

SCREENSHOT FACEBOOK SEBAGAI ALAT BUKTI TINDAK PIDANA PENCIPTAAN INFORMASI ELEKTRONIK PALSU

Clarisa Permata Hariono Putri

Fakultas Hukum Universitas Surabaya | clarisapermatahp@gmail.com

Hwian Christianto

Fakultas Hukum Universitas Surabaya | hw_christianto@staff.ubaya.ac.id

Anton Hendrik Samudra

Fakultas Hukum Universitas Surabaya | antonhendrik@staff.ubaya.ac.id

ARTICLE INFO

Article history:

Received

30 Mei 2020

Revised

6 Juli 2020

Accepted

15 April 2021

Kata-kata Kunci:

Alat Bukti; Screenshot;
Tindak Pidana
Penciptaan Informasi
Elektronik Palsu.

Keywords:

Evidence; Screenshot;
The Crime of Creating
False Electronic
Information.

Abstrak

Penelitian ini bertujuan untuk mengetahui pembuktian tindak pidana penciptaan informasi elektronik palsu menggunakan *screenshot facebook* sebagai alat bukti berdasarkan Undang – Undang Informasi dan Transaksi Elektronik dan perubahannya, serta peraturan terkait dengan melihat pada kasus yang ada dalam putusan No. 43/Pid.Sus/2018/PN Mjl. Metode penelitian yang digunakan adalah metode yuridis normatif yaitu suatu metode penelitian yang dilakukan dengan studi kepustakaan. Hasil penelitian ini adalah *screenshot facebook* tidak cukup untuk dapat digunakan sebagai alat bukti tindak pidana penciptaan informasi elektronik palsu karena masih diragukan keabsahannya secara materiil sebagai alat bukti dan penerapannya sebagai alat bukti masih kurang memenuhi dan membuktikan tiap unsur tindak pidana penciptaan informasi elektronik palsu. Oleh karena itu perlu digunakan alat bukti lain dalam mekanisme pembuktian tindak pidana penciptaan informasi elektronik palsu dan perlunya diadakan pengaturan penyitaan atas akun.

Abstract

This study aims to determine the validity of Facebook screenshots as a proof of the false electronic information crime based on the perspective of the Information and Electronic Transactions Act and its amendments Act also other related regulations by looking at the case in decision number 43 / Pid.Sus / 2018 / PN Mjl. The used research method is a normativ juridical method that carries out with literature study. This research results that Facebook screenshots are not sufficient to be used as evidence in false electronic information crimes since the validity of the Facebook screenshots as evidence is doubtful substantively. Moreover, the application does not fulfill all elements of the false electronic information crime. In conclusion, it is necessary to use other evidence in proving the false electronic information crime. Also, a rule regarding the confiscation of social media accounts is needed.

PENDAHULUAN

Pembuktian secara sederhana dapat dimaknai sebagai ketentuan-ketentuan yang berisi penggarisan dan pedoman tentang cara-cara yang dibenarkan undang-undang untuk membuktikan kesalahan yang didakwakan kepada terdakwa.¹ Dalam hukum acara pidana, pembuktian adalah hal yang penting atau esensial karena terkait penentuan nasib seseorang, yang dalam hal ini adalah terdakwa. Seorang terdakwa dinyatakan bersalah atau tidak sebagaimana surat dakwaan ditentukan dengan pembuktian.² Sebagaimana yang dapat diketahui pula, dalam hukum acara pidana, kebenaran yang hendak dicapai adalah kebenaran materiil atau kebenaran substantif. Untuk mencapai kebenaran tersebut, maka dalam tiap-tiap perkara pidana atau dalam tiap kejahatan yang terjadi, diperlukan adanya bukti yang sah menurut undang-undang.³

Bukti yang sah menurut undang-undang dalam hukum acara pidana, mengacu pada ketentuan mengenai jenis alat bukti yang telah diatur dalam ketentuan hukum pidana formil yaitu Pasal 184 Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (selanjutnya disebut dengan KUHAP). Sebagaimana yang dikatakan oleh Alfian Mardiansyah, jenis-jenis alat bukti yang sah dalam KUHAP, diatur secara limitatif yang meliputi keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa.⁴ Namun sebagaimana yang telah diatur dan dapat dilihat dalam Pasal 284 ayat (2) KUHAP, dapat dipahami bahwa KUHAP membuka peluang adanya kemungkinan pengesampingan aturan KUHAP oleh undang-undang pidana formil yang sifatnya lebih khusus.⁵ Hal ini tentunya mungkin saja terjadi, mengingat dalam hukum dikenal adanya prinsip *lex specialist derogat legi generalis* yang pada dasarnya memberikan makna bahwa aturan hukum yang khusus mengesampingkan atau dapat “mengalahkan” aturan hukum yang sifatnya lebih umum.

Dalam hal ini, salah satu undang-undang tersebut adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut dengan UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut dengan Perubahan Atas UU ITE). UU ITE dan Perubahan atas UU ITE merupakan undang-undang yang bukan hanya mengatur hukum pidana materiil sebagai substansi dalam undang-undangnya, seperti pengaturan mengenai jenis kejahatan atau tindak pidana dalam bidang teknologi informasi, namun mengatur juga hukum formil sebagai *lex specialis* seperti mengatur mengenai jenis alat bukti elektronik yang belum diatur dalam KUHAP, yaitu alat bukti informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya yang dapat ditemui dalam Pasal 5 UU ITE.

¹ M. Yahya Harahap, *Pembahasan dan Penerapan KUHAP* (Jilid II, Pustaka Kartini 1993) 793.

² Edmon Makarim, *Kompilasi Hukum Telematika* (PT. RajaGrafindo Persada 2004) 419.

³ Mohammad Nurul Huda, 'Pentingnya Alat Bukti Dalam Pembuktian Minim Saksi (The Importance of The Evidence in Proof of Minimal Witness)' (2017) 1 (2) *Voice Justisia* 95, 98.

⁴ Alfian Mardiansyah, 'Mekanisme Pembuktian Dalam Perkara Tindak Pidana Siber (The Verification Mechanisms In The Event Of Cyber Crime)' (2015) 12 (4) *Jurnal Legislasi Indonesia* 11.

⁵ Anton Hendrik Samudra, 'Modus Operandi dan Problematika Penanggulangan Tindak Pidana Penipuan Daring' (2019) 31 (1) *Mimbar Hukum* 59,72.

Secara umum, penggunaan bukti elektronik yang diatur dalam UU ITE sebagai bukti di sidang pengadilan memicu kekhawatiran bahwa saat diperlukan sebagai pembuktian di sidang pengadilan, kondisi bukti tersebut dapat tidak sesuai atau tidak sama dengan kondisi awalnya. Permasalahan dalam penggunaan bukti elektronik dalam pembuktian di sidang pengadilan ini dipicu dengan kondisi bukti elektronik yang rawan untuk diubah, dihapus, *dicopy*, maupun dipindahkan.⁶

Berkaitan dengan bukti elektronik tersebut, pada tahun 2017 terdapat suatu kasus hukum yang terjadi di Majalengka yang telah diputus berdasarkan putusan No. 43/Pid.Sus/2018/PN Mjl yang diawali dengan perbuatan AS yang membuat akun *facebook* atas nama "ADE" yang menggunakan nama, identitas dan foto dari AN, karena ingin membalas dendam pada AN. Akun tersebut dipergunakan untuk mencari dan menghina teman-teman AN sehingga teman-teman AN mengira bahwa perbuatan tersebut dilakukan oleh AN. Berkaitan dengan hal tersebut, A salah satu teman dari AN menemui AN dan menyampaikan perihal status *facebooknya* yang menerima kata-kata penghinaan dari akun *facebook* atas nama AN. AN kemudian menduga bahwa perbuatan tersebut dilakukan oleh AS karena sebelumnya memiliki permasalahan pribadi dengan AS. Ketika AN menemui AS, AS pada akhirnya mengakuinya. Berkaitan dengan hal tersebut, AS didakwa dengan dakwaan alternatif oleh Jaksa Penuntut Umum dengan dakwaan pertama yaitu Pasal 51 ayat (1) jo. Pasal 35 UU ITE atau dakwaan kedua Pasal 45 ayat (1) jo. Pasal 27 ayat (3) UU ITE. Pada proses pembuktian, Jaksa Penuntut Umum mengajukan alat bukti keterangan saksi sejumlah 4 orang, keterangan ahli sejumlah 2 orang dan barang bukti antara lain 1 buah telepon genggam, 2 buah nomor kartu dan 1 buah CD berisi *screenshot* hasil postingan akun *facebook* atas nama AN yang menunjukkan adanya akun atas nama "ADE" yang menggunakan nama, identitas dan foto AN, yang menuliskan kata-kata menghina pada beberapa akun, yang dalam hal ini adalah akun dari teman-teman AN. Pada akhirnya berdasarkan putusan No. 43/Pid.Sus/2018/PN Mjl yang diperoleh dari direktori putusan Mahkamah Agung Republik Indonesia, dapat diketahui bahwa AS diputus bersalah melakukan tindak pidana penciptaan informasi elektronik palsu sebagaimana dakwaan pertama berdasarkan Pasal 51 ayat (1) jo. Pasal 35 UU ITE.

Berkaitan dengan latar belakang yang berasal dari kasus hukum di Majalengka tersebut, terdapat satu bukti yang digunakan oleh Jaksa Penuntut Umum yang menarik untuk dikaji lebih mendalam melalui penelitian hukum ini, yaitu bukti *screenshot facebook*. Dalam hal ini penelitian akan dilakukan secara lebih mendalam untuk membahas mengenai *screenshot facebook* yang digunakan sebagai alat bukti, terbatas untuk pembuktian tindak pidana penciptaan informasi elektronik palsu, melalui rumusan masalah yakni: 1. Apakah kedudukan *Screenshot Facebook* sebagai alat bukti pada tindak pidana penciptaan informasi elektronik palsu ditinjau dari UU ITE dan Perubahan atas UU ITE? 2. Bagaimanakah mekanisme pembuktian *screenshot facebook* sebagai alat bukti pada tindak pidana penciptaan informasi elektronik palsu ditinjau dari UU ITE dan Perubahan atas UU ITE?

Adapun metode penelitian yang digunakan untuk membahas rumusan masalah tersebut adalah dengan menggunakan metode penelitian hukum yuridis

⁶ Sutarman, *Cybercrime Modus Operandi dan Penanggulangannya* (Laksbang Pressindo 2007)

normatif. Metode penelitian ini didasari dengan melakukan studi kepustakaan pada berbagai bahan hukum, baik menggunakan bahan hukum primer seperti peraturan perundang-undangan, maupun bahan hukum lainnya yaitu literatur-literatur lainnya yang terkait dengan permasalahan hukum yang akan diteliti. Berkaitan dengan hal tersebut, maka pendekatan masalah yang digunakan dalam penelitian ini adalah menggunakan pendekatan undang-undang (*statute approach*) yang dilakukan dengan menelaah semua undang-undang maupun regulasi yang terkait dengan isu hukum yang sedang ditangani. Selain itu digunakan pendekatan konseptual (*conceptual approach*) yang merupakan suatu pendekatan yang didasari dengan doktrin atau pandangan yang ada dan berkembang dalam ilmu hukum.

Bahan hukum yang digunakan dalam penelitian ini meliputi bahan hukum primer yaitu peraturan perundang-undangan antara lain Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana, serta Peraturan Menteri Komunikasi dan Informatika Nomor 7 Tahun 2016 tentang Administrasi Penyidikan dan Penindakan Tindak Pidana di Bidang Teknologi Informasi dan Transaksi Elektronik (selanjutnya disebut Permenkominfo No. 7 Tahun 2016) dan bahan hukum sekunder meliputi segala literatur yang terkait dengan hukum siber dan hukum acara pidana.

PEMBAHASAN

Kedudukan Screenshot Facebook sebagai Alat Bukti Tindak Pidana Penciptaan Informasi Elektronik Palsu Ditinjau Dari UU ITE dan Perubahan atas UU ITE

Secara umum, ketentuan mengenai hukum acara pidana diatur dalam KUHAP. Namun, walaupun pengaturan mengenai hukum acara pidana telah diatur dalam KUHAP, terdapat ketentuan-ketentuan lain sebagai *lex specialis* dari KUHAP. Dalam hal ini, sebagaimana yang dinyatakan oleh Anton Hendrik Samudra, hal tersebut dimungkinkan dengan adanya ketentuan dalam Pasal 284 ayat (2) KUHAP yang membuka peluang adanya pengesampingan aturan KUHAP oleh undang-undang pidana formil yang sifatnya lebih khusus.⁷ Berkaitan dengan hal tersebut, maka UU ITE dan Perubahan Atas UU ITE, merupakan salah satu ketentuan lain yang dapat termasuk sebagai *lex specialis* dari KUHAP. Hal tersebut dikarenakan secara umum UU ITE mengatur mengenai informasi dan transaksi elektronik dan perbuatan yang dilarang, namun juga mengatur mengenai hal yang berhubungan dengan pembuktian yaitu mengatur mengenai alat bukti lain sebagai perluasan alat bukti dalam KUHAP.⁸

Adapun ketentuan mengenai jenis alat bukti yang digunakan pada penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut UU ITE dapat didasarkan Pada Pasal 44 UU ITE yang sebenarnya mengacu pada jenis alat bukti yang diatur dalam Pasal 184 yang meliputi keterangan saksi, keterangan ahli, surat,

⁷ Samudra (n 5).

⁸ Nur Laili Isma & Arima Koyimatun, 'Kekuatan Pembuktian Alat Bukti Informasi Elektronik Pada Dokumen Elektronik Serta Hasil Cetaknya Dalam Pembuktian Tindak Pidana' (2014) 1 (2) Jurnal Penelitian Hukum 109, 110.

petunjuk, dan keterangan terdakwa, serta juga dapat mengacu pada jenis alat bukti yang diatur dalam Pasal 5 UU ITE yang meliputi informasi elektronik dan/atau dokumen elektronik, termasuk juga hasil cetak dari informasi elektronik dan/atau dokumen elektronik.

Membahas mengenai alat bukti pasti bukan hanya membahas mengenai bentuk atau jenis dari alat bukti yang dapat digunakan dalam pembuktian dalam persidangan. Namun dalam hal ini penting juga membahas mengenai keabsahan alat bukti tersebut untuk dipergunakan di persidangan. Hal ini penting karena penggunaan alat bukti dalam pembuktian di persidangan tidak hanya didasarkan dari apakah telah sesuai atau memenuhi bentuk atau jenis alat bukti yang diatur dalam peraturan perundang-undangan, namun apakah alat bukti tersebut telah sah sebagai suatu alat bukti yang berimplikasi pada dapat digunakannya hal tersebut sebagai alat bukti di persidangan.

Terkait dengan hal tersebut, informasi elektronik dan/atau dokumen elektronik yang diakui eksistensinya sebagai alat bukti yaitu sebagai jenis alat bukti elektronik sesuai Pasal 44 UU ITE yang mengacu pada Pasal 5 UU ITE juga memiliki syarat keabsahan alat bukti agar dapat benar-benar digunakan dalam pembuktian tindak pidana. Menurut Josua Sitompul, terdapat dua jenis syarat keabsahan alat bukti elektronik yaitu syarat materiil dan syarat formil. Syarat materiil adalah ketentuan atau syarat yang berkaitan untuk menjamin keutuhan, ketersediaan, keamanan, keotentikan, dan keteraksesan informasi atau dokumen elektronik dalam proses penyidikan, penuntutan dan pemeriksaan di sidang pengadilan. Syarat materiil dari bukti elektronik ini dapat ditemui dalam Pasal 5 ayat (3) UU ITE yang pada intinya menyatakan bahwa suatu informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam UU ITE. Ketentuan mengenai sistem elektronik pada UU ITE diatur dalam Pasal 15 hingga Pasal 16 UU ITE. Dari ketentuan itu, dapat dipahami bahwa, secara materiil, penggunaan informasi elektronik dan/atau dokumen elektronik sebagai alat bukti elektronik dianggap sah apabila menggunakan sistem elektronik yang sesuai dengan Pasal 15 dan Pasal 16 UU ITE. Selain terdapat dalam Pasal 5 ayat (3), syarat materiil juga terdapat dan terlihat dalam Pasal 6 UU ITE yang pada intinya menyatakan bahwa informasi elektronik atau dokumen elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Adapun untuk syarat formil dari alat bukti elektronik diatur dan terlihat dalam Pasal 5 ayat (4) UU ITE yang pada intinya menyatakan mengenai bentuk atau jenis informasi elektronik dan/atau dokumen elektronik yang tidak berlaku atau tidak dapat digunakan sebagai alat bukti, maupun juga Pasal 43 ayat (3) dan Pasal 43 ayat (4) UU ITE mengenai penggeledahan dan penyitaan dari sistem elektronik.⁹

Selain itu, mengacu pada Putusan Mahkamah Konstitusi (MK) No. 20/PUU-XIV/2016, sebenarnya terdapat hal lain yang juga menentukan keabsahan dari alat bukti elektronik. Hal tersebut nampak dalam amar putusan MK yang pada intinya menyebutkan bahwa, “Frasa Informasi Elektronik dan/atau Dokumen Elektronik”

⁹ Sitompul, *Cyberspace Cybercrimes Cyberlaw Tinjauan Aspek Hukum Pidana* (PT Tatanusa 2012) 282-286.

dalam Pasal 5 ayat (1) dan ayat (2) serta Pasal 44 huruf b UU ITE bertentangan dengan UUD 1945 dan tidak mempunyai kekuatan hukum mengikat sepanjang tidak dimaknai khususnya frasa “Informasi Elektronik dan/atau Dokumen Elektronik sebagai alat bukti dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang sebagaimana ditentukan dalam Pasal 31 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik”.¹⁰ Dari ketentuan tersebut, sebenarnya dapat dipahami bahwa, suatu informasi elektronik dan/atau dokumen elektronik dapat digunakan sebagai alat bukti elektronik di persidangan apabila ada permintaan dari penegak hukum. Atau dengan kata lain, secara *a contrario* dapat dimaknai bahwa implikasi atau dampak dari adanya putusan ini adalah apabila tidak ada permintaan dari aparat penegak hukum, maka alat bukti elektronik tersebut tidak sah atau tidak memiliki keabsahan.¹¹

Seperti yang telah diketahui bahwa, salah satu bukti yang digunakan oleh Jaksa Penuntut Umum dalam kasus hukum yang terjadi di Majalengka merupakan bukti *screenshot facebook* yang dimasukkan dalam satu buah CD. Berkaitan dengan hal tersebut, maka bila melihat ketentuan Pasal 44 UU ITE yang mengacu pada ketentuan Pasal 184 KUHAP dan Pasal 5 UU ITE, *screenshot facebook* tersebut sebenarnya dapat dikategorikan sebagai alat bukti informasi elektronik berdasarkan Pasal 5 UU ITE. Hal tersebut dikarenakan, hakikat dari *screenshot facebook* merupakan suatu gambar, yang dalam hal ini adalah suatu gambar tampilan yang diambil dari layar monitor, baik layar monitor komputer, *tablet PC*, dan *smartphone*.¹² Bila pengertian *screenshot* tersebut dikaitkan dengan pengertian informasi elektronik dalam Pasal 1 angka 1 UU ITE yang menyatakan bahwa, “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.”, maka dapat dipahami bahwa salah satu data elektronik yang termasuk dalam pengertian informasi elektronik adalah gambar sehingga *screenshot facebook* yang merupakan suatu gambar dapat dimasukkan dalam jenis alat bukti informasi elektronik. Dalam hal ini, *screenshot facebook* tersebut merupakan alat bukti informasi elektronik dalam bentuk original, dikarenakan disimpan secara elektronik dalam satu buah CD. Bila dijadikan dalam bentuk *print out*, dapat pula masuk dalam jenis alat bukti hasil cetak informasi elektronik.

Namun, kedudukan *screenshot facebook* sebagai alat bukti pada tindak pidana penciptaan informasi elektronik palsu, tidak hanya didasari dengan apakah *screenshot facebook* tersebut dapat memenuhi ketentuan mengenai jenis alat bukti. Namun dalam hal ini juga dilihat dari sudut pandang lain yang dapat dilihat dari

¹⁰ Putusan Mahkamah Konstitusi Republik Indonesia Nomor 20/PUU-XIV/2016, Mahkamah Konstitusi, 7 September 2016

¹¹ Arief Heryogi, Masruchin Ruba'I, Bambang Sugiri, 'Fungsi Bukti Elektronik Dalam Hukum Acara Pidana Pasca Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016' (2017) 2 (1) Jurnal Ilmiah Pendidikan Pancasila dan Kewarganegaraan 7, 12.

¹² Soeb Aripin, G.L. Ginting, Natalia Silalahi, 'Penerapan Metode Retinex Untuk Meningkatkan Kecerdasan Citra Pada Hasil Screenshot' (2017) 2 (1) Media Informatika Budidarma 24.

berbagai sudut pandang, yaitu dari kekuatan pembuktiannya dalam membuktikan unsur tindak pidana penciptaan informasi elektronik palsu, keabsahannya sebagai suatu alat bukti elektronik, maupun dari segi keandalannya sebagai suatu alat bukti. Namun, dalam bagian ini, akan lebih fokus untuk melihat kedudukan *screenshot facebook* sebagai alat bukti pada tindak pidana penciptaan informasi elektronik palsu dari segi keabsahannya sebagai alat bukti.

Dari segi keabsahannya sebagai suatu alat bukti, bila dikaitkan atau dipandang dari syarat keabsahan alat bukti elektronik dalam UU ITE sebagaimana telah dijabarkan sebelumnya, maka sesungguhnya alat bukti *screenshot facebook* dapat dipandang masih diragukan mengenai keabsahannya sebagai alat bukti karena belum cukup untuk dapat memenuhi syarat materiil dari alat bukti elektronik. Sebagaimana yang telah dijelaskan sebelumnya, berdasarkan Pasal 5 ayat (3) UU ITE, suatu informasi elektronik dan/atau dokumen elektronik dianggap sah sebagai suatu alat bukti apabila menggunakan sistem elektronik yang sesuai dengan ketentuan UU ITE dalam Pasal 15 dan 16 UU ITE. Selain itu, sesuai dengan Pasal 6 UU ITE, maka informasi elektronik dan/atau dokumen elektronik dinyatakan sah sebagai alat bukti elektronik bila informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhan dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Dalam hal ini, berkaitan dengan syarat materiil tersebut, *screenshot facebook* dapat dianggap belum memenuhi syarat materiil dikarenakan informasi yang terdapat dalam bukti *screenshot facebook* belum dapat terjamin mengenai keutuhannya dan belum dapat dipertanggungjawabkan untuk menerangkan suatu keadaan, sebab sistem elektronik yang merupakan sumber dari perolehan *screenshot facebook* yaitu akun *facebook* itu sendiri masih belum dapat memenuhi seluruh syarat sistem elektronik dalam Pasal 15 dan Pasal 16 UU ITE, khususnya syarat mengenai bahwa sistem elektronik dapat menampilkan kembali informasi atau dokumen elektronik secara utuh, dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elektronik karena masih dimungkinkan terjadi akses ilegal pada akun *facebook* tersebut sewaktu-waktu. Hal ini menyebabkan, secara materiil keabsahan dari substansi yang ditampilkan pada *screenshot facebook* tersebut masih dapat diragukan sebagai alat bukti. Ancaman akses ilegal yang bisa terjadi pada akun *facebook* sebagai sistem elektronik yang menjadi sumber perolehan *screenshot facebook* membuat dapat diragukannya materi yang ditampilkan pada *screenshot* tersebut. Bisa saja, materi yang ditampilkan pada *screenshot* berbeda dengan materi atau substansi pada akun *facebook*. Dapat saja dilakukan perubahan pada substansi pada akun *facebook* pra atau pasca pengambilan *screenshot* atas akun *facebook* tersebut, sehingga kebenaran atau keabsahan secara materiil pada alat bukti *screenshot facebook* khususnya pada tindak pidana penciptaan informasi elektronik palsu, masih dapat diragukan.

Permasalahan mengenai diragukannya alat bukti *screenshot facebook* untuk memenuhi syarat keabsahan materiil sebagai alat bukti elektronik dalam kasus tindak pidana penciptaan informasi elektronik palsu memberikan pemahaman pentingnya suatu jaminan untuk menjamin keabsahan *screenshot facebook* secara materiil, yang mana seharusnya jaminan dari *screenshot facebook* tersebut sebagai suatu alat bukti adalah akun *facebook* itu sendiri. Namun dalam kasus ini, akun

facebook tersebut tidak turut disita untuk menjadi suatu bukti maupun untuk menjadi jaminan dari bukti *screenshot facebook* dikarenakan belum adanya aturan hukum yang mengakomodir penyitaan atas sistem elektronik, yang dalam hal ini lebih spesifiknya adalah penyitaan atas akun, baik pada KUHAP sebagai *lex generalis* dalam hukum pidana formil, maupun UU ITE, dan juga peraturan perundang-undangan lain yang terkait, seperti dalam Permenkominfo No. 7 Tahun 2016. Hal ini menyebabkan belum adanya aturan yang baku dan jelas mengenai penyitaan atas bukti elektronik yang dalam hal ini adalah sistem elektronik atau lebih spesifiknya adalah penyitaan atas akun. Hal ini berbeda dengan Inggris dan Amerika Serikat yang telah memiliki aturan baku mengenai penyitaan bukti elektronik. Aturan baku tersebut tercantum dalam *Good Practice Guide for Computer-Based Electronic Evidence, Association of Chief Police (ACPO)* di Inggris dan untuk Amerika Serikat adalah pada *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, U.S. Department of Justice*.¹³

Pengaturan mengenai penyitaan sistem elektronik dalam UU ITE hanya tercantum pada Pasal 43 ayat (3) dan Pasal 43 ayat (4) UU ITE. Terkait dengan pengaturan mengenai penyitaan sistem elektronik dalam UU ITE tersebut, sebenarnya masih memiliki beberapa kekurangan, antara lain, tidak adanya pengaturan yang jelas mengenai prosedur penyitaan, sifat penyitaan bukti elektronik berbeda dengan penyitaan perangkat biasa karena penyitaan bukti elektronik bersifat *mirroring* yaitu menyalin data dari perangkat sehingga pada banyak kasus pemilik data masih dapat mengakses data tersebut sedangkan seharusnya esensi dari penyitaan adalah mengambil alih dan membatasi akses terhadap barang tersebut agar tidak berubah, pengaturan yang masih terbatas pada penyitaan atas obyek fisik atau benda tidak bergerak sedangkan bukti elektronik sendiri adalah suatu data yang tidak berwujud dan bukan perangkatnya sehingga belum mengakomodir penyitaan bukti elektronik dalam suatu jaringan atau sistem.¹⁴

Dalam Permenkominfo No. 7 Tahun 2016 yang sebenarnya mengatur dengan lebih rinci atau spesifik mengenai penyidikan dan penindakan tindak pidana di bidang teknologi informasi dan transaksi elektronik khususnya yang dalam hal ini dilakukan oleh Pejabat Pegawai Negeri Sipil di bidang teknologi informasi, namun tetap juga tidak terlihat adanya ketentuan spesifik mengenai penyitaan atas akun. Dalam Pasal 39 hingga Pasal 41 Permenkominfo No. 7 Tahun 2016 memang diatur ketentuan mengenai penyitaan, namun tidak terdapat ketentuan yang spesifik yang menjelaskan penyitaan atas akun termasuk mengenai prosedur dari penyitaan atas akun sebagai sistem elektronik. Pada Pasal 39 ayat (2) huruf f Permenkominfo No. 7 Tahun 2016, memang dinyatakan bahwa sistem elektronik, informasi elektronik, atau dokumen elektronik yang diperoleh melalui proses forensik terhadap sistem elektronik yang digeledah merupakan salah satu hal yang dapat dikenai penyitaan.¹⁵ Sehingga akun yang dapat dimaknai sebagai suatu sistem elektronik dapat

¹³ Kemitraan Partnership, LeIP, IDLO, Kingdom of the Netherland, 'Booklet Bukti Elektronik di Indonesia Pengaturan Tentang Perolehan, Pemeriksaan, dan Pengelolaan Bukti Elektronik (Electronic Evidence)' (Seminar Publik, Menuju Pengaturan Bukti Elektronik yang Akuntabel, LEIP dan Kemitraan, Surabaya, 24 Juli 2019).

¹⁴ *Ibid.*

¹⁵ Pasal 39 ayat (2) huruf F Permenkominfo No. 7 Tahun 2016.

dilakukan penyitaan. Namun, tidak dijelaskan secara rinci, bagaimana penyitaan atas sistem elektronik berupa akun. Hal ini seharusnya juga patut dijelaskan dan diatur dalam suatu instrumen hukum, mengingat bahwa penyitaan atas akun sebagai sistem elektronik tentu berbeda prosedurnya dengan penyitaan benda pada umumnya.

Dalam kasus ini sendiri, penyitaan yang dilakukan oleh aparat penegak hukum yang menyita telepon genggam milik AS tidak serta merta menjadikan akun *facebook* tersebut turut disita dikarenakan akun *facebook* tersebut terhubung dengan jaringan yang sewaktu-waktu masih dapat dimungkinkan adanya ancaman yang terjadi yang mengganggu integritas dan keutuhan dari informasi yang ada dalam akun maupun pada akun itu sendiri. Sehingga selama akun *facebook* tersebut tidak dilakukan penyitaan, maka keabsahan secara materiil dari *screenshot facebook* tersebut sebagai alat bukti masih dapat diragukan.

Lalu, bagaimana konsep atau prosedur penyitaan atas akun itu sendiri? Terkait dengan hal tersebut, selain masih bersifat *mirroring* sebagaimana telah dijelaskan pada penjelasan sebelumnya, untuk saat ini seperti yang dinyatakan oleh kemitraan dan lembaga kajian dan advokasi untuk independensi peradilan pada naskah akademik kerangka hukum perolehan, pemeriksaan, dan pengelolaan bukti elektronik (*electronic evidence*), penyitaan atas akun masih dimaknai dan hanya terbatas pada pengambilalihan akses atas akun, yang serupa dengan pemblokiran rekening. Pemblokiran akses tersebut dapat dilakukan dengan meminta penyelenggara sistem elektronik atau dengan mengambil alih kata kunci, PIN atau sejenisnya dari pemilik akses.¹⁶ Konsep penyitaan akun dengan pemblokiran akses seperti ini pun sebenarnya dapat dipandang masih memiliki kelemahan. Hal tersebut dikarenakan, hal tindak pidana di bidang teknologi informasi berhubungan dengan jaringan. Melakukan penyitaan akun dengan mengambil alih kata kunci, PIN atau sejenisnya dari pemilik akun, juga masih membuka peluang adanya pembobolan, akses ilegal dari pihak lain untuk dapat mengakses akun yang disita tersebut. Dalam hal ini, diperlukan suatu mekanisme atau prosedur baru, yang penting untuk dipikirkan dalam rangka menyita dan membekukan akun, yang benar-benar meminimalisir bahkan menutup adanya kemungkinan pembobolan dan perubahan pada akun oleh pihak lain. Sehingga, keabsahan secara materiil dari substansi akun dapat terjaga dan dapat dijadikan jaminan yang sah bagi alat bukti *screenshot* yang dalam hal ini adalah *screenshot facebook*.

Bila didasarkan dari syarat keabsahan informasi elektronik dan/atau dokumen elektronik dari Putusan MK No. 20/PUU-XIV/2016, maka pembahasan yang sebelumnya telah dijabarkan akan terlihat bertentangan apabila kedudukan *screenshot facebook* sebagai alat bukti informasi elektronik hanya didasarkan atau dilihat dari Putusan MK saja. Sebab, Putusan MK membawa adanya implikasi bahwa keabsahan *screenshot facebook* sebagai informasi elektronik dapat sah sebagai suatu alat bukti, karena dalam kasus ini *screenshot facebook* tersebut digunakan dalam rangka penegakan hukum dan atas permintaan penegak hukum yang dalam hal ini adalah jaksa yang mempergunakannya sebagai alat bukti di

¹⁶ Kemitraan dan Lembaga Kajian dan Advokasi Untuk Independensi Peradilan, 'Naskah Akademik Kerangka Hukum Perolehan, Pemeriksaan, dan Pengelolaan Bukti Elektronik (*Electronic Evidence*)' (Seminar Publik, Menuju Pengaturan Bukti Elektronik yang Akuntabel, LEIP dan Kemitraan, Surabaya, 24 Juli 2019).

persidangan. Pertentangan ini dapat muncul karena sebagaimana yang dijelaskan oleh Arief Heryogi, Masruchin Ruba'I dan Bambang Sugiri, implikasi dari adanya Putusan MK ini memang dapat membawa adanya ketidakpastian hukum terhadap keabsahan alat bukti elektronik dan menyebabkan multitafsir bagi aparat penegak hukum.¹⁷ Dalam penelitian ini, kedua implikasi tersebut tidak dijelaskan lebih lanjut dan secara mendalam mengingat agar tidak semakin melebarnya pokok bahasan yang ada. Namun sebenarnya dalam hal ini memahami kedudukan dari *screenshot facebook* sebagai alat bukti haruslah dilihat secara menyeluruh dari segala aspek. Bukan hanya melihat penggunaannya yang dalam rangka penegakan hukum dan atas permintaan dari aparat penegak hukum, namun harus melihat pula pada prosedur atau sisi formilnya maupun substansinya sebagai alat bukti (syarat materiil) sebagaimana yang telah dijabarkan pada penjelasan sebelumnya.

Didasari dengan adanya hal-hal yang telah dijelaskan ini, maka, dapat dipahami bahwa sesungguhnya *screenshot facebook* tidak cukup sah untuk dapat digunakan sebagai alat bukti pada tindak pidana penciptaan informasi elektronik palsu meskipun *screenshot facebook* tersebut dipergunakan dalam penegakan hukum dan atas permintaan dari aparat penegak hukum. Hal tersebut dikarenakan salah satu alasannya adalah keabsahannya sebagai alat bukti elektronik masih dapat diragukan. Dalam hal ini keberadaan jaminan dari keabsahan materiil pada *screenshot facebook* tersebut sangat penting untuk diadakan, dan jaminan tersebut dapat menggunakan akun *facebook* yang perlu dilakukan penyitaan oleh aparat penegak hukum untuk menjamin keabsahan materiil dari *screenshot* tersebut. Oleh karena itu, diperlukan adanya suatu ketentuan hukum mengenai penyitaan atas akun yang juga menjelaskan mengenai prosedurnya, agar penyitaan atas akun memiliki suatu payung hukum yang sah dan dapat dilakukan, dikarenakan pentingnya keberadaan akun sebagai suatu bukti untuk mengungkap tindak pidana yang terjadi maupun untuk mendukung dan menjadi jaminan bagi alat bukti lain seperti alat bukti *screenshot facebook* pada pembuktian di pengadilan.

Mekanisme Pembuktian *Screenshot Facebook* Sebagai Alat Bukti Tindak Pidana Penciptaan Informasi Elektronik Palsu Ditinjau Dari UU ITE dan Perubahan atas UU ITE

Sebagaimana yang telah dijelaskan pada bagian sebelumnya, bahwa sesungguhnya *screenshot facebook* dalam kasus ini yang dimasukkan dalam satu buah CD, dapat dikategorikan sebagai salah satu jenis alat bukti berdasarkan Pasal 44 jo. Pasal 5 UU ITE, yaitu sebagai alat bukti informasi elektronik. Namun, keabsahannya sebagai alat bukti elektronik masih dapat diragukan, karena belum dapat memenuhi seluruh syarat keabsahan alat bukti elektronik, yang dalam hal ini adalah syarat keabsahan materiil. Dalam bagian ini akan dibahas mengenai bagaimana penerapan *screenshot facebook* bila digunakan sebagai alat bukti pada tindak pidana penciptaan informasi elektronik palsu.

Untuk melihat bagaimana penerapan *screenshot facebook* sebagai alat bukti tindak pidana penciptaan informasi elektronik palsu, maka perlu melihat bagaimana *screenshot facebook* membuktikan tiap unsur-unsur tindak pidana penciptaan informasi elektronik palsu dalam Pasal 35 UU ITE. Atau dengan kata lain, akan

¹⁷ Heryogi (n 11).

dilihat mengenai kekuatan pembuktian *screenshot facebook* sebagai alat bukti terkait dengan tindak pidana penciptaan informasi elektronik palsu, khususnya yang terjadi di Majalengka sebagai kasus hukum yang dijadikan acuan dalam penelitian hukum ini.

Terkait dengan hal tersebut, Leden Marpaung menyatakan bahwa, suatu tindak pidana secara umum terdiri dari dua unsur pokok yaitu unsur subyektif dan unsur obyektif.¹⁸ Berdasarkan hal tersebut, maka unsur tindak pidana yang diatur dalam ketentuan Pasal 35 UU ITE adalah:

1. Unsur subyektif : dengan sengaja
2. Unsur obyektif :
 - a. Sifat melawan hukum: tanpa hak atau melawan hukum.
 - b. Perbuatan: melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan.
 - c. Obyek: informasi elektronik dan/atau dokumen elektronik.
 - d. Akibat: dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.

Untuk melihat penerapan *screenshot facebook* sebagai alat bukti tindak pidana penciptaan informasi elektronik palsu, penting untuk kembali mengingat bahwa *screenshot facebook* yang digunakan sebagai bukti oleh Jaksa Penuntut Umum pada kasus ini adalah *screenshot facebook* yang substansinya menunjukkan adanya akun *facebook* atas nama “ADE” yang dibuat oleh AS, dimana akun *facebook* tersebut sebenarnya menggunakan nama dan foto profil dari AN. Pada *screenshot facebook* tersebut juga terlihat bahwa akun *facebook* atas nama “ADE” buatan AS tersebut menuliskan komentar penghinaan pada beberapa status *facebook* orang lain.

Untuk melihat penerapan dari *screenshot facebook* sebagai alat bukti pada tindak pidana penciptaan informasi elektronik palsu, akan dilihat dari penerapannya pada unsur tindak pidana yang pertama, yaitu unsur kesalahan sebagai unsur subyektif. Berdasarkan *Memorie van Toelichting* (MvT) WvS Belanda, yang dimaksud dengan sengaja melakukan kejahatan adalah melakukan suatu perbuatan yang dilarang dengan “dikehendaki” dan “diketahui”. Dari hal ini dapat diperoleh suatu pemahaman bahwa menurut MvT ada dua aspek atau dua unsur kesengajaan yaitu kesengajaan sebagai pengetahuan (*wetens*) dan kesengajaan sebagai kehendak (*willens*).¹⁹ Di sisi lain, sebagaimana yang dinyatakan oleh Adami Chazawi dan Ardi Ferdian, sebenarnya unsur subyektif dalam Pasal 35 UU ITE ini tidak hanya terlihat dari unsur “dengan sengaja” namun juga terlihat dari kata “dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.” Sebagai akibat atau tujuan yang dilarang dalam pasal ini.²⁰ Dengan kata lain, sebenarnya kesengajaan yang diatur dalam pasal ini adalah kesengajaan sebagai maksud. Maksud yang ingin dicapai dari kesengajaan tersebut adalah agar informasi elektronik yang dimanipulasi, diciptakan, diubah, dihilangkan atau dirusak tersebut dianggap suatu informasi elektronik yang otentik atau asli baik secara sumber maupun konten, sedangkan sesungguhnya adalah palsu.

¹⁸ Leden Marpaung, *Unsur-Unsur Perbuatan yang Dapat Dihukum (Delik)* (Sinar Grafika 1991) 6.

¹⁹ Adami Chazawi dan Ardi Ferdian, *Tindak Pidana Informasi & Transaksi Elektronik* (ed. revisi Media Nusa Creative 2015) 14.

²⁰ *Ibid.*, 20.

Dengan demikian, kesengajaan sebagai maksud yang diatur dalam Pasal 35 UU ITE belum dapat terpenuhi dengan penggunaan *screenshot facebook* ini. Hal itu dikarenakan *screenshot facebook* tersebut hanya menunjukkan adanya akun atas nama AN yang dibuat oleh AS yang menuliskan komentar bernada penghinaan dan pencemaran pada status *facebook* beberapa orang yang merupakan teman dari AN. Oleh karena itu, yang dapat terlihat dari *screenshot facebook* tersebut adalah adanya kehendak pengelola akun *facebook* yang namanya tertera pada akun tersebut agar komentar tersebut diketahui khalayak umum sehingga orang yang menerima komentar tersebut dapat mencemarkan nama baiknya dan merasa terhina. Penggunaan *screenshot* tersebut justru tidak menunjukkan adanya pemenuhan unsur kesengajaan sebagai maksud menciptakan informasi elektronik palsu dari diri pelaku, sedangkan hanya menunjukkan adanya kesengajaan pelaku untuk mencemarkan nama baik seseorang.

Mengenai unsur obyektif, unsur obyektif yang pertama yaitu “tanpa hak atau melawan hukum”. Unsur tanpa hak sebenarnya dimaksudkan untuk memberi perlindungan hukum bagi setiap orang yang melakukan perbuatan yang dilarang namun sebenarnya ia berhak melakukan.²¹ Dari pengertian tersebut maka dapat dipahami bahwa penggunaan unsur “tanpa hak” dalam ketentuan Pasal 35 UU ITE diperuntukkan bagi setiap orang yang tidak memiliki hak untuk melakukan perbuatan yang diatur dalam Pasal 35 UU ITE tersebut. Berkaitan dengan hal tersebut, Leden Marpaung menegaskan bahwa sifat melawan hukum dalam suatu delik ada yang dinyatakan secara tegas sebagai unsur tindak pidana tapi ada pula yang tidak secara jelas dinyatakan namun tetap dianggap sebagai suatu unsur dalam delik.²² Terkait dengan hal ini, maka apabila sifat melawan hukum dimuat dalam suatu pasal sebagai suatu unsur, maka sifat melawan hukum tersebut harus dibuktikan di persidangan sedangkan bila tidak tertulis sebagai unsur suatu pasal, maka tidak harus dibuktikan walaupun dianggap tetap ada sebagai unsur perbuatan pidana. Dalam Pasal 35 UU ITE, unsur melawan hukum dimuat sebagai suatu unsur, maka sifat melawan hukum dari perbuatan yang dilarang dalam Pasal 35 UU ITE haruslah dibuktikan oleh alat bukti yang diajukan di persidangan.

Adapun unsur “tanpa hak atau melawan hukum” berhubungan dengan unsur perbuatan yang diatur dalam Pasal 35 UU ITE, yang sebenarnya meliputi lima jenis perbuatan, namun dalam kasus ini dipilih perbuatan “penciptaan” sebagai *actus reus* yang diterapkan. Mengacu pada pendapat Adami Chazawi dan Ardi Ferdian, pada hakekatnya penciptaan adalah kegiatan mencipta atau menciptakan, yang mana menciptakan adalah menjadikan sesuatu yang baru yang sebelumnya belum ada atau lain dari yang semula sudah ada. Adapun tujuan dari penciptaan dalam pasal ini adalah agar isi informasi dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik/benar.²³ Selain itu, penting untuk mengingat bahwa berdasarkan ketentuan Pasal 35 UU ITE, obyek yang dikenai perbuatan penciptaan tersebut adalah informasi elektronik dan/atau dokumen elektronik, dan untuk akibat atau tujuan yang dilarang dalam ketentuan Pasal 35 UU ITE ini adalah “dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut

²¹ *Ibid.*, 21.

²² Marpaung (n 18) 53.

²³ Chazawi, Ferdian (n 19) 197-198.

dianggap seolah-olah data yang otentik.”. Kata “dianggap seolah-olah data yang otentik” menunjukkan unsur palsu dalam ketentuan Pasal 35 UU ITE ini. Perbuatan yang diatur dan dilakukan dalam Pasal 35 UU ITE dimaksudkan untuk membuat informasi elektronik tersebut dianggap seolah otentik sedangkan sesungguhnya tidak otentik.

Dalam hal ini, menurut Josua Sitompul, yang dimaksud dengan otentik adalah bahwa informasi elektronik tersebut bersumber dari orang yang memiliki hak atau kewenangan untuk membuat atau mengeluarkan informasi elektronik tersebut, dan secara konten, maka kontennya juga harus konten yang dikehendaki oleh sumber tersebut. Otentik dalam hal ini tidak hanya sekedar dimaknai sebagai data yang dibuat oleh atau dihadapan pejabat yang berwenang berdasarkan peraturan perundang-undangan.²⁴ Hal tersebut memberikan pemahaman bahwa secara *a contrario* suatu informasi elektronik dianggap tidak otentik atau palsu bila dikeluarkan oleh sumber yang tidak berwenang dan kontennya atau isi informasi elektronik tersebut bukanlah yang dimaksud oleh sumber.

Berdasarkan uraian penjelasan tersebut, penggunaan *screenshot facebook* tidaklah cukup untuk membuktikan unsur-unsur obyektif dalam Pasal 35 UU ITE. Hal itu dikarenakan dengan penggunaan *screenshot facebook* tersebut, unsur *actus reus* yang terbukti bukanlah “penciptaan” sebagaimana unsur *actus reus* dari Pasal 35 UU ITE yang dikenakan pada kasus ini. Hal itu dikarenakan tidak terlihat adanya perbuatan penciptaan yang dapat ditunjukkan pada *screenshot facebook* tersebut. Tidak terlihat dalam *screenshot facebook* tersebut bahwa telah ada atau telah terjadi tindakan atau kegiatan menjadikan suatu informasi elektronik yang baru yang sebelumnya belum ada atau informasi elektronik lain dari yang sudah ada yang dilakukan oleh pengelola akun *facebook* tersebut. Yang terlihat justru adalah tindakan mengirimkan komentar pada status *facebook* orang lain. Terkait pula dengan obyeknya, maka penggunaan *screenshot facebook* tersebut akan lebih fokus untuk membuktikan dan menunjukkan komentar yang memiliki muatan penghinaan dan/atau pencemaran nama baik sebagai obyek informasi elektronik, sehingga fokus obyek yang dibuktikan bukanlah informasi elektronik palsu berupa nama, identitas dan foto yang ada dalam akun *facebook* yang tertera pada *screenshot facebook* tersebut maupun akun *facebook* palsu itu sendiri. Sebab, dengan penggunaan *screenshot facebook* tersebut tidak terlihat adanya persoalan yang perlu dibuktikan mengenai akun *facebook* itu sendiri.

Maksud atau akibat yang dilarang dalam Pasal 35 UU ITE yaitu, “dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.” juga belum cukup terbukti dengan penggunaan *screenshot facebook* tersebut. Perlu dipahami sebelumnya bahwa, dalam kasus ini akun *facebook* buatan AS merupakan akun *facebook* palsu karena pembuatan akun *facebook* tersebut maupun substansi di dalam akun *facebook* tersebut mengandung keadaan ketidakbenaran. Dalam hal ini, secara substansi informasi elektronik berupa nama, foto, identitas dalam akun *facebook* yang dibuat oleh AS tidak menggunakan nama, foto dan identitas dirinya pribadi, melainkan menggunakan nama, foto dan identitas dari AN. Selain itu, email yang digunakan untuk membuat akun *facebook* tersebut bukanlah email asli milik AN yaitu dheamoree@yahoo.co.id

²⁴ Sitompul (n 9) 247-248.

(yang dalam hal ini digunakan oleh AN untuk membuat akun *facebook* asli miliknya) namun akun *facebook* tersebut dibuat dengan menggunakan nomor *handphone* pribadi AS untuk mendaftar dan *login* pada akun *facebook* tersebut. Bila dikaitkan dengan penggunaan *screenshot facebook* sebagai alat bukti maka *screenshot facebook* tersebut tidak cukup untuk menunjukkan bahwa akun *facebook* yang ditampilkan melalui *screenshot* sebenarnya adalah akun *facebook* palsu yang mengandung informasi elektronik palsu atau tidak otentik. Tidak dapat terlihat maksud atau akibat bahwa perbuatan membuat akun *facebook* yang dilakukan oleh AS dengan memakai nama dan foto dari AN bertujuan agar akun maupun substansinya terlihat otentik sebagai akun dari AN sedangkan sebenarnya tidak otentik. Di sisi lain, *screenshot facebook* tersebut lebih menunjukkan adanya maksud atau akibat untuk menghina dan mencemarkan nama baik seseorang karena *screenshot facebook* tersebut menunjukkan adanya akun *facebook* dengan nama dan identitas AN yang menuliskan kata-kata menghina pada beberapa akun *facebook* lainnya.

Pada Putusan Pengadilan Negeri Majalengka sendiri, yaitu Putusan No. 43/Pid.Sus/2018/PN Mjl, pada bagian pertimbangan hakim, tidak dapat dilihat dengan akurat telah terjadi pemenuhan unsur tindak pidana dan bagaimana pertimbangan hakim terkait dengan terjadinya tindak pidana tersebut ditinjau dari penggunaan *screenshot facebook*. Pertimbangan hakim dalam memutus dan menyatakan perbuatan pelaku memenuhi unsur Pasal 51 jo. Pasal 35 UU ITE adalah lebih didasarkan dengan hal lain sebagaimana termaktub dalam kalimat berikut, “Menimbang, bahwa berdasarkan fakta dalam persidangan bahwa pada hari Minggu tanggal 05 Nopember 2017 sekitar pukul 21.00 Wib melihat konten komentar akun Facebook bernama ADE dengan foto profil yang terpasang adalah foto profil saksi Ade Nurprihatin Bin Sunardi, pada status Facebook akun milik saksi Arif Sagita Bin Suha dengan perkataan antara lain “Moal pyu di jual nu modelan ktu mh. Bnget na oge jiga bagong” , “Haaa sia teu ngenah anjink” , “Aing bdak gandu blok senen anjink” , “teu kdu ke pting anjink ayena ae sok jdah” Menimbang, bahwa saat saksi Arif Sagita Bin Suha melihat konten komentar tersebut, saksi Arif Sagita Bin Suha mengira bahwa konten komentar tersebut telah dibuat oleh saksi Ade Nurprihatin Bin Sunardi, karena profil dan foto pada akun facebook tersebut menggunakan nama dan foto saksi Ade Nurprihatin Bin Sunardi, selanjutnya karena saksi Arif Sagita Bin Suha merasa kalimat itu tidak sepatasnya dilontarkan dalam status facebook, maka saksi Arif Sagita Bin Suha kemudian menemui saksi Ade Nurprihatin Bin Sunardi untuk menanyakan mengenai hal tersebut, selanjutnya saksi Ade Nurprihatin Bin Sunardi memastikan kepada saksi Arif Sagita Bin Suha bahwa akun facebook atas nama Ade yang menggunakan foto saksi Ade Nurprihatin Bin Sunardi adalah bukan milik saksi Ade Nurprihatin Bin Sunardi, dan atas kejadian tersebut, saksi Ade Nurprihatin Bin Sunardi merasa dirugikan dan keberatan sehingga saksi Ade Nurprihatin Bin Sunardi melaporkan hal tersebut ke Polres Majalengka. Menimbang, bahwa selanjutnya berdasarkan informasi yang diterima, Petugas Kepolisian kemudian melakukan pemeriksaan terhadap terdakwa dan barang bukti berupa 1 (satu) buah Handphone merk Samsung Galaxy J1 Ace warna hitam milik terdakwa, dan ternyata benar bahwa di dalam handphone tersebut ada akun Facebook bernama ADE dengan foto profil yang terpasang adalah foto profil saksi Ade Nurprihatin Bin Sunardi yang memuat komentar pada status

Facebook akun milik saksi Arif Sagita Bin Suha dengan kalimat yang tidak sepantasnya dan saat dilakukan pemeriksaan terhadap terdakwa, terdakwa pun mengakui bahwa melakukan hal tersebut dengan cara merubah identitas facebook milik terdakwa menjadi identitas saksi Ade Nurprihatin Bin Sunardi dan mengganti foto profil facebook terdakwa menjadi foto profil saksi Ade Nurprihatin Bin Sunardi, sehingga unsur tersebut telah terpenuhi”.²⁵

Dari uraian pertimbangan hakim ini pun sebenarnya belum dapat menunjukkan pemenuhan setiap unsur tindak pidana penciptaan informasi elektronik palsu maupun tidak secara kuat membuktikan pelaku adalah benar sebagai pelaku tindak pidana tersebut. Tidak terlihat adanya pembuktian telah terjadi perbuatan penciptaan dan apakah benar memang pelaku adalah yang menciptakan informasi elektronik tersebut dari fakta hukum yang dipaparkan dan diperoleh hakim dari alat bukti yang ada. Dalam hal ini pun, pengakuan dari pelaku sebagaimana yang dinyatakan dalam pertimbangan hakim, seharusnya tidak dapat dijadikan dasar utama dalam membuktikan tindak pidana yang terjadi. Mengingat, kebenaran yang dianut dalam hukum acara pidana, merupakan kebenaran materiil yang berbeda dengan kebenaran formil yang dianut dalam hukum acara perdata.

Oleh karena itu, diperlukan adanya alat bukti lain untuk membuktikan tindak pidana penciptaan informasi elektronik palsu yang telah terjadi. Adapun alat bukti yang dapat digunakan dalam mekanisme pembuktian tersebut dapat mengacu pada ketentuan dalam Pasal 44 UU ITE yang sebenarnya mengacu pada ketentuan jenis alat bukti dalam Pasal 184 KUHP dan Pasal 5 UU ITE. Dalam hal ini, berdasarkan Pasal 183 KUHP, diperlukan setidaknya dua alat bukti yang sah yang dapat menimbulkan keyakinan hakim untuk menjatuhkan pidana terhadap terdakwa. Terkait dengan hal tersebut, sebenarnya dalam mekanisme pembuktian tindak pidana penciptaan informasi elektronik palsu, dapat diajukan alat bukti seperti alat bukti keterangan ahli digital forensik. Keterangan dari ahli digital forensik ini diperlukan mengingat bahwa sebenarnya dalam tiap tindakan kejahatan yang terjadi, selalu meninggalkan suatu jejak, dan dalam hal ini, jejak dari tindak pidana yang berkaitan dengan teknologi informasi pada umumnya disebut sebagai *digital fingerprint*. *Digital fingerprint* tersebut dapat terlacak dengan suatu ilmu pengetahuan dan penanganan khusus yaitu melalui ilmu digital forensik yang dilakukan oleh ahli digital forensik. Digital forensik sendiri menurut Sara Sarwar Mir, Umar Shoaib dan Muhammad Shahzad Sarfraz adalah suatu bidang penelitian yang baru muncul yang berasal dari seringnya penggunaan komputer dan perangkat penyimpanan oleh penjahat yang terdiri dari berbagai fase atau alur dengan cara yang dapat diterima secara hukum.²⁶

Sebenarnya proses dari digital forensik yang menjadi dasar keterangan ahli forensik digital di pengadilan sangatlah beragam, namun secara umum, sebagaimana yang dinyatakan oleh Sara Sarwar Mir, Umar Shoaib, dan Muhammad Shahzad Sarfraz, alur dari digital forensik itu terbagi menjadi beberapa tahap. Tahap pertama adalah *preservation* yaitu tahapan untuk mengamankan tempat kejadian

²⁵ Asep Supriatna Bin Dayat, No. 43/Pid.Sus/2018/PN Mjl, Pengadilan Negeri Majalengka, 16 Mei 2018.

²⁶ Sara Sarwar Mir, Umar Shoaib, Muhammad Shahzad Sarfraz, 'Analysis Of Digital Forensic Investigation Models' (2016) 14 (11) International Journal of Computer Science and Information Security 292.

perkara atau tempat bukti tersebut berada untuk mencegah kerusakan pada informasi digital. Tahap kedua adalah *collection* yaitu tahap pengumpulan dan penemuan berbagai informasi atau bukti digital yang ada. Tahap yang ketiga adalah *examination* yaitu tahap untuk melakukan pencarian dan pemeriksaan secara sistematis untuk mendapat bukti. Tahap berikutnya adalah *analysis* yaitu tahap untuk menemukan kesimpulan berdasarkan bukti yang telah ditemukan, dan yang terakhir adalah *reporting* untuk melaporkan mengenai setiap aktivitas atau kegiatan yang dilakukan selama digital forensik. Hal ini penting untuk menjamin keabsahan dari setiap proses digital forensik.²⁷ Dalam Permenkominfo No. 7 Tahun 2016, sebenarnya juga mengatur mengenai proses forensik pada sistem elektronik, sebagaimana yang diatur dalam Pasal 46 Permenkominfo No. 7 Tahun 2016 pada Pasal 46 ayat (2) diatur mengenai tahapan dari proses forensik tersebut yang meliputi tahap identifikasi, akuisisi, pengujian dan analisa, serta dokumentasi dan pelaporan. Berkaitan dengan kasus ini sebenarnya keterangan ahli forensik sebagai salah satu alat bukti di pengadilan, dapat diperoleh dengan dilakukannya proses digital forensik oleh ahli forensik tersebut terhadap akun *facebook* yang dibuat oleh AS. Untuk melakukan hal ini tentu perlu dilakukan terlebih dahulu penyitaan atas akun. Hal inilah yang juga menunjukkan pentingnya penyitaan atas akun dan aturan hukum sebagai payung hukum untuk penyitaan atas akun sebagaimana yang telah dijelaskan pada bagian sebelumnya.

Namun perlu diingat bahwa, sebagaimana yang diamanatkan dalam Pasal 183 KUHAP, maka terdapat ketentuan minimal 2 alat bukti dalam hakim menjatuhkan putusan pidana terhadap terdakwa. Dalam hal ini, keterangan ahli digital forensik sebagai salah satu alternatif alat bukti yang dapat digunakan dalam mekanisme pembuktian tindak pidana penciptaan informasi elektronik palsu perlu didukung dengan alat bukti lain seperti keterangan saksi ataupun jenis alat bukti lain sesuai dengan ketentuan Pasal 184 KUHAP dan Pasal 5 UU ITE.

PENUTUP

Berdasarkan uraian di atas, dapat disimpulkan beberapa hal: *Pertama*, kedudukan *screenshot facebook* tidak cukup sah untuk dapat digunakan sebagai alat bukti tindak pidana penciptaan informasi elektronik palsu. Hal tersebut dikarenakan keabsahan dari *screenshot facebook* sebagai alat bukti elektronik masih dapat diragukan mengingat bahwa *screenshot facebook* belum memenuhi seluruh syarat keabsahan alat bukti elektronik, yang dalam hal ini adalah syarat materiil dalam Pasal 5 ayat (3) dan Pasal 6 UU ITE. Hal tersebut juga dipengaruhi karena akun *facebook* yang seharusnya dapat menjadi jaminan keabsahan secara materiil dari *screenshot facebook* sebagai alat bukti, tidak turut disita dalam kasus ini dikarenakan masih belum adanya ketentuan hukum yang secara jelas mengatur dan mengakomodir tindakan penyitaan akun.

Kedua, penerapan *screenshot facebook* sebagai alat bukti tindak pidana penciptaan informasi elektronik palsu juga masih kurang memenuhi dan membuktikan tiap unsur tindak pidana penciptaan informasi elektronik palsu dalam Pasal 35 UU ITE. Sehingga dalam hal ini diperlukan adanya suatu jenis alat

²⁷ *Ibid.*, 294.

bukti lain yang lebih memadai untuk diterapkan sebagai alat bukti pada tindak pidana penciptaan informasi elektronik palsu sesuai dengan jenis alat bukti dalam Pasal 44 UU ITE, yang mengacu pada ketentuan mengenai jenis alat bukti dalam Pasal 184 KUHAP dan Pasal 5 UU ITE.

Berkaitan dengan hal tersebut, maka dapat diajukan saran yaitu: *Pertama*, perlunya dilakukan penelitian lebih lanjut mengenai eksistensi dan pengaturan hukum mengenai penyitaan dan pembekuan alat bukti elektronik beserta dengan prosedurnya untuk dapat digunakan dalam persidangan. Mengingat, belum adanya aturan hukum yang jelas yang menjadi dasar tindakan penyitaan dan pembekuan alat bukti elektronik yang dalam hal ini terutama adalah penyitaan atas akun, serta prosedur dari penyitaan atas akun atau alat bukti elektronik hanya sejauh pengambilalihan akses. Hal ini dipandang kurang memadai mengingat alat bukti elektronik seperti juga akun, terhubung dengan jaringan yang aksesnya tidak dapat tertutup apabila hanya mengambil alih akses dengan pengambilan password atau pin saja. *Kedua*, perlunya penggunaan jenis alat bukti lain untuk pembuktian terhadap tindak pidana penciptaan informasi elektronik palsu untuk lebih memenuhi unsur-unsur tindak pidana penciptaan informasi elektronik palsu yang dapat mengacu pada ketentuan Pasal 184 KUHAP dan Pasal 5 UU ITE.

DAFTAR REFERENSI

Buku

- Chazawi A dan Ferdian A, *Tindak Pidana Informasi & Transaksi Elektronik* (ed. revisi Media Nusa Creative 2015).
- Harahap MY, *Pembahasan Permasalahan dan Penerapan KUHAP* (Jilid II, Pustaka Kartini 1993).
- Makarim E, *Kompilasi Hukum Telematika* (PT RajaGrafindo Persada 2004).
- Marpaung L, *Unsur-Unsur Perbuatan yang Dapat Dihukum (Delik)* (Sinar Grafika 1991).
- Sitompul J, *Cyberspace Cybercrimes Cyberlaw Tinjauan Aspek Hukum Pidana* (PT Tatanusa 2012)
- Sutarman, *Cybercrime Modus Operandi dan Penanggulangannya* (Laksbang Pressindo 2007)

Artikel Jurnal

- Aripin S, Ginting GL, Silalahi N, 'Penerapan Metode Retinex Untuk Meningkatkan Kecerdasan Citra Pada Hasil Screenshot' (2017) 1 (1) Media Informatika Budidarma.
- Heryogi A, Ruba'I M, Sugiri B, 'Fungsi Bukti Elektronik Dalam Hukum Acara Pidana Pasca Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016' (2017) 2 (1) Jurnal Ilmiah Pendidikan Pancasila Dan Kewarganegaraan.
- Huda MN, 'Pentingnya Alat Bukti Dalam Pembuktian Minim Saksi (The Importance of The Evidence in Proof of Minimal Witness)' (2017) 1 (2) Voice Justisia.

Isma NL dan Koyimatun A, 'Kekuatan Pembuktian Alat Bukti Informasi Elektronik Pada Dokumen Elektronik Serta Hasil Cetaknya Dalam Pembuktian Tindak Pidana' (2014) 1 (2) Jurnal Penelitian Hukum.

Mardiansyah A, 'Mekanisme Pembuktian Dalam Perkara Tindak Pidana Siber (The Verification Mechanisms In The Event Of Cyber Crime)' (2015) 12 (4) Jurnal Legislasi Indonesia.

Mir SS, Shoaib U, Sarfraz SM, 'Analysis Of Digital Forensic Investigation Models' (2016) 14 (11) International Journal of Computer Science and Information Security.

Samudra AH, 'Modus Operandi dan Problematika Penanggulangan Tindak Pidana Penipuan Daring' (2019) 31 (1) Mimbar Hukum.

Seminar

Kemitraan Partnership, LeIP, IDLO, Kingdom of the Netherland, 'Booklet Bukti Elektronik di Indonesia Pengaturan Tentang Perolehan, Pemeriksaan, dan Pengelolaan Bukti Elektronik (Electronic Evidence)' (Seminar Publik, Menuju Pengaturan Bukti Elektronik yang Akuntabel, LEIP dan Kemitraan, Surabaya, 24 Juli 2019).

Kemitraan dan Lembaga Kajian dan Advokasi Untuk Independensi Peradilan, 'Naskah Akademik Kerangka Hukum Perolehan, Pemeriksaan, dan Pengelolaan Bukti Elektronik (Electronic Evidence)' (Seminar Publik, Menuju Pengaturan Bukti Elektronik yang Akuntabel, LEIP dan Kemitraan, Surabaya, 24 Juli 2019).

Putusan Pengadilan

Putusan Mahkamah Konstitusi Republik Indonesia Nomor 20/PUU-XIV/2016, Mahkamah Konstitusi, 7 September 2016.

Asep Supriatna Bin Dayat, Nomor 43/Pid.Sus/2018/PN Mjl, Pengadilan Negeri Majalengka, 16 Mei 2018.

Peraturan Perundang-Undangan

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana.

Peraturan Menteri Komunikasi dan Informatika Nomor 7 Tahun 2016 tentang Administrasi Penyidikan dan Penindakan Tindak Pidana di Bidang Teknologi Informasi dan Transaksi Elektronik.