ISSN (p) 2354-9629 ISSN (e) 2549-1334

WASPADA *CYBERCRIME* DAN INFORMASI *HOAX* PADA MEDIA SOSIAL FACEBOOK

Machsun Rifauddin* dan Arfin Nurma Halida*

Pengutipan: Rifauddin, M., Halida, A. N. (2018). Waspada *cybercrime* dan informasi *hoax* pada media sosial facebook. *Khizanah al-Hikmah* : *Jurnal Ilmu Perpustakaan, Informasi, dan Kearsipan*. 6(2), 98-111.

DOI: https://doi.org/10.24252/kah.v6i2a2

**Institut Agama Islam Negeri Tulungagung*
Email korespondensi: machsunr@yahoo.com, arfin.nurma.halida19@gmail.com

ABSTRAK

Informasi dengan sangat mudah tersebar menggunakan teknologi informasi dan internet saat ini. Namun berbagai permasalahan muncul akibat penyalahgunaan teknologi tersebut, seperti cybercrime dan penyebaran informasi hoax. Kontrol informasi sangat penting untuk mengevaluasi kredibilitas informasi dan sumbernya. Penelitian ini menjelaskan bagaimana mengatasi cybercrime dan hoax melalui seleksi informasi yang tepat. Pendekatan kualitatif dengan metode studi kepustakaan digunakan dalam penelitian ini serta delengkapi dengan data dan dokumen. Hasil penelitian menunjukkan bahwa cybercrime dan penyebaran informasi hoax masih terjadi bahkan sampai saat ini. Terdapat tiga ancaman UU ITE di Indonesia yang berpotensi menimpa pelaku cybercrime dengan memanfaatkan facebook yaitu ancaman pelanggaran kesusilaan pasal 27 ayat (1), penghinaan atau pencemaran nama baik pasal 27 ayat (3), dan penyebaran kebencian berdasarkan suku, agama, ras dan antar golongan (SARA) pasal 28 ayat (2). Upaya untuk mencegah cybercime dapat dilakukan dengan cara melindungi komputer dari virus, menjaga privasi, mengamankan e-mail, melindungi Id/Account, membuat backup data, dan selalu up to date terhadap informasi. Terdapat beberapa faktor yang harus diperhatikan dalam menyeleksi sumber informasi dari internet agar terhindar dari bahaya cybercrime, yaitu: relevansi, akurasi, otoritas reputasi, objektivitas, kekinian, cakupan, bukti yang kuat, serta bahasa dan gaya penulisan.

Kata kunci: Cybercrime; hoax; internet; media sosial; facebook; UU ITE

ABSTRACT

Information is very easily spread use of information technology and the internet today. But various problems arise out due to the abuse of this technology, such as cybercrime and dissemination hoax. Control of information is very important to evaluate the credibility of the information and its source. The study explains how to overcome cybercrime and hoax through the selection of appropriate information. Qualitative approach with literature study method was used in this research and complemented by data and document. The results showed that cybercrime and hoax information still occur even today. There were three threats of UU ITE in Indonesia that could potentially overwrite the perpetrators of cybercrime by utilizing facebook; the threat of moral violation in article 27 section (1), insults or defamation in article 27 section (3), and the dissemination of hatred based on ethnic, religion, race and intergroup (SARA) in article 28 section (2). Efforts to prevent cybercime can be done by protecting the computer from viruses, maintaining privacy, secure e-mail, protecting ID/account data, making backups, and always up to date to information. There are several factors that must be considered in selecting the source of information from the internet to avoid the dangers of cybercrime; relevance, accuracy, authority of reputation, objectivity, currency, coverage, strong evidence, as well as the language and style of writing.

***Keywords*: Cybercrime; hoax; internet; social media; facebook; UU ITE**

1. PENDAHULUAN

Kemajuan teknologi informasi saat ini telah membawa dampak besar terhadap perubahan sosial masyarakat di dunia, termasuk juga perubahan perilaku dalam pencarian informasi. Hal ini didukung oleh adanya internet sebagai media pencarian informasi yang canggih. Perkembangan pengguna internet sendiri mengalami peningkatan yang sangat signifikan di mana hingga saat ini lebih dari delapan triliun halaman *interface* pada web dan tidak mungkin dapat membaca semuanya, bahkan hanya melihatpun tidak mungkin sampai selesai (Yusuf & Subekti, 2010: 121). Penelusuran informasi melalui internet sendiri sudah menjadi tren terkini bagi kalangan masyarakat baik itu akademisi maupun non akademisi. Penetrasi pengguna internet di Indonesia pada Tahun 2016 sebesar 132,7 juta jiwa, dan meningkat pada Tahun 2017 menjadi 143,26 juta jiwa dari total populasi penduduk Indonesia 262 juta orang (APJII, 2017). Sedangkan berdasarkan survei *We Are Social* (2018) menunjukkan jumlah pengguna internet di dunia pada kuartal kedua 2018 sebesar 4.087 miliar, dengan jumlah pengguna media sosial facebook mencapai total 2,234 miliar dan Indonesia menempati urutan ketiga terbanyak pengguna facebook setelah India dan Amerika.

Sumber informasi dapat dikategorikan sebagai sumber informasi cetak dan non cetak (*electronic*), dalam hal ini sumber informasi dari internet termasuk dalam kategori sumber informasi non cetak. Internet sebagai sumber informasi non-cetak memiliki banyak kelebihan dari segi kemudahan, kecepatan dan ketepatan, kapasitas (*free space*), kerahasiaan, efisiensi dan keefektifan (Yusuf & Subekti, 2010; 57-59). Tanpa disadari kehadiran internet saat ini memudahkan seseorang dalam mengakses informasi dari berbagai penjuru dunia, berinteraksi satu sama lain tanpa harus bertatap muka. Pada sisi lain, penggunaan internet yang nyaris tanpa kendali menyebabkan berbagai tindak kejahatan di dunia maya, angka kejahatan *online* alias *cybercrime* telah menjadi tren baru di banyak negara saat ini, termasuk di Indonesia kejahatan tersebut terjadi sejak tahun 1983 (Widodo, 2013: 30). *Cybercrime* merupakan setiap aktifitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, dan komputer sebagai sasaran kejahatan (Widodo, 2013: 4).

Kasus besar terkait *cybercrime* di Indonesia adalah pembajakan website resmi mantan Presiden Republik Indonesia Susilo Bambang Yudhoyono pada tahun 2013 yang membuktikan kerentanan jaringan sistem teknologi informasi di Indonesia dan dunia Internasional (Widodo, 2013: III). Kejahatan *cyber* meningkat sangat cepat seiring dengan perkembangan teknologi, dan penyelidikan kejahatan *cyber* menjadi tugas yang sangat rumit untuk dilakukan tanpa kerangka kerja yang tepat (Poonia, 2014: 119). Tindak pidana *cybercrime* di Indonesia telah di atur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Pasal 27 dan 28, namun penerapanya belum maksimal sampai pada saat ini, terbukti dalam pembuktian mengenai *cybercrime* Kitab Undang-Undang Hukum Acara Pidana belum mengatur mengenai informasi elektronik sebagai salah satu alat bukti (Windara & Sukranatha, 2013: 5).

Cybercrime dengan sangat mudah menyebar dan berkembang di media sosial, karena media sosial menyediakan *platform* bagi penggunanya untuk berbicara tentang apa pun topik tanpa

sensor atau kontrol yang diawasi (Goyal, 2012: 16). Sebagai contoh facebook yang memungkinkan penggunanya berinteraksi dengan orang lain baik yang dikenal maupun tidak, sehingga membuka peluang bagi kejahatan dunia maya seperti, penculikan, perdagangan manusia (*trafficking*), hingga pembunuhan (Jayanti, dkk, 2016: 30), dan yang paling sering dijumpai di facebook adalah penyebaran informasi atau berita *hoax*.

Indonesia merupakan negara demokrasi terbesar ketiga di dunia setelah India dan Amerika yang mengalami permasalahan serius soal penyebaran berita palsu (*fake news/hoax*) (Firmansyah, 2017: 230). *Hoax* telah menyebar seperti virus yang bermula dari para pembuat berita, opini, data, foto, dan gambar yang mengandung *hoax* dan dibagikan melalui media sosial seperti facebook, twitter, whatsapp, line, youtube, path, dan instagram (Triartanto, 2015: 33). Setidaknya sampai saat ini masih banyak masyarakat yang belum memahami dengan benar dan tanpa sengaja melakukan aktifitas yang mengandung unsur *cybercrime* di media sosial. Oleh sebab itu perlu kajian ulang mengenai *cybercrime* dan *hoax* serta upaya untuk menanggulanginya.

2. KAJIAN PUSTAKA

a. Informasi dan Sumber Informasi Internet

Informasi merupakan salah satu istilah atau kata yang sering digunakan dalam kehidupan sehari-hari hingga saat ini. Dalam *Oxford English Dictionary*, informasi mempunyai pengertian, "1) *The action of informing*; *The action of telling or fact of being told of something*, 2) *That which one is apprised or told; intelegence, news*" (Case, 2007: 40-42). Sementara, dalam KBBI online, informasi mempunyai arti, yaitu, "1) penerangan; 2). pemberitahuan; kabar atau berita tentang sesuatu; 3). keseluruhan makna yang menunjang amanat yang terlihat dalam bagian-bagian amanat itu". Pengertian informasi menurut Estabrook, adalah suatu rekaman fenomena yang diamati, atau bisa juga berupa putusan-putusan yang dibuat (Yusuf & Subekti, 2010: 1). Sedangkan menurut Basuki (2010: 135) informasi adalah sesuatu yang mempengaruhi atau mengubah status pikiran. Informasi dapat dipahami sebagai segala sesuatu yang memberikan penerangan, atau pemberitahuan yang mempunyai nilai penting, dan dapat mempengaruhi atau mengubah status pikiran manusia. Informasi merupakan suatu kebutuhan yang penting bagi manusia, dengan adanya informasi maka manusia akan mengetahui kejadian-kejadian baru yang saat ini terjadi di kehidupan dan lingkungan sekitar.

Jika diibaratkan informasi itu ialah isi, maka sumber informasi adalah wadah dari isi tersebut (Basuki, 2010: 15). Sumber informasi dapat dipahami dan diartikan sebagai tempat berkumpulnya informasi dan tempat dimana informasi itu berasal. Sumber informasi jika dilihat berdasarkan jenisnya sangat beragam, antara lain manusia, koran, televisi, VCD, *e-mail*, internet, dll. Informasi yang terekam dari berbaga media termasuk internet, merupakan benda mati apabila tidak memberikan manfaat atau digunakan (Yusuf dan Subekti, 2010: 120). Adapun sumber informasi yang terkait dengan kegiatan ilmiah adalah buku, jurnal, standar, paten, *thesis*, laporan penelitian, yang tersedia di perpustakaan atau dapat di akses melalui internet, pangkalan data, maupun katalog secara online (Hartina, dkk, 2012: 12). Selain perpustakaan, internet merupakan media yang sering digunakan oleh masyarakat dalam melakukan penelusuran informasi. Hal ini dikarenakan internet merupakan media yang bisa digunakan dengan tanpa batas. Internet adalah sebuah jaringan yang dibuat sedemikian rupa sehingga dapat menghubungkan perangkat komputer dari berbagai wilayah sehingga masing-masing data dapat ditransmisikan ke dalam jaringan dan dapat diakses dari berbagai wilayah (Yusuf dan Subekti, 2010: 55).

b. *Cybercrime* dan Penyebaran Berita Palsu (*Hoax*)

Pada awalnya *cybercrime* didefinisikan sebagai kejahatan komputer. Para sarjana sendiri mendeskripsikan *cybercrime* dengan menggunakan beberapa istilah seperti "*computer misuse*", "*computer abuse*", "*computer fraud*", "*computer-related crime*", atau "*computer crime*", dari beberapa definisi tersebut "*computer crime*" yang lebih luas dan biasa digunakan dalam dunia internasional (Puslitbang Hukum dan Peradilan MA RI, 2004: 4). *The British Law Commission* dalam Suhariyanto mengartikan "*computer fraud*" sebagai manipulasi komputer dengan cara apapun yang dilakukan dengan iktikad buruk untuk memperoleh uang, barang atau keuntungan lainnya atau dimaksudkan untuk menimbulkan kerugian pada pihak lain (Widodo, 2013: 9-10). *Cybercrime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan/ atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital (Wahid & Labib, 2005: 40). Sedangkan Mansur (2005: 10) mendiskripsikan *cybercrime* dengan segala tindak pidana yang berkenaan dengan sistem informasi, sistem informasi (*information system*) itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian/ pertukaran informasi kepada pihak lainnya (*transmitter/originator to reciptient*). Secara garis besar *cybercrime* dapat diartikan sebagai segala bentuk tidak kriminal/perbuatan melanggar hukum yang memanfaatkan teknologi komputer berbasis pada kecanggihan perkembangan teknologi internet. Sedangkan penjahat *cyber* adalah orang yang melakukan tindakan ilegal dengan niat bersalah atau melakukan kejahatan dalam konteks kejahatan dunia maya (Poonia, 2014: 119). Sama seperti kejahatan konvensional, *cybercrime* juga terdiri dari banyak tipe. Berbagai bentuk kejahatan yang dapat dikategorikan sebagai *cybercrime*, diantaranya *e-mail crime*, *hacking*, *cyber terrorism*, *financial crime*, *cyber pornography*, *cyber stalking*, dsb. (lihat Poonia, 2014: 120). Termasuk salah satu bentuk *cybercrime* adalah penyebaran berita palsu (*hoax*), yaitu artikel berita yang sengaja dibuat untuk menyesatkan pembaca (Firmansyah, 2017: 231). *Hoax* merupakan sebuah isu atau informasi palsu yang dibuat dan disebarkan oleh seseorang atau kelompok dengan maksud dan tujuan tertentu. Informasi *hoax* ini muncul seiring dengan perkembangan teknologi informasi saat ini. Informasi *hoax* biasanya disebarkan oleh orang yang membuat informasi namun tidak menutup kemungkinan orang lain yang tanpa sengaja menyebarkan informasi tersebut karena kurangnya pemahaman.

c. Kategori Pelaku *Cybercrime*

Skema taksonomi atau klasifikasi yang dilakukan (Rogers dalam Ghosh dan Turrini, 2010: 2018-220), menghasilkan tujuh kategori perilaku kriminal *cybercrime* yang meliputi:

1) *Script Kiddies*: Individu dengan pengetahuan teknis terbatas dan menganggap menyerang suatu sistem adalah sensasi menggetarkan dan memberikan dorongan adrenalin, tidak memahami konsekuensi dari tindakan mereka, cenderung memiliki pemahaman moral yang belum berkembang, sering sesumbar tentang eksploitasi mereka dan mencari perhatian dan menyerang ego orang lain.
2) *Cyber-punks*: yaitu kelompok yang memperluas mentalitas "*punk*" dunia nyata ke dalam dunia maya, tidak menghormati otoritas dan simbolnya serta mengabaikan norma-norma kemasyarakatan. Kelompok ini didominasi oleh laki-laki berusia 12 hingga 18 tahun, dan mereka telah memahami konsekuensi dari tindakan mereka, tetapi masih kurang peduli karena konsekuensi terhadap diri mereka masih sangat ringan.
3) *Hacktivist*: Individu atau kelompok yang hanya mencoba menyembunyikan tindakan mereka dibalik semantik kamuflase untuk menyamarkan tindakan menyimpangnya, cenderung membenarkan perilaku destruktif mereka, termasuk merusak situs web, dengan label

"pembangkangan publik" dan pembenaran politik dan moral atas perilakunya. Motif pelaku ini adalah balas dendam, kekuasaan, keserakahan, pemasaran, atau perhatian media.

4) *Thieves*: Termasuk kategori penjahat biasa, dan motivasi utama kelompok ini adalah uang dan keserakahan. Kejahatan yang dilakukan biasanya adalah penipuan transfer bank dan penyalahgunaan nomer kartu kredit, serta pencurian identitas.
5) *Virus Writers*: Sensasi individu berasal dari tantangan mental dan latihan akademis yang terlibat dalam penciptaan virus, namun sering kali orang yang menyebarkan virus bukanlah orang yang menciptakannya dan orang ini memiliki karakteristik dan motivasi yang mirip dengan kelompok *cyber-punks*, yaitu menginginkan perhatian, pencarian sensasi, dan tidak takut sanksi.
6) *Profressional*: Kategori kelompok yang paling elit dalam kelompok penjahat *cyber*, yang memiliki inteligensi kompetitif dan aktivitas yang abu-abu. Kelompok ini terlibat dalam penipuan tingkat tinggi hingga spionase korporat, dan menjual informasi dan kekayaan intelektual mereka kepada penawar tertinggi. Bagi kelompok ini, kegiatan kriminal adalah sebuah pekerjaan dan mereka sangat profesional.
7) *Cyber-terrorist*: Merupakan bagian dari militer atau paramiliter sebuah negara dan diposisikan sebagai tentara maupun sebaliknya sebagai pejuang pembebasan dalam medan peperangan di dunia maya. Kelompok ini menjalankan dua fungsi yaitu menyerang sistem pertahanan musuh dan melindungi sistemnya sendiri dari serangan serupa dari pihak lawan.

d. Undang-Undang yang Mengatur *Cybercrime* di Indonesia

Cybercrime (kejahatan dunia maya) di Indonesia diatur dalam Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU-ITE). Dalam UU ITE tersebut diatur tentang bentuk-bentuk *cybercrime* di Indonesia yaitu sebagai berikut:

1) *Cybercrime* yang berkaitan dengan perbuatan mengakses komputer dan/ atau sistem elektronik milik orang lain secara tidak sah, yaitu:
   a) Distribusi atau penyebaran, transmisi, dapat diaksesnya isi (muatan) yang tidak sah, yang mengandung unsur-unsur berikut:
      (1) Bertentangan dengan rasa kesusilaan sebagai mana di atur dalam pasal 27 ayat 1
      (2) Perjudian sebagaimana diatur dalam pasal 27 ayat 2
      (3) Penghinaan atau pencemaran nama baik sebagaimana di atur dalam pasal 27 ayat 3
      (4) Pemerasan atau pengancaman sebagimana dalam pasal 27 ayat 4.
      (5) Berita bohong yang menyesatkan dan merugikan konsumen sebagaimana diatur dalam pasal 28 ayat 1
      (6) Menimbulkan rasa kebencian berdasarkan suku, agama, ras, dan antar golongan (SARA) sebagaimana diatur dalam pasal 28 ayat 2
      (7) Informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan kepada pribadi sebagaimana di atur dalam pasal 29 (Widodo, 2013: 9).
   b) Dengan cara apapun mengakses secara tidak sah terhadap sistem elektronik sebagaimana diatur dalam pasal 30.
   c) Intersepsi tidak sah terhadap informasi atau dokumen elektronik dan sistem elektronik sebagaimana diatur dalam pasal 31
2) Tindak pidana yang berkaitan dengan gangguan (interpensi) terhadap informasi atau dokumen elektronik, yaitu terdiri atas perbuatan berupa:
   a) Gangguan terhadap informasi atau dokumen elektronik sebagaiman di ataur dalam pasal 32
   b) Gangguan terhadap sistem elektronik sebagaimana diatur dalam pasal 33
3) Tindak pidana yang memfasilitasi perbuatan yang dilarang oleh hukum sebagaimana diatur dalam pasal 34.

4) Tindak pidana pemalsuan informasi atau dokumen elektronik sebagaimana diatur dalam pasal 35 (Widodo, 2013: 9-10).

Cybercrime dapat dipahami sebagai kejahatan dalam arti yuridis, yaitu kejahatan yang kualifikasinya sudah diatur dalam undang-undang. Namun aplikasi dari semua ketentuan hukum pidana di Indonesia tersebut tunduk pada "ketentuan induk" hukum pidana, yaitu ketentuan KUHP (Widodo, 2013: 10).

3. METODOLOGI PENELITIAN

Penelitian ini dilakukan dengan menggunakan pendekatan kualitatif dengan metode studi kepustakaan. Analisis data dilakukan dengan mengumpulkan sejumlah literatur baik dari buku, jurnal, *website* ataupun karya ilmiah lain, selanjutnya dianalisis dan disimpulkan dalam pembahasan hasil penelitian. Tujuan dari penelitian ini adalah untuk menjelaskan unsur-unsur apa saja yang termasuk dalam kategori pidana *cybercrime* khususnya di media sosial facebook, dan diharapkan pembaca mampu memahami secara lebih mendalam mengenai *cybercrime* dan penerapan UU ITE melalui beberapa kasus yang dipaparkan penulis dalam penelitian ini. Sehingga *feedback* bagi pembaca agar lebih berhati-hati dalam menggunakan media sosial khususnya media sosial facebook.

4. HASIL PENELITIAN DAN PEMBAHASAN

a. Kasus *Cybercrime* di Facebook dan Ancaman Pidana UU ITE

Internet menyediakan berbagai sumber informasi yang bisa memenuhi kebutuhan informasi penggunanya. Sumber informasi yang ada di internet sangat banyak tanpa batas dan bisa diakses dengan fasilitas *online*. Koleksi dari fasilitas online baik berbayar maupun tidak berbayar (*free*) jumlah setiap harinya terus bertambah, dan sumber informasi tersebut bisa diakses dimana saja dan kapan saja tanpa melihat ruang dan waktu. Salah satu produk perkembangan teknologi dan internet saat ini adalah facebook. Facebook adalah sebuah layanan jejaring sosial dan situs web yang diluncurkan pada 4 Februari 2004, yang dibuat oleh Mark Zuckerberg, seorang mahasiswa Harvard kelahiran 14 Mei 1984. Facebook merupakan situs media sosial di mana seseorang dapat berinteraksi, berbagi data dan informasi, serta menjalin relasi sesama penggunanya (Jayanti, dkk, 2016: 30). Facebook menurut Madcoms (2010: 1) adalah suatu situs jejaring sosial yang dapat dijadikan sebagai tempat untuk menjalin hubungan pertemanan dengan seluruh orang yang ada di belahan dunia untuk dapat berkomunikasi satu dengan yang lainnya. Facebook merupakan situs pertemanan yang dapat digunakan oleh manusia untuk bertukar informasi, berbagi foto, video, dan lainnya.

Penggunaan media sosial facebook yang tanpa kontrol terkadang menimbulkan dampak negatif bagi penggunanya seperti kasus *cybercrime*. Beberapa contoh kasus *cybercrime* yang pernah terjadi pada media sosial facebook di Indonesia antara lain:

1) Kasus Pornografi/Asusila via Facebook

Sebagaimana di lansir majalah Tempo (16 April 2014) Direktorat Tindak Pidana Khusus Ekonomi Badan Reserse Kriminal Mabes Polri mengungkap kasus pornografi anak melalui media Facebook dan Kaskus di Surabaya, Jawa Timur. Kasus yang terjadi tersebut menimpa korban enam anak di bawah umur. Polisi berhasil mengidentifikasi pelaku dan menetapkan manajer PT. KSM yang

berinisial TAG sebagai tersangka. Kasus yang dilakukan tersangka termasuk dalam ranah *cybercrime*. Pelanggaran yang dilakukan pelaku *cybercrime* sesuai dengan kasus pornografi/asusila via facebook di atas sesuai dengan ketentuan Pasal 27 ayat (1) UU ITE dan ancaman pidana bagi pelanggar pasal tersebut adalah sesuai yang dijelaskan pada Pasal 45 ayat (1) UU ITE yaitu pidana penjara paling lama enam tahun dan/atau denda paling banyak satu miliar rupiah. Apabila dipahami secara lebih mendalam, ketentuan pasal 27 ayat (1) UU ITE memiliki cakupan yang sangat luas. Cakupan tersebut bisa saja setiap *user/member* facebook yang memberikan gambar-gambar senonoh atau memberikan *hyperlink* ke sebuah situs yang memiliki muatan pornografi atau jasa penjualan seks komersial dan memanfaatkan facebook sebagai tempat transaksi juga dapat dikenakan dalam pasal ini. Meskipun pengertian porno sendiri masih sangat kabur dan tidak dapat diinterpretasikan dengan jelas, misalnya gambar tersebut dikategorikan sebagai unsur seni fotografi. Dalam hal ini tentunya diperlukan prosedur dan pemahaman lebih mendalam dari para penyidik dan hakim.

2) Kasus Pencemaran Nama Baik Lewat Facebook

Rektor IKIP Mataram, NTB, melaporkan dosen Bahasa Inggris Fakultas Pendidikan Bahasa dan Sastra Institut Keguruan dan Ilmu Pendidikan Mataram ke polisi. Dosen tersebut yang menyamarkan identitasnya di facebook menjadi Chunk Jagger kerap menuliskan hinaan kepada Said. Menurut Kasubag Humas Polres Mataram, kemungkinan terlapor akan dikenakan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) (Hazliansyah, 2012). Kasus pencemaran nama baik yang dilakukan seseorang baik senganja maupun tidak sengaja dapat dikenakan Pasal 27 ayat (3) UU ITE tentang penyebaran dokumen elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik, dan ancaman pidana bagi pelanggar pasal tersebut adalah sesuai yang dijelaskan pada Pasal 45 ayat (1) UU ITE yaitu pidana penjara paling lama enam tahun penjara dan/atau denda paling banyak satu miliar rupiah. Dalam ketentuan pasal 27 ayat (3) dan pasal 45 ayat (3) Undang-Undang ITE tersebut tidak terdapat definisi secara jelas apa yang dimaksud dengan penghinaan atau pencemaran nama baik. Untuk menentukan secara jelas apa yang dimaksud dengan penghinaan atau pencemaran nama baik, harus merujuk pada ketentuan pasal 310 ayat (1) KUHP mengenai pencemaran lisan (*smaad*), pasal 310 ayat (2) mengenai pencemaran tertulis (*smaadscrifft*), dan pasal 310 ayat (3) sebagai penghapusan pidana (untuk kepentingan umum dan pembelaan terpaksa). Ketentuan dari Pasal 27 ayat (3) UU ITE dapat kita pahami bahwa cakupan pasal tersebut juga cukup luas. Mengenai, perbuatan memberikan *hyperlink* ke sebuah situs yang memiliki muatan penghinaan atau pencemaran nama baik juga dapat dijerat unsur ketiga pasal tersebut. Karena itu mungkin dapat dipahami mengapa sebagian orang melihat pasal tersebut sebagai ancaman serius bagi pengguna facebook pada umumnya. Disisi lain, dalam UU ITE juga dinyatakan bahwa suatu informasi/ dokumen elektronik tidak dengan serta-merta atau otomatis akan menjadi suatu bukti yang sah. Untuk menentukan apakah informasi/ dokumen eletronik dapat menjadi alat bukti yang sah masih memerlukan suatu prosedur tertentu yang diatur berdasarkan undang-undang tersebut. Dalam UU No. 11 Tahun

2008 tentang ITE ini berlaku untuk semua orang yang memberikan suatu informasi yang memiliki unsur penghinaan. Oleh karena itu, etika dalam berkomunikasi menggunakan media sosial harus tetap dijaga oleh segenap masyarakat.

3) Kasus Penyebaran kebencian berdasarkan suku, agama, ras dan antar golongan (SARA)

Menurut laporan merdeka.com dalam Mangadil (2016: 124) menyatakan bahwa status facebook salah seorang mahasiswa inisial IRF pada 16 Maret 2010 memicu kemarahan masyarakat Bali, yang mayoritas beragama Hindu. Sebab di saat mayoritas masyarakat Bali menggelar ritual Nyepi, ia malah menulis status yang memicu konflik. Status tersebut langsung menuai komentar kemarahan dari sejumlah temannya di akun tersebut, hingga akhirnya yang bersangkutan menuliskan status terbaru yang menyatakan permintaan maaf kepada seluruh masyarakat Bali, khususnya yang beragama Hindu. Namun sejumlah grup bermunculan yang menyatakan penentangan, dan salah satu grup menggalang dukungan untuk mengusir IRF dari Bali.

Kasus tentang SARA sebenarnya telah menjadi masalah besar masyarakat di dunia, dan kasus seperti ini sangat sering terjadi di Indonesia mengingat masyarakat Indonesia yang beraneka ragam, terdiri dari banyak suku, ras, golongan bahkan agama sehingga memungkinkan terjadinya ketegangan antara golongan tersebut. Kata-kata dalam bentuk hinaan atau pencemaran nama baik dan dapat menimbulkan rasa kebencian bagi seseorang atau golongan (SARA), dan dapat dikenakan Pasal 28 ayat (2) UU ITE dengan ancaman pidana sebagaimana dijelaskan pada Pasal 45A ayat (2) UU ITE yaitu pidana penjara paling lama enam tahun dan/atau denda paling banyak satu miliar rupiah. Ababila digeneralisasikan, ancaman pidana ini juga dapat menjerat seseorang yang memberikan *hyperlink* ke sebuah situs yang memiliki muatan berbau SARA ataupun status facebook yang dianggap mengandung SARA dan bisa juga komentar-komentar di facebook yang mengakibatkan kelompok, suku atau agama lain terusik ketenangannya. Pada kasus ini tidak terlalu banyak pihak yang dirugikan secara finansial/materi maupun ekonomi, namun yang jadi permasalahan adalah dampak yang ditimbulkan. Penghinaan terhadap kepercayaan atau agama dapat menimbulkan ketidaknyamanan atau bahkan kerusuhan antar umat beragama.

4) Kasus Penyebaran Informasi bohong (*Hoax*)

Termasuk dalam ranah *cybercrime* yang paling familiar saat ini adalah penyebaran informasi bohong (*hoax*). Apabila penyebaran informasi *hoax* ini mengandung unsur-unsur pelanggaran sebagaimana dijelaskan pada UU ITE maka juga dapat dikenakan pidana. Kasus terbaru menimpa salah seorang dosen Pegawai Negeri Sipil (PNS) Universitas Sumatera Utara (USU). Direktorat Krimsus Subdit *cybercrime* Polda Sumatera Utara menangkap tersangka karena salah satu postingan akun facebook yang menyebutkan kalau 3 bom gereja di Surabaya hanyalah pengalihan isu hingga menjadi viral dan mengundang perdebatan *netizen* karena diduga mengandung unsur ujaran kebencian (SARA) (TribrataNews, 2018).

Masyarakat media *cyber* telah terbiasa dengan segala teks yang cenderung *hoax*, sehingga sulit membedakan informasi mana yang benar dan yang bohong (Triartanto, 2015: 33). Meskipun tidak

terlihat secara langsung, dampak yang ditimbulkan daripada penyebaran informasi *hoax* ini, banyak pihak yang dirugikan diberbagai sektor, mulai dari masalah politik, ekonomi, dan sosial. Setidaknya sampai saat ini penyebaran informasi *hoax* di Indonesia semakin tumbuh subur dan merajalela seakan tidak ada kontrol. Maka dari itu setiap pengguna facebook diharapkan memahami secara mendalam mengenai aturan-aturan dalam UU ITE kaitannya dengan ranah pidana *cybercrime* dan penyebaran informasi *hoax*.

b. Upaya untuk Mengatasi Bahaya *Cybercrime*

Pengguna media sosial khususnya facebook diharapkan berhati-hati dan menjaga etika agar tidak terjadi pelanggaran hukum *cybercrime*. Beberapa contoh kasus di atas dapat dijadikan peringatan bagi siapa saja yang secara sengaja ataupun tidak untuk tidak menyalahgunakan media sosial sebagai tempat pencurahan kata-kata penghinaan atau sejenisnya. Beberapa cara yang dapat dilakukan untuk mengatasi bahaya *cybercrime* adalah:

1) Melindungi komputer. *Cybercrime* seringkali dilakukan pelaku melalui penyebaran virus melalui internet. Setidaknya setiap pengguna komputer perlu mengaplikasikan beberapa program untuk menjaga keamanan, yaitu *antivirus, antispyware*, dan *firewall*. Fungsi dari ketiga aplikasi tersebut menjaga perangkat komputer dari virus yang semakin beragam. Persepsi masyarakat Indonesia terhadap keamanan internet dengan pemasangan *anti-virus* sebesar 58,52% (APJII, 2017). Itu artinya sebagian besar masyarakat pengguna internet di Indonesia belum menyadari arti pentingnya sebuah keamanan *cyber*, dan ini memungkinkan terjadinya *cybercrime*.
2) Menjaga privasi (identitas diri). Pelaku *cybercrime* pastinya tidak akan melakukan kejahatan menggunakan identitasnya sendiri melainkan memanfaatkan identitas orang lain. Oleh sebab itu, kerahasiaan identitas bagi segenap pengguna internet sangat penting, dan jangan sesekali memberitahukan identitas penting seperti NIK, nomor rekening, tanggal lahir, dsb kepada orang lain yang belum dikenal, karena akan sangat mudah disalah gunakan oleh pelaku kejahatan *cyber*. Selain itu, penguna internet harus selalu berhati-hati dan waspada apabila mengisi identitas diri pada aplikasi atau situs web yang kurang terpercaya, biasaya pelaku *cybercrime* mengarahkan *user* pada sebuah *link* dan meminta untuk memasukkan biodata. Hanya 61,38% masyarakat pengguna internet di Indonesia yang menyadari pentingnya menjaga kerahasiaan data (APJII, 2017), dan itu yang menjadi salah satu faktor *cybercrime* tumbuh subur di Indonesia.
3) Mengamankan *e-mail*. Salah satu bentuk *cybercrime* yang paling mudah dan sering digunakan pelaku adalah penyerangan *e-mail*. Pengguna *e-mail* harus waspada setiap menerima atau mengirim *e-mail* yang belum diketahui identitasnya dengan jelas. Jika menerima *e-mail* dari seseorang yang tidak diketahui identitasnya dengan pesan yang aneh atau mengarahkan pada *link* tertentu maka sebaiknya abaikan. Selain itu juga harus mewaspadai *e-mail* palsu yang sekarang banyak digunakan pelaku *cybercrime*.
4) Melindungi *ID/account*. Penggunaan kata sandi dalam sebuah aplikasi selain mudah diingat juga harus bervariasi (susah ditebak). Setiap kali membuat

kata sandi pada sebuah aplikasi sebaiknya menggunakan kombinasi angka, huruf, dan simbol, agar tidak mudah diketahui orang lain atau dibajak. Menggunakan password yang sulit dan bervariasi merupakan tindakan tepat guna menghindari *cybercrime*. Selain itu, sebaiknya password harus rutin diubah secara berkala, dan mengeluarkan akun (*log-out*) dari aplikasi setiap meninggalkan komputer (biasanya dalam penggunaan komputer kantor atau warnet).

5) Membuat *backup* atau salinan data. Para pengguna komputer sebaiknya memiliki salinan dari dokumen pribadinya, baik dokumen pribadi yang berupa foto, musik, atau yang lainnya. Data-data tersebut akan terselamatkan apabila sewaktu-waktu terjadi pencurian data atau ada kesalahan pada sistem komputer.
6) Selalu *Up to Date* dan mencari informasi. Pelaku *cybercrime* selalu melihat adanya celah-celah pada sistem komputer calon korbanya saat melakukan kejahatanya. Oleh karena itu, harus rutin melakukan *update* aplikasi mulai dari aplikasi *antivirus* dan aplikasi-aplikasi penunjang lainnya. Selain itu pengguna internet dapat memantau perkembangan informasi pada salah satu penyedia jasa layanan keamanan internet, seperti *National Cyber Alert System* dan sebagainya. Pencarian informasi dimaksudkan untuk mengetahui informasi jenis *cybercrime* yang sedang marak terjadi dan bagaimana menanggulanginya.

Terkait media sosial facebook, terdapat banyak informasi *hoax* yang tekadang sulit untuk dibedakan dengan informasi yang sebenarnya. Terdapat beberapa informasi di facebook dapat dindikasikan sebagai informasi *hoax* antara lain:

1) Informasi *hoax* selalu tidak mencantumkan sumber informasi dengan jelas (bukan dari instansi resmi), namun terkadang hanya mencatumkan nama tokoh tertentu. Beberapa informasi *hoax* di facebook biasanya hanya mencantumkan sumber informasi "dari group sebelah" atau "dari kamar sebelah".
2) Informasi *hoax* sering kali bersifat provokatif atau cenderung menggunakan bahasa yang provokatif, sebagai contoh "ayo viralkan". Informasi *hoax* biasanya bersifat aneh atau tidak wajar, seperti tidak adanya kesesuaian antara judul dengan isi atau bertolak belakang. Informasi *hoax* biasanya hanya mencantumkan judul dengan isi yang sepotong kemudian mencantumkan *hyperlink* yang sekedar untuk di *share, like* dan *comment*.
3) Informasi *hoax* biasanya memanfaatkan isu yang sedang tren, misalnya kasus pornografi yang melibatkan tokoh terkenal/ pejabat, pelayanan instansi pemerintah yang buruk, atau masalah terorisme dan bom. Isi dari informasi yang disebarkan biasanya tidak berkualitas dan hanya sebatas menviralkan dan terkadang juga digunakan untuk promosi atau iklan.
4) Informasi *hoax* sering menggunakan gaya bahasa tidak baku atau sederhana, dan judul terkesan melebih-lebihkan.
5) Informasi *hoax* biasanya mengandung unsur penghinaan, pencemaran nama baik bahkan SARA. Seseorang yang dengan atau tanpa sengaja membagikan informasi *hoax* yang mengandung unsur-unsur tersebut dapat dipidanakan.

c. Seleksi Informasi dari Internet

Internet menyediakan berbagai sumber informasi yang bisa memenuhi kebutuhan informasi penggunanya. Sumber

informasi yang ada di internet sangat banyak dan tanpa batas. Koleksi elektronik dengan internet bisa diakses dengan fasilitas online, dan jumlahnya terus bertambah, dapat diakses dari mana saja dan kapan saja. Alasan inilah yang mendasari tentang diperlukannya seleksi informasi melalui internet. Terdapat beberapa faktor yang perlu diperhatikan dalam menyeleksi informasi dari internet, yaitu:

1) Relevansi adalah penilaian tentang sejauh mana informasi yang dikandung suatu sumber informasi sesuai dengan masalah yang akan dibahas. Penilaian ini dapat dilakukan dengan cara melihat judul, daftar isi, abstrak, dan pendahuluan atau tujuan suatu sumber, baik tercetak maupun noncetak, termasuk situs (Diao, 2010: 51).
2) Akurasi (*accuracy*) adalah menentukan keakuratan suatu informasi sering kali menjadi alasan untuk mengkritisi suatu sumber informasi. Akurasi suatu informasi selalu dikaitkan dengan orang yang menulis atau yang bertanggung jawab atas informasi tersebut, dan penjelasan keakuratan sebuah informasi dalam website bisa dilihat dalam menu *about us*, atau *profile*, atau *contact us* (Cooke, 2001: 21).
3) Otoritas reputasi. Menurut Cooke (2001, 69) faktor utama untuk menilai otoritas dari suatu sumber informasi adalah pengetahuan dan keahlian penanggung jawab pembuat informasi. Suatu sumber informasi umumnya memiliki otoritas jika ditulis oleh seorang yang ahli, atau diproduksi oleh sebuah lembaga yang dikenal berpengetahuan dan keahlian dalam bidang tertentu. Otoritas terkait erat dengan reputasi sumber informasi dan reputasi dari penanggung jawab yang memproduksi informasi tersebut. Penilaian sejauh mana otoritas dan reputasi suatu informasi dapat dilakukan dengan pertanyaan berikut:
   a) Siapa atau instansi apa yang mempublikasi informasi?
   b) Periksa domain situs dari institusi yang mempublikasi informasi tersebut. Apakah doamin tersebut termasuk domain yang dapat dipercaya (*.edu, ac.*[kode negara], *.sch*[kode negara], *.gov* atau *.go*[kode negara]. Atau domain lain seperti *.com, .co*[kode negara], *.org*, *.or*[kode negara], *.net,* dan lain sebagainya.
   c) Apakah ada informasi mengenai kualifikasi penulis ataupun lembaga yang mengeluarkan informasi?
   d) Apakah jelas siapa yang mensponsori dan memlihara konten situs tersebut?
   e) Apakah ada informasi yang bernilai mendeskripsikan tujuan suatu lembaga ataupun lembaga yang mensponsori?
   f) Apakah ada cara untuk memverifikasi legitimasi halaman lembaga. Seperti terdapat nomor telepon atau alamat yang tersedia untuk menghubungi dan menanyakan informasi lebih lanjut?
4) Objektivitas (*objectivity*) adalah situs yang terpercaya di dalamnya menjelaskan tujuan dari situs tersebut. Misalnya, situs tersebut untuk siapa, digunakan untuk membahas apa, dan dibuat untuk apa. Informasi tersebut dapat di lihat pada menu yang terdapat pada situs, sepeti *about us* (Diao, 2010: 51-52). Untuk mengidentifikasi tujuan dari sebuah sumber, dapat dilakukan dengan menggunakan pertanyaan berikut:
   a) Apakah ada pernyataan yang menunjukkan tujuan dari situs tersebut?

b) Siapakah pembaca yang dituju oleh informai tersebut?
c) Adakah tujuan dalam situs tersebut bersifat mempengaruhi, menjual, mendasarkan pada pandangan pribadi tanpa data pendukung atau bias terhadap suatu hal?

5) Kekinian (*currency*). Berhubungan erat dengan ke-*update*-an informasi, dan juga menunjukkan bahwa informasi tersebut senantiasa diperbarui. Pertimbangan dan penilaian untuk melihat sejauh mana suatu informasi dikatakan update (Chooke, 2001: 75):
   a) Apakah tercantum tanggal pada halaman web yang mengindikasikan kapan halaman situs tersebut di tulis dan kapan halaman situs tersebut direvisi atau diedit?.
   b) Apakah ada indikasi lain bahwa materi informasi yang disajikan diperbarui secara berkala untuk memastikan seberapa baru informasi tersebut?
6) Cakupan (*coverage*). Terkait dengan isi informasi atau dokumen dalam situs, seperti hal apa yang dibahas, seberapa dalam/*detail* informasi yang disajikan, dan adakah *link* yang terhubung ke situs-situs lain yang dapat dipercaya dengan pembahasan informasi yang sama (Proboyekti, 2014).
7) Bukti yang kuat yaitu membandingkan informasi yang diperoleh dengan informasi lainnya yang berasal dari situs lain yang terpercaya, apakah ada kesamaan ataukah perbedaan (Proboyekti, 2014).
8) Bahasa dan gaya penulisan. Penulis yang tidak memiliki kredibiltas kurang memperhatikan aspek bahasa dan gaya penulisanya. Meskipun situs yang memiliki bahasa dan gaya penulisan yang bagus bukan merupakan indikator situs yang akurat, namun kecerobohan mungkin akan menjadikan situs tersebut kurang dapat diandalkan (Doyle, 2006: 56-57).

Selain memperhatikan faktor-faktor seleksi informasi sebagaimana yang telah disebutkan, setiap pengguna media sosial khususnya facebook juga harus mematuhi etika dalam penyampaian informasi untuk mencegah terjadinya *cybercrime* dan penyebaran informasi *hoax*. *Cybercrime* dan *hoax* sebenarnya dapat diminimalisir apabila setiap pengguna internet menyadari batasan-batasan dan selalu memperhatikan etika berkomunikasi di dunia maya dengan *netiquette*, yaitu panduan untuk bersikap dan berperilaku sesuai dengan kaidah normatif di lingkungan internet. Inti aturan *netiquette* adalah menyadari bahwa kita semua manusia, bahkan saat berada di internet sekalipun, mengikuti aturan seperti di kehidupan nyata saat online, selalu ingat dimana berada ketika sedang online, dan menghormati orang lain ketika sedang online (Nur Hadi, 2006).

5. KESIMPULAN

Pengguna internet yang semakin banyak menyebabkan berbagai tindak kejahatan *cybercrime* dibanyak negara termasuk Indonesia. Secara garis besar pelaku kejahatan *cybercrime* baik disengaja maupun tidak disegaja akan dijerat dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Setidaknya ada tiga ancaman yang dibawa UU ITE di Indonesia yang berpotensi menimpa pelaku *cybercrime* dengan memanfaatkan facebook yaitu ancaman pelanggaran kesusilaan Pasal 27 ayat (1), penghinaan dan/atau pencemaran nama baik Pasal 27 ayat (3), dan penyebaran kebencian berdasarkan suku, agama, ras dan antargolongan (SARA) Pasal 28 ayat (2). Ancaman pidana bagi pelanggar pasal

tersebut sesuai yang dijelaskan pada Pasal 45 ayat (1), Pasal 45 ayat (3) dan Pasal 45A ayat (2) UU ITE yaitu penjara paling lama enam tahun dan/atau denda paling banyak satu miliar rupiah. Setiap pengguna internet dan media sosial khususnya facebook harus melakukan upaya yang dapat dilakukan untuk mencegah *cybercrime* diantaranya dilakukan dengan cara melindungi komputer dari virus, menjaga privasi, mengamankan e-mail, melindungi *Id/Account*, membuat *backup* data, dan selalu *up to date* terhadap informasi. mempertimbangkan etika berkomunikasi yang baik dan seleksi informasi. Terdapat beberapa faktor yang harus diperhatikan dalam menyeleksi sumber informasi dari internet, yaitu relevansi, akurasi, otoritas reputasi, objektivitas, kekinian (*currency*), cakupan, bukti yang kuat, serta bahasa dan gaya penulisan.

DAFTAR PUSTAKA

APJII (Asosiasi Penyelenggara Jasa Internet Indonesia). (2017). *Infografis Penetrasi & Perilaku Pengguna Internet Indonesia 2017*. Diakses 26 April 2018 dari: https://apjii.or.id/survei2017.

Baskoro, D. G. (2010). "*Effective Internet Research", Seminar Workshop Literasi Informasi untuk Trainer*. Diakses 20 Desember 2017 dari: http://eprints.rclis.org/25690/.

Basuki, S. (2010). *Materi Pokok Pengantar Ilmu Perpustakaan*. Jakarta: Universitas Terbuka.

Case, D. O. (2007). *Looking for Information: A Survey of Research on Information Seeking, Needs, and Behaviour*. London: Academic Press.

Cooke, A. (2001). *A Guide to Finding Quality Information on The Internet: Selection and Evaluation Strategies*. London: Facet Publishing.

Doyle, T and John L. H. (2006). *Net Cred: Evaluating The Internet as a Research Source. Reference Service Review, Academic Research Library*, 34 (1). 56-70.

Diao, L. A, *dkk*. (2010). *Literasi Informasi 7 Langkah Knowledge Management*. Jakarta: Penerbit Universitas Atma Jaya.

Firmansyah, R. (2017). Web Klarifikasi Berita Untuk Meminimalisir Penyebaran Berita *Hoax*. *JURNAL INFORMATIKA*, 4 (2). 230-235.

Ghosh. S. dan Turrini. E. (Ed). (2010). *Cybercrimes: A Multidisciplinary Analysis*. New York: Springer.

Goyal, S. (2012). Facebook, Twitter, Google+: Social Networking. *International Journal of Social Networking and Virtual Communities (Int J SocNet & Vircom),*1 (1). 16-18.

Hartina, S., Djatin, J dan Tupan, (2012), *Penelusuran Literatur*. Tangerang Selatan: Universitas Terbuka.

Hazliansyah. (2012) *Tuding Dihina di Facebook, Rektor Polisikan Dosen*. Diakses 21 Desember 2017 dari: http://www.republika.co.id/berita/nasional/umum/12/05/10/m3srs3-tuding-dihina-di-facebook-rektor-polisikan-dosen.

Jayanti, L, *dkk*. (2016). Analisa Pola Penyalahgunaan Facebook Sebagai Alat Kejahatan Trafficking Menggunakan Data Mining. *E-journal Teknik Informatika*, 8 (1). 30-35.

Kamus Besar Bahasa Indonesia (KBBI) versi online. Diakses 21 Desember 2017 dari: http://kbbi.web.id/.

Mangadil, D. M. (2016). Dampak Yuridis Penggunaan Media Sosial Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektonik". *Lex et Societatis*, 4 (1). 120-128.

Mansur, D. M. Arief dan Ghultom, E. (2005). *Cyber law-Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama.

Nur Hadi, W. (2006). *Etika Berkomunikasi di Dunia Maya dengan Netiquette*. Diakses 21 Desember 2017 dari: eprints.uny.ac.id/7229/.

Puslitbang Hukum dan Peradilan Mahkamah Agung RI. (2004). *Naskah Akademis Kejahatan Internet (Cybercrimes)*. Jakarta: Mahkamah Agung.

Poonia A. S. (2014). Cyber Crime: Challenges and its Classification. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, 3 (6). 119-121.

Proboyekti, U. (2014). *Pengujian Hasil Pencarian di Internet*. Diakses 22 Desember 2017 dari http://lecturer.ukdw.ac.id/othie/index.php?itemid=43.

Tempo.co. (2014). *Sebar 10 Ribu Pornografi Anak, Manajer Ditangkap*. Diakses 21 Desember 2017 dari: https://nasional.tempo.co/read/571209/sebar-10-ribu-pornografi-anak-manajer-ditangkap.

Triartanto A. Y. (2015). Kredibilitas Teks *Hoax* Di Media Siber. *Jurnal Komunikasi*, VI (2). 33-36.

Tribrata News. (2018). *Breaking News, Polda Sumut Tangkap Oknum PNS Dosen USU Karena Sebut Bom Surabaya Sebagai Pengalihan Isu*. Diakses 21 Mei 2018 dari: http://tribratanews.sumut.polri.go.id/2018/05/19/breaking-news-polda-sumut-tangkap-oknum-pns-dosen-usu-karena-sebut-bom-surabaya-sebagai-pengalihan-isu/.

Windara, I M. A dan Sukranatha AA. K. (2013). Kendala dalam Penanggulangan *Cybercrime* Sebagai Suatu Tindak Pidana Khusus. *Kertha Negara*, 01(04).

Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Wahid, A dan Labib, M. (2005). *Kejahatan Mayantara (Cyber Crime*). Jakarta: PT. Refika Aditama.

Widodo. (2013). *Memerangi Cybercrime (Karakteristik, Motivasi, dan Strategi Penanganannya dalam Prespektif Kriminologi)*. Yogyakarta: Aswaja Pressindo.

We Are Social. (2018). *Social Media Use Jumps in Q1 Despite Privacy Fears*. Diakses 26 April 2018 dari https://wearesocial.com/blog/2018/04/social-media-use-jumps-in-q1-despite-privacy-fears.

Yusup, M. P dan Subekti, P. (2010). *Teori & Praktik Penelusuran Informasi*. Jakarta: Kencana Prenada Media Group.