletes the existing logs to reduce the server load.

Keywords: *Barriers; Investigation; Manipulation; Information; Electronic.*

Abstrak

Penelitian ini bertujuan membahas hambatan teknis dalam penyidikan tindak pidana manipulasi informasi elektronik dan/atau dokumen elektronik oleh penyidik. Penelitian ini menggunakan metode penelitian yuridis empiris dengan menggunakan data hukum primer dan sekunder. Hasil penelitian menunjukkan hambatan teknis yang terjadi pada pemeriksaan saksi dan korban pada proses penyidikan, sebab saksi hanya mengetahui setelah kejadian berlangsung karena menerima dampak dari serangan yang dilancarkan. Data serangan di *log server* sudah dihapus terjadi pada kasus *deface*, sehingga penyidik kesulitan mencari *log* statistik di *server* sebab secara otomatis *server* menghapus *log* yang ada untuk mengurangi beban *server.* Maka penyidik harus melakukan kerjasama dengan penyidik negara lain. Selanjutnya dengan menggunakan keterangan atau pendapat para ahli telematika yang mempunyai keahlian di bidangnya, agar dapat jadi pertimbangan bagi hakim ketika memutus suatu perkara.

Kata Kunci: Hambatan; Penyidikan; Manipulasi; Informasi; Elektronik.

A. Pendahuluan

Semakin majunya perkembangan di bidang teknologi informasi semakin banyak juga kejahatan yang muncul salah satunya di dunia *cyber*. Keamanan Informasi dan Transaksi Elektronik (ITE) saat ini selalu dibayang-bayangi dengan tingginya kejahatan ITE tersebut sehingga menyebabkan banyak orang yang menjadi korban dari kejahatan *cyber* khususnya di

[1] Jurnal ini adalah hasil penelitian yang dibiayai dari dana penellitian internal LPPM Universitas Ekasakti Tahun 2020.

Indonesia (Arifah, 2011). Internet atau *interconnecting networking* menjadi kebutuhan utama dalam kehidupan sehari-hari dan memberikan banyak manfaat khususnya informasi terkini tentang hukum, politik dan ekonomi (Rahardjo, 2002). Perkembangan teknologi komputer dan jaringan internet telah menciptakan dunia baru yang dinamakan *cyberspace*, yaitu sebuah wadah bagi seseorang dimana mereka dapat berkomunikasi satu sama lain dengan berbasis jaringan internet pada komputer mereka. Akan tetapi perkembangan internet bagaikan dua sisi mata pedang, di satu sisi sangat memudahkan dalam memperoleh informasi tentang hukum, ekonomi dan politik, di sisi lain banyak juga terjadi kejahatan melalui internet. Perkembangan internet bisa jadi memberi celah bagi pelaku kejahatan untuk menjalankan aksinya.

Kejahatan yang sering terjadi yaitu manipulasi informasi elektronik dengan diawali oleh tindakan *illegal access.* Akses adalah kegiatan melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau dalam jaringan sebagaimana ketentuan Pasal 1 ayat (15) Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Sedangkan *Ilegal* dalam arti luas menurut kamus besar bahasa Indonesia (KBBI) yaitu tidak sah, tanpa hak, tanpa izin, tidak menurut hukum. Gagasan tanpa hak dan tidak menurut hukum memperoleh bentuk yang jelas dalam pemikiran yang dipelopori oleh L.J. van Apeldoorn tanpa hak mempunyai terminologi yang disebut *wederrechtelijk* dalam hukum pidana diartikan bertentangan dengan hukum *in strijd met het rech* atau melanggar hak orang lain *met krenking van eens anders recht* dan tidak berdasarkan hukum *niet steunend op het recht* (Remmelink, 2003)*,* dalam rangka menanggulangi kejahatan yang berupa *illegal access* tersebut maka dikembangkanlah suatu rezim hukum baru yaitu hukum siber.

Rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika. Hukum *cyber* atau *cyber law*, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Hal yang dilarang dan yang diperbolehkan dalam aktivitas pemanfaatan teknologi informasi dan komunikasi inilah yang diatur dalam rezim hukum *Cyber* atau *Cyber Law* (Hill & Marion, 2016). 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*) dan hukum dunia maya (*virtual world law*) (Putranti, 2010).

Penelitian ini menggunakan contoh kasus pada Polda Sumatera Barat, kejahatan dunia *cyber* hingga pertengahan 2020 mencapai 126 kasus. Kasus tersebut meliputi pencemaran nama baik, *hate speech, spam*, penyalahgunaan jaringan teknologi informasi, *carding* dan *illegal access*. Salah satu kejahatannya yaitu *Illegal Access* yang sangat tergantung pada pola hidup atau kemajuan teknologi yang berkembang di masyarakat yang lebih popular dengan istilah *cyber crime*.

Kejahatan *Illegal Access* yang terjadi dimana proses penyidikan yang dilakukan penyidik pada Ditreskrimsus Polda Sumbar pada sebuah akun *facebook* yang palsu atau bodong mengaku sebagai seorang pejabat pada salah satu instansi di Sumatera Barat. Melalui akun tersebut pelaku meminta uang kepada bendahara pada instansi tersebut dan kawan-kawan dekat pejabat tersebut. Bendahara pada instansi tersebut dan kawan-kawan dekat pejabat tersebut percaya karena profil pada akun sama dengan akun asli pejabat tersebut. Postingan dan bahasa yang digunakan juga disamakan dengan aslinya. Akibatnya para korban menderita kerugian sekitar Rp 60.000.000, - (Enam puluh juta Rupiah). Penyidik kesulitan untuk menentukan tersangka dan barang bukti yang digunakan pelaku saat melakukan kejahatannya, hal lain yang menjadi hambatan teknis penyidikan kejahatan ini adalah menentukan *locus* dan *tempus* kejahatannya, hal inilah yang menyebabkan proses pengungkapan kejahatan manipulasi elektronik sulit dilakukan.

Penelitian ini berbeda dengan penelitian sebelumnya seperti yang ditulis oleh Kornelius Benuf yang membahas mengenai hambatan formal penegakan hukum terhadap kejahatan pencurian data pribadi (Benuf, 2021). Penelitian ini secara spesifik akan membahas

permasalahan hambatan teknis dalam penyidikan tindak pidana manipulasi informasi elektronik dan/atau dokumen elektronik oleh penyidik.

B. Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif, adapun yang dimaksud pendekatan kualitatif adalah menguraikan kata demi kata secara sistematis sehingga dapat menemukan jawaban permasalahan. Jenis penelitian yang digunakan yaitu yuridis empiris, yakni suatu penelitian yang dilakukan dengan cara meneliti data primer sebagai sumber utama data penelitian (Amiruddin & Asikin, 2012). Data yang digunakan dalam penelitian ini adalah data primer dan didukung dengan data sekunder. Data primer yaitu berupa informasi terkait hambatan yang dihadapi penyidik dalam penyidikan tindak pidana manipulasi informasi elektronik. Data sekunder yaitu bahan pustaka yang mencakup dokumen-dokumen resmi, buku-buku perpustakaan, peraturan perundang-undangan, karya ilmiah, serta artikel-artikel yang berkaitan dengan materi penelitian (Depri, 2014). Data primer diperoleh melalui wawancara dan data sekunder diperoleh dari penelusuran pustaka *(library research)* yaitu dengan mencari, menginventarisasi, mencatat, mempelajari, dan mengutip data yang diperoleh dari artikel ilmiah, jurnal-jurnal, kamus hukum dan buku-buku yang mendukung dengan penelitian ini. Teknik analisis data yang digunakan dalam penelitian ini yaitu analisis kualitatif, yaitu menguraikan data secara komprehensif dalam bentuk kalimat yang teratur, runtun, logis, tidak tumpang tindih, dan selektif, sehingga memudahkan interpretasi data dan pemahaman hasil analisis.

C. Hasil dan Pembahasan

1. Hambatan Teknis dalam Penyidikan Tindak Pidana Manipulasi Informasi Elektronik

Unsur tindak pidana sangat penting untuk diketahui oleh setiap penegak hukum, khususnya penyidik tindak pidana. Unsur tindak pidana penting karena dari unsur-unsurnyalah suatu tindak pidana bisa diidentifikasi dan bisa dibuktikan. Sehingga dalam penegakan hukum pidana adalah hal yang penting untuk mengetahui dan menguraikan unsur tindak pidana (Arifah, 2011). Pada konteks penelitian ini tindak pidana yang dibahas adalah tindak pidana manipulasi informasi elektronik dan/atau dokumen elektronik merupakan perbuatan yang sangat tercela dan dapat merugikan banyak masyarakat. Tindak pidana manipulasi Informasi Elektronik dan/atau Dokumen Elektronik dilakukan melalui media elektronik, sehingga hal-hal yang menyangkut pembuktiannya akan sedikit banyak berbeda dengan tindak pidana biasa (Arief, 2006). Namun, seringkali tindakan tindak pidana manipulasi informasi elektronik dan/atau dokumen elektronik yang terjadi di masyarakat tidak dilaporkan ke pihak kepolisian, hal ini dikarenakan sering terjadinya kasus tersebut dan belum sadarnya masyarakat akan pentingnya penegakan hukum atas tindak pidana tersebut (Sugiarto, 2016). Sehingga membuat para pemilik akun bodong ini terus melakukan penipuan secara terus menerus. Pembuatan akun bodong yang mengatasnamakan orang lain dapat menimbulkan pencemaran nama baik bagi orang lain karena telah menyebarkan informasi bohong yang merugikan pihak lain.

Melihat realitas virtual yang sedang dijalani saat ini sangat membuka kemungkinan terjadinya tindak pindana pencurian data pribadi (Benuf, Mahmudah, & Priyono, 2019) serta tindakan-tindakan jahat lainnya yang sangat terbuka dilakukan oleh oknum yang tidak bertanggung jawab melalui sarana komunikasi atau dilakukan secara virtual, seperti misalnya penyebaran berita bohong *(Hoax),* penipuan dalam bertransaksi melalui *e-commerce*, penyebaran berita-berita atau konten-konten yang mengandung SARA, serta konten yang mengandung unsur asusila, bisa dilakukan secara mudah dan cepat di era virtualisasi seperti layaknya saat ini (Rumlus & Hartadi, 2020). Oleh karenanya mengingat sangat terbuka lebarnya kemungkinan terjadinya kejahatan di ruang virtual saat ini maka perlu peran pemerintah dalam mengatasi permasalahan tersebut demi tercapainya masyarakat yang tertib dan terlindungi oleh hukum.

Peran pemerintah ini dimaksudkan untuk mencegah penyebarluasan konten ilegal. Hal ini karena pemerintah memiliki kewenangan untuk melakukan pengawasan dan pengaturan serta bisa melakukan kriminalisasi terhadap perbuatan penyebarluasan konten ilegal di Indonesia (Hanim, 2011). Pentingnya peran Pemerintah dalam menanggulangi kejahatan di media elektronik dan kejahatan yang dilakukan secara virtual yaitu dengan menyusun politik hukum yang bersifat kolaboratif dengan menggunakan kewenangan dari Penyidik untuk mengumpulkan bukti-bukti terkait kejahatan yang sedang terjadi, selain itu dibutuhkan juga peran dari penyelenggara sistem elektronik di bawah kementerian informasi dan transaksi elektronik untuk mengetahui alur informasi dan transaksi yang terkait dengan tempat perbuatan jahat tersebut *(locus)* dan waktu terjadinya tindak kejahatan tersebut *(tempus)*. Peran-peran pemerintah tersebut bisa saling berkoordinasi dan berkolaborasi untuk segera memutus akses publik terhadap konten-konten kejahatan tersebut supaya bisa terwujud ketertiban di masyarakat Indoensia.

Berdasarkan Putusan Mahkamah Konstitusi Nomor SO/PUU-VII2OOS dan Nomor 2/PUUVII 2OO9, pada intinya menyatakan bahwa tindak pidana penghinaan dan pencemaran nama baik yang dilakukan dengan menggunakan sarana Elektronik bukan semata-mata sebagai tindak pidana umum namun merupakan delik aduan. Artinya harus ada pengadu terhadap konten tersebut baru bisa diproses secara hukum, hal ini deemi terciptanya keadilan, kepastian dan kemanfaatan hukum di Indonesia. Dijadikannya tindak pidana penghinaan dan pencemaran nama baik dalam bidang Informasi Elektronik dan Transaksi Elektronik sebagai delik aduan maka tanpa adanya aduan dari orang yang dirugikan maka kepolisian tidak bisa menindak tindak pidana tersebut (Satria, 2018).

Tindak Pidana manipulasi informasi elektronik dan/atau dokumen elektronik diatur pada Pasal 35 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik dan ancaman pidananya terdapat pada Pasal 51 dan 45 undang-undang tersebut. Adapun unsur-unsur yang diterapkan oleh penyidik adalah yang pertama unsur subjektif yaitu "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum", hal ini terpenuhi dengan adanya alat bukti yaitu keterangan saksi yang menyatakan telah mengirimkan sejumlah uang dikarenakan adanya whatsapp dengan seseorang yang mengaku sebagai Kombespol Joko Sadono, S.H., S.I.K., M.H dan Alat bukti lain adalah keterangan ahli dan bukti elektronik berupa *screenshoot* akun facebook mengatasnamakan Joko Sadono dengan URL Link https://www.facebook.com/joko.sadono.165. Semua alat bukti menunjukkan dugaan bahwa tindak pidana tersebut dilakukan oleh subjek hukum perorangan.

Setiap Orang, sesuai definisi Pasal 1 butir 21 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang dimaksud dengan Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum. Jadi yang dimaksud orang di sini adalah subjek hukum yang diakui dalam hukum Indonesia (Adhim, Mahmudah, & Benuf, 2020). Orang yang dimaksud adalah pelaku mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang mengandung muatan sebagaimana dimaksud di dalam Pasal-Pasal Undang-Undang Republik Indonesia Nomor 11/2008 tentang Informasi dan Transaksi Elektronik.

Yang Dengan Sengaja, unsur yang dimaksud "*yang dengan sengaja*" adalah adanya bukti suatu kehendak untuk mewujudkan unsur di dalam suatu delik menurut Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik adalah pelaku aktif atau yang terbukti melakukan tindakan yang dapat dimaknai sebagai suatu perbuatan hukum termasuk perbuatan secara teknis dalam penggunaan teknologi, namun dengan tanpa mempertimbangan motif dan alasannya – sebagaimana yang telah dirumuskan oleh Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan pelaku telah mengetahui atau menyadari atau menghendaki akibat dari perbuatan tersebut. Bukti kesengajaan antara lain dapat ditunjukkan dengan perbuatan Pelaku yang terekam ke dalam sistem elektronik, dari catatan aktivitas akun miliknya atau yang sedang dikuasainya atau

yang sedang digunakannya dan/atau yang dilaksanakan berulang kali sehingga diketahui oleh Saksi.

Selanjutnya adalah unsur Tanpa Hak, sedangkan yang dimaksud "*tanpa hak*" adalah suatu perbuatan yang tidak dilandasi suatu hak atau kewenangan berdasarkan Undang-Undang atau ijin dan alas hukum lain yang sah, termasuk apabila perbuatan tersebut dilakukan melampaui hak atau kewenangan yang diberikan oleh Undang-Undang atau ijin dan alas hukum lain yang sah, atau melanggar hak orang lain atau melawan hukum (Benuf et al., 2019). Pada contoh kasus yang terjadi secara subjektif unsur ini terbukti dilakukan oleh tersangka yang menjelaskan bahwa tersangka membuat akun facebook mengatasnamakan Kombespol Joko Sadono, S.H., S.I.K., M.H. tersebut sebanyak 2 (dua) buah akun *facebook.*

Unsur objektif yang diterapkan adalah "melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik", unsur ini sesuai dengan alat bukti keterangan saksi yang berteman pada akun facebook dan menerima pesan whatsapp seolah benar dari yang bersangkutan. Alat bukti lainnya adalah surat atau dokumen elektronik berupa Surat/dokumen elektronik *printout screenshot* percakapan whatsapp dengan seseorang yang mengaku sebagai Kombespol Joko Sadono, S.H., S.I.K., M.H.

Perbuatan Manipulasi, yaitu proses rekayasa melalui penambahan atau pengurangan atau penghilangan atau mengkaburkan atau menyembunyikan sebagian atau keseluruhan suatu realitas, kenyataan, fakta-fakta ataupun sejarah dan/atau material (benda) yang dilakukan dengan menggunakan alat sistem perancangan atau sebuah tata sistem nilai, tanpa disadari oleh pihak penerima informasi dan/atau dokumen elektronik; sehingga sesuatu itu akan seolah-olah menjadi memiliki makna, substansi/kandungan, yang berbeda dari aslinya (tidak otentik) atau diarahkan pada pengertian lain yang diinginkan oleh pengirim.

Perbuatan manipulasi tersebut dilakukan dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah adalah data yang otentik. Adanya persesuaian keterangan saksi, ahli, dokumen elektronik diketahui bahwa adanya facebook dan whatsapp palsu yang mengatasnamakan Kombespol Joko Sadono, S.H., S.I.K., M.H. yang mana diduga kuat Ganda Hirahman Wahyu memanipulasi dengan menciptakan Facebook dan whatsapp palsu tersebut mengatasnamakan Kombespol Joko Sadono, S.H., S.I.K., M.H. Selanjutnya unsur "dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik" sesuai dengan alat bukti keterangan saksi-saksi yang menduga informasi elektronik tersebut asli dan keterangan ahli.

Pasal 35 Undang Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik ini diatur secara alternatif, maksudnya cukup dibuktikan bahwa pelaku dengan sengaja melakukan salah satu atau beberapa dari perbuatan yang dimaksud. Melalui perbuatan-perbuatan ini maka muncul hak yang tidak sah bagi dirinya atau orang lain. Dimana penggunaan hak yang dimaksud adalah tanpa alas hukum atau kewenangan sehingga menjadi tidak sah atau melanggar hak orang lain. Pada perkara ini perbuatan yang dilakukan adalah manipulasi data.

Perbuatan tersangka juga dikaitkan dengan ketentuan Pasal 45 ayat (4) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik "Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman". Dimana unsur yang terpenuhi "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum". Berdasarkan keterangan saksi, ahli dan dokumen elektronik ditemukan adanya persesuaian bahwa tersangka atas nama Ganda Hirahman Wahyu Pgl Ganda menggunakan akun facebook dan whatsapp dengan mengatasnamakan Joko Sadono yang mana dengan facebook dan whatsapp tersebut tersangka meminta bantuan dari Yon Friadi untuk mengirimkan uang sebanyak Rp. 20.000.000,- (dua puluh juta rupiah) dan hal tersebut dikuatkan sendiri dengan

keterangan tersangka.

Unsur selanjutnya adalah “mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman”. Tersangka atas nama Ganda Hirahman Wahyu Pgl GANDA menerangkan bahwa motivasi tersangka membuat facebook dan whatsapp dengan mengatasnamakan Kombespol Joko Sadono, S.H., S.I.K., M.H. hanya untuk menakut-nakuti Syamsul Ridwan, dikarenakan niat tersangka menakut-nakuti Syamsul Ridwan tersebut berhasil maka tersangka menjadi keterusan dan mencoba mencari korban lainnya untuk memberikan sejumlah uang.

Ada permasalahan dalam penegakan hukum pidana terkait dengan Pasal-Pasal dalam UU ITE khususnya dengan frasa “mendistribusikan”, "mentransmisikan" dan frasa "membuat dapat diakses". Jika diuraikan satu-satu frasa tersebut yang mana dalam UU ITE menguraikan demikian; mendistribusikan" yaitu mengirimkan dan/atau menyebarkan Informasi Elektronik dan/ atau Dokumen Elektronik kepada banyak Orang atau berbagai pihak melalui Sistem Elektronik. Frasa ini menyangkut semakin menjadi luas penafsirannya ketika maknanya ditafsirkan secara umum, sehingga mengakibatkan setiap tindakan untuk mendistribusikan bisa dipahami secara luas. Selanjutnya frasa "mentransmisikan" adalah mengirimkan Informasi Elektronik dan/ atau Dokumen Elektronik yang ditujukan kepada satu pihak lain melalui Sistem Elektronik. Seterusnya tentang frasa "membuat dapat diakses" UU ITE menentukan bahwa semua perbuatan lain selain mendistribusikan dan mentransmisikan melalui Sistem Elektronik yang menyebabkan Informasi Elektronik dan/atau Dokumen Elektronik dapat diketahui pihak lain atau publik. Ketiga frasa tersebut telah memberikan makna yang luas sehingga setiap tindakan yang bisa mengakibatkan suatu konten kejahatan bisa dilihat orang lain karena tindakan kita sebagai pengguna media sosial maka bisa ditafsirkan bahwa kita ikut melakukan tindak kejahatan tersebut. Pengertian yang sangat luas tersebut di satu sisi menguntungkan bagi penegak hukum karena bisa menjerat siapapun yang terlibat dalam kejahatan tersebut, namun di sisi lain karena keluasan arti tersebut telah mengakibatkan frasa-faras tersebut menjadi multi tafsir. Sebagai contoh ketika ada konten yang mengandung asusila dalam postingan Instagram selanjutnya sebagai pengguna kita me-*like* postingan tersebut. Tindakan kita tersebut bisa dikategorikan sebagai tindak kejahatan bila mendasarkan pada pengertian dari frasa membuat dapat diakses, karena ketika di-*like* maka postingan tersebut akan muncul pada beranda *followers* kita.

Harus ada dukungan dari aparat penegak hukum terkait dengan proses digital pengelolaan inventarisasi barang, baik yang terjadi pada saat penulisan maupun pada saat pengelolaan inventarisasi pada saat pendistribusian. Dalam pengolahan data elektronik, diperlukan kata dan frase khusus untuk mencegah data digital tersebut rusak. Akibatnya, penyidik harus memahami peralatan elektronik awal pada komputer di TKP, pemeriksaan fisik setiap sektor TKP (*forensik imaging*), analisis sistem file sistem operasi Microsoft Windows, pencarian dan menemukan file yang telah dihapus atau diubah atau data yang tidak pernah disebarkan tetapi hanya dicetak (*files recovery)*, analisis perangkat bergerak (*mobile forensic*), analisis rekaman suara (*audio forensic*), dan prosedur terkait lainnya (forensik citra). *Cybercime* adalah jenis tulisan formal khusus yang metode penulisannya mungkin berbeda dengan penulisan formal.

Kasus c*ybercime* adalah suatu kasus yang memiliki kekhususan tersendiri dari kasus-kasus pidana umum lainnya, hal ini berpengaruh terhadap proses penyidikan yang khusus pula terhadap kasus *cybercrime.* Penyidik yang mempunyai wewenang khusus untuk melakukan proses penyidikan terhadap kasus *cybercrime* adalah reserse khususnya satuan *cybercrime*, adapun dasar hukum pelaksanaan wewenang tersebut yaitu undang-undang terkait dengan tindak pidana *cybercrime* di Indoensia. Penyidik yang tergabung dalam satuan *cybercrime* bertugas melakukan penyidikan terhadap tindak pidana *cybercrime* yang terjadi di Indonesia. Wewenang tersebut menjadikan penyidik berwenang untuk mengumpulkan alat bukti terkait dengan kasus

cybercrime tersebut. Pedoman alat bukti telah diatur dalam ketentuan Pasal 184 KUHAP, yang menentukan bahwa alat bukti adalah keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Susunan alat bukti tersebut telah menentukan kekuatan pembuktian suatu tindak pidana.

Penyidik dalam menyidik tindak pidana *cybercrime* alat bukti bisa berupa informasi elektronik dan dokumen elektronik yang bisa dihadirkan dalam persidangan bisa berupa tangkapan layar atau hasil cetakan *file*. Informasi dan dokumen elektronik tersebut bisa menjadi alat bukti yang sah dan digunakan sebagai dasar pertimbangan dalam putusan hakim jika diperoleh dari proses penyidikan yang sesuai dengan aturan dalam UU ITE. Informasi atau dokumen elektronik yang merupakan hasil penyidikan dan dicetak selanjutnya dihadirkan di muka sidang bisa menjadi alat bukti yang saah secara hukum. Alat bukti tersebut merupakan perluasan makna dari alat bukti yang selama ini diatur dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP) yang berlaku sebagai hukum positif di Indonesia dan dijadikan pedoman dalam menentukan alat bukti suatu tindak pidana. Hasil cetakan informasi atau dokumen elektronik tersebut yang dijadikan alat bukti berlaku sebagai alat bukti yang sah apabila setidaknya memenuhi persyaratan antara lain yaitu surat yang menurut undang-undang harus berbentuk tertulis, dan persyaratan yang lain yaitu dokumen atau informasi elektronik tersebut harus bersifat otentik karena dibuat oleh pejabat yang berwenang. Ada penjelasan lainnya yang mensyaratkan bahwa informasi atau dokumen elektronik tersebut bisa digunakan sebagai alat bukti yang sah menurut hukum apabila bisa diakses secara umum, bisa dijamin kebenarannya serta bisa didukung oleh ahli di bidang digital forensik.

Mengenai subjek tindak pidana dalam UU ITE telah ditentukan bahwa subjek yang kepadanya bisa dimintakan pertanggungjawaban terhadap tindak pidana yang berkaitan dengan kejahatan yang diatur dalam UU ITE adalah orang perorangan dan atau korporasi. Selanjutnya yang dimaksud orang perorangan adalah setiap orang yang sudah dewasa atau sudah menikah menurut undang-undang yang berlaku di Indonesia. Sedangkan yang dimaksud korporasi adalah setiap badan usaha yang berbentuk badan hukum dan yang bukan badan hukum. Selanjutnya di dalam ketentuan lain yang mengatur tentang subjek hukum orang perorangan ditentukan bahwa orang perorangan adalah setiap warga negara Indonesia, warga negara luar negeri, maupun badan hukum. Secara eksplisit UU ITE telah mengatur bahwa pertanggungjawaban hukum korporasi terkait tindak pidana yang diatur dalam UU ITE menganut sistem perumusan yang alternatif komulatif artinya bisa dipisah dan bisa disatukan unsur tindak pidananya. Sebagaimana diatur dalam Pasal 52 ayat (4) UU ITE. Hal yang menjadi penegasan terhadap pasal tersebut bahwa sifatnya mengandung pemberatan pidana. Mengenai jenis sanksi yang diatur dalam UU ITE bahwa terhadap tindak pidana yang berkaiatan dengan kejahatan yang diatur dalam UU ITE ditentukan 2 (dua) jenis sanksi yaitu sanksi pidana penjara bagi individu orang perorangan dan atau individu penanggungjawab dalam suatu korporasi serta pidana denda bagi orang perorangan dan atau korporasi. Hal lain yang menjadi permasalahan dalam penegakan hukumnya adalah kesulitan dalam menentukan siapa yang harus dimintakan pertanggungjawaban dalam suatu korporasi dalam konteks tindak pidana yang diatur dalam UU ITE, siapa yang harus bertanggungjawab, apakah pegawai yang notabenenya adalah orang yang disuruh atau diperintah oleh atasan dalam melaksanakan pekerjaannya di suatu perusahaan atau orang yang menyuruh lakukan tindakan tersebut. Saksi pidana denda yang diatur dalam UU ITE menentukan bahwa pidana penjara paling lama 12 tahun dan paling rendah 6 tahun, sedangkan sanksi pidana dendanya adalah maksimal 12 miliar rupiah dan minimal 600 (enam ratus) juta rupiah.

Tindak pidana yang dilakukan secara elektronik khususnya tindak pidana manipulasi elektronik dan atau dokumen elektronik, sering dilakukan dengan menggunakan paksaan atau tipu muslihat terhadap korban. Berbagai tindakan yang sering dilakukan adalah dengan modus yang hampir serupa yaitu seperti memanfaatkan secara melawan hukum perkembangan informasi elektronik. Tindakan pidana yang berupa manipulasi informasi dan dokumen

elektronik tersebut ditujukan untuk mencuri atau membobol data dengan cara menipu korban. Misalnya yang sering terjadi adalah menyalahgunakan data atau dokumen pribadi korban untuk tujuan mendapatkan keuntungan dari tindakannya tersebut di satu sisi, yaitu dari sisi korban tindakan manipulasi data atau dokumen elektronik yang dialami akan menimbulkan kerugian materil dan kerugian imateril. Tindakan-tindakan manipulasi data atau dokumen elektronik tersebut antara lain seperti: kejahatan kartu kredit antara lain yaitu *Phising, Carding, Hacking, Skimming* dan *Ekstrapolasi,* tindakan-tindakan jahat tersebut yang sering terjadi di masyarakat Indonesia (Sitompul, 2001).

Pada kasus *cybercrime* secara spesifik tentang tindak pidana manipulasi data dan/atau dokumen elektronik dalam praktik di lapangan ternyata pada tahap penyidikan terhadap kasus tersebut, sering kali penyidik diperhadapkan pada hambatan teknis yang sedikit banyak berpengaruh terhadap nilai pembuktian ketika kasus tindak pidana manipulasi data dan/atau dokumen elektronik tersebut dipersidangkan. Hambatan teknis tersebut lebih kepada sarana dan prasarana yang mendukung proses penemuan alat bukti untuk membuktikan dan membuat terang suatu tindak pidana manipulasi data dan/atau dokumen elektronik (Mulyadi, 2010). Selain itu hambatan teknis yang dihadapi seorang penyidik dalam menangani tindak pidana manipulasi data dan/atau dokumen elektronik adalah menemukan tersangka, menentukan tempat kejadian *(lucus)* tindak pidananya dan kesulitan dalam menentukan waktu terjadinya *(tempus)* tindak pidana manipulasi data dan/atau dokumen elektronik. Hambatan teknis lainnya yaitu banyak teknologi yang dirancang dengan sistem keamanan yang sulit untuk dibaca atau diketahui oleh orang lain dengan menggunakan kata sandi atau password untuk bisa masuk ke dalam sistem elektronik tersebut. Sehingga kesulitan tersebut yang menjadi hambatan teknis penyidik dalam menangani tindak pidana manipulasi data dan/atau dokumen elektronik, dan dibutuhkannya sumber daya manusia yang mumpuni dan peralatan komputer forensik yang baik.

Terkait dengan penentuan *locus* tindak pidana yang dilakukan secara elektronik seperti halnya tindak pidana manipulasi data dan/atau dokumen elektronik terutama mengenai kompetensi kepolisian daerah mana yang berwenang memeriksa tindak pidana manipulasi data dan/atau dokumen elektronik tersebut. Selain itu mengenai penentuan *tempus* dalam tindak pidana manipulasi data dan/atau dokumen elektronik menjadi permasalahan sendiri karena tindakan pidana tersebut apabila tidak ditangani secara patut oleh penyidik yang mumpuni maka kesulitan menentukan *tempus* dalam tindak pidana manipulasi data dan/atau dokumen elektronik akan terjadi (Purnomo & Soponyono, 2015).

Seperti hal lainnya yang terkait dengan penyidikan tindak pidana manipulasi data dan/atau dokumen elektronik dari hasil pencarian terjauh hanya mengembalikan alamat IP pelaku dan komputer yang digunakan. Ada banyak masalah dalam penyitaan bukti karena pengadu biasanya terlalu lambat untuk melapor, menyebabkan data penyerangan dihapus dari *log server*, yang biasanya terjadi pada kasus pelanggaran, sehingga sangat sulit bagi penyelidik untuk menemukan kesulitannya adalah *log* statistik yang terdapat di server, karena server biasanya otomatis. Hapus *log* yang ada untuk mengurangi beban server. Oleh karena itu, penyidik mungkin tidak mendapatkan data yang perlu dijadikan bukti, padahal data *log* statistik merupakan salah satu alat bukti yang paling penting.

Pemeriksaan saksi dan korban menghadapi banyak kendala karena tidak ada saksi yang melihat tindak pidana (*testimonium de auditu*) pada saat tindak pidana itu terjadi atau dilakukan. Mereka baru mengetahuinya setelah kejadian itu terjadi, karena mereka merasakan dampak penyerangan yang telah dilakukan. Saksi ahli berperan sangat penting dalam memberikan keterangan dalam perkara pidana yang berkaitan dengan manipulasi informasi dan/atau dokumen elektronik, karena yang terjadi di dunia maya memerlukan keahlian dan pengetahuan khusus. Dalam tindak pidana manipulasi informasi dan/atau dokumen elektronik, saksi ahli dapat terdiri dari lebih dari satu saksi ahli, tergantung pada permasalahan yang dihadapi, seperti dalam

perkara pembelaan, selain saksi ahli yang mahir dalam desain grafis dan saksi ahli yang mengerti masalah jaringan dan saksi juga membutuhkan ahli program.

Setelah dilakukan investigasi secara menyeluruh, dan permasalahan yang ditemukan berupa berkas adalah masalah pembuktian, karena tidak ada kesamaan persepsi di kalangan penegak hukum bahwa bukti digital adalah bukti manipulasi informasi dan/atau kasus kriminal. Dokumen elektronik yang definisinya tidak jelas, karena bukti digital tidak selalu dalam bentuk fisik yang sebenarnya. Misalnya dalam kasus pembunuhan, pisau adalah alat bukti utama untuk melakukan pembunuhan, sedangkan dalam kejahatan komputer, komputer adalah alat bukti utama, tetapi komputer hanya bersifat fisik, sedangkan yang terpenting adalah data yang ada di komputer, *disk* dalam bentuk *file*, yang bila dicetak sebenarnya membutuhkan banyak kertas untuk dituangkan ke atasnya, dapatkah barang bukti dalam bentuk CD, sampai saat ini belum ada undang-undang yang mengatur tentang bentuk barang bukti digital yang diajukan sebagai alat bukti di persidangan.

Hambatan lain bagi penegak hukum untuk menggunakan alat bukti digital melalui forensik komputer adalah lemahnya digital forensik, karena Lab Komputer Forensik Polda Sumbar belum tersedia. Seperti disebutkan di atas, pemeriksaan alat bukti digital dilakukan oleh para ahli. Misalnya, laboratorium forensik yang digunakan berada di wilayah hukum Polda Sumbar. Laboratorium forensik digital tidak dimiliki Polri di semua daerah. Keberadaannya sangat penting untuk mencegah dan menangani kasus-kasus yang berkaitan dengan kejahatan dunia maya. Kendala lain adalah kejahatan dunia maya yang seringkali melibatkan negara (*borderless*) dan tidak mengenal batas negara serta berada di luar yurisdiksi hukum Indonesia sehingga menyulitkan penyidik atau Interpol untuk mengambil tindakan dan sangat baik dalam mengejar pelaku kejahatan/operator. Komisi dari semua jenis kejahatan. Hal ini terkait dengan kurangnya sumber daya manusia dalam hal pengetahuan teknologi digital dan kode digital di tingkat Polri, kejaksaan dan hakim, sehingga jelas ada masalah dalam menangani kejahatan dunia maya. Selain itu, undang-undang kejahatan dunia maya masih lemah, faktor yang dapat digunakan penjahat dunia maya untuk menemukan celah hukum untuk menghindari hukum.

Upaya digitalisasi bukti dengan menggunakan komputer forensik melibatkan pertukaran informasi dan kesaksian dari detektif polisi dan penyidik dari negara lain, yang dapat digunakan sebagai bukti untuk meyakinkan juri akan kebenaran kasus tersebut dilakukan oleh terdakwa. Oleh karena itu, penegakan hukum memerlukan kerja sama internasional (Aqimuddin, 2012). Selain itu, hakim dapat meninjau perkara berdasarkan bukti-bukti, dengan menggunakan keterangan, keterangan dan pendapat yang tersedia dari para ahli telematika di bidangnya. Mendeklarasikan dan mengamankan bukti digital untuk analisis jangka panjang sehingga dapat dimintai pertanggungjawaban. Dengan pendekatan teknologi, aparat penegak hukum dan masyarakat dunia tidak dapat menyelesaikan permasalahan melalui pemanfaatan teknologi dalam pemrosesan perkara pidana.

D. Simpulan dan Saran

Pada proses penegakan hukum terhadap tindak pidana *cybercrime* menghadapi hambatan teknis, khasnya pada tahap pemeriksaan saksi dan korban pada tahap penyidikan oleh reserse khususnya satuan *cybercrime.* Hal ini dikarenakan seorang saksi yang seharusnya melihat, mendengar atau mengetahui secara *realtime* suatu tindak pidana tetapi karena sifat tindak pidana manipulasi data dan atau dokumen elektronik adalah dilakukan secara elektronik maka saksi hanya mengetahui setelah tindak pidana tersebut terjadi. Selain itu data serangan di *log server* terkadang sudah dihapus biasanya terjadi pada kasus *deface*, hal ini menyebabkan Penyidik menemui hambatan teknis dalam menemukan faktanya. Saran agar proses penyidikan tindak pidana manipulasi data dan/atau dokumen elektronik tidak menghadapi hambatan teknis lagi yaitu dengan kerjasama antara penyidik Polri dengan penyidik dari negara lain untuk saling bertukar informasi dan barang bukti, sehingga barang bukti tersebut dapat digunakan sebagai alat

bukti untuk membangun keyakinan hakim akan kebenaran tindak pidana yang dilakukan oleh terdakwa. Selanjutnya, informasi atau pendapat dari profesional TI yang ahli di bidangnya harus digunakan, dan informasi yang diperoleh dapat diperhitungkan ketika hakim memutuskan kasus berdasarkan bukti yang tersedia.

DAFTAR PUSTAKA

Adhim, N., Mahmudah, S., & Benuf, K. (2020). Telaah Yuridis Pemberian Hak Guna Bangunan Kepada Persekutuan Komanditer (CV). *Justitia Et Pax*, *36*(1), 51–68. https://doi.org/10.24002/jep.v36i1.3070

Amiruddin, A., & Asikin, Z. (2012). *Pengantar Metode Penelitian Hukum*. Jakarta: Rajagrafindo Persada.

Aqimuddin, E. A. (2012). Tanggung Jawab Negara Terhadap Tindak Pidana Internasional. *Negara Hukum*, *12*(2), 12–29.

Arief, B. N. (2006). *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*. Jakarta: Rajagrafindo Persada.

Arifah, D. A. (2011). Kasus Cybercrime Di Indonesia. *Jurnal Bisnis Dan Ekonomi*, *18*(2), 185–195. Retrieved from https://www.unisbank.ac.id/ojs/index.php/fe3/article/view/2099

Benuf, K. (2021). Hambatan Formal Penegakan Hukum Pidana Terhadap Kejahatan Pencurian Data Pribadi. *Majalah Hukum Nasional*, *51*(2), 261–279. Retrieved from http://mhn.bphn.go.id/index.php/MHN/article/view/148

Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). Perlindungan Hukum terhadap Keamanan Data Konsumen Financial Technology di Indonesia. *Refleksi Hukum: Jurnal Ilmu Hukum*, *3*(2), 145–160. https://doi.org/10.24246/jrh.2019.v3.i2.p145-160

Hanim, L. (2011). Pengaruh Perkembangan Teknologi Informasi Terhadap Keabsahan Perjanjian Dalam Perdagangan Secara Elektronik (E-Commerce) di Era Globalisasi. *Jurnal Dinamika Hukum*, *11*(Edisi Khusus), 59–66. https://doi.org/10.20884/1.jdh.2011.11.Edsus.262

Hill, J. B., & Marion, N. E. (2016). *Introduction to Cybercrime-Computer Crimes, Laws, and Policing in the 21st Century*. Santa Barbara, California: Praeger.

Mulyadi, L. (2010). Pembuktian Terbalik Kasus Korupsi. *Jurnal Mahkamah Agung*, *13*(1), 1–3.

Purnomo, M. A., & Soponyono, E. (2015). Rekonseptualisasi Penyidikan Tindak Pidana Korupsi Oleh Polri Dalam Rangka Efektifitas Pemberantasan Tindak Pidana Korupsi. *Law Reform*, *11*(2), 230–240. https://doi.org/10.14710/lr.v11i2.15771

Putranti, I. R. (2010). *Lisensi Copyleft dan Perlindungan Open Source Software*. Yogyakarta: Gallery Ilmu.

Rahardjo, A. (2002). *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. Bandung: Citra Aditya Bakti.

Remmelink, J. (2003). *Hukum Pidana : Komentar Atas Pasal-Pasal Terpenting Dari Kitab Undang-Undang Hukum Pidana Belanda Dan Padanannya Dalam Kitab Undang-Undang Hukum Pidana Indonesia*. Jakarata: Gramedia Pustaka Utama.

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. *Jurnal HAM*, *11*(2), 285–299. https://doi.org/10.30641/ham.2020.11.285-

299

Satria, H. (2018). Restorative Justice: Paradigma Baru Peradilan Pidana. *Jurnal Media Hukum*, *25*(1), 111–123. https://doi.org/10.18196/jmh.2018.0107.111-123

Sitompul, A. (2001). *Hukum Internet Pengenalan Mengenai Masalah Hukum di Cyberspace* (1st ed.). Bandung: Citra Aditya Bakti.

Sonata, D. L. (2014). Metode Penelitian Hukum Normatif Dan Empiris: Karakteristik Khas Dari Metode Meneliti Hukum. *Fiat Justisia: Jurnal Ilmu Hukum*, *8*(1), 15–35. https://doi.org/10.25041/fiatjustisia.v8no1.283

Sugiarto, E. (2016). Implikasi Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 Terhadap Informasi Elektronik Dan/Atau Dokumen Elektronik Dan/Atau Hasil Cetaknya Sebagai Alat Bukti Dalam Perkara Perdata. *Rechtidee*, *11*(2), 182–199. https://doi.org/10.21107/ri.v11i2.2171