KAMBOTI
Jurnal Ilmu Sosial dan Humaniora

Pelanggaran Hukum dalam Tindakan Vandalisme di Ruang *Cyberspace*

Fajar Rachmad Dwi Miarsa[1*], Ahmad Heru Romadhon[2*]

[1]Universitas Maarif Hasyim Latif; fajar_rahmad@dosen.umaha.ac.id
[2]Universitas Bhayangkara; ahmad-heru-romadhon@fh.umaha.ac.id
*Correspondence: ahmad-heru-romadhon@fh.umaha.ac.id

Abstract:
This research has a specific objective in providing descriptions and information about criminal offenses in cyberspace, today, various kinds of goals and motives carried out by a group of irresponsible individuals or people who then deliberately make a fuss with their special expertise, as a result. The existence of these crimes has implications for a global threat to the whole world, especially to individuals, legal entities, and government agencies. This research uses the normative juridical method, namely research that focuses on literature studies such as books, scientific papers / journals, legislation and other legal materials that support this research which is then implicated in case studies that occur in cyberspace. So far, the impact or implication of criminal violations in cyberspace is not only misleading for readers of electronic information, but also threatens national sovereignty and the slow pace of economic growth. Crime in cyberspace that does not recognize space and time, if a legal umbrella is not immediately prepared in upholding the law and achieving justice for society, it has the potential to increase the level of crime violations that have started to enter the era of the Industrial Revolution 4.0 and will transform in the 5.0 era. prioritizing the digital side as a technology communication tool that is increasingly dangerous for the young generation to come, if not immediately anticipated by the regulation of a more adequate and more dynamic legal system. Even though currently Indonesia already has ITE Law no. 11/2008 and some have been updated by the issuance of Law no. 16/2016 but it is still not enough to deal with global flows across countries.
Keywords: *cyberspace; industrial revolution 4.0; legal system; dynamic.*

Abstrak:.
Penelitian ini mempunyai tujuan khusus dalam memberikan gambaran dan informasi mengenai pelanggaran kejahatan di dalam dunia maya, dewasa ini, berbagai macam tujuan dan motif yang dilakukan oleh sekelompok oknum atau orang tidak bertanggung jawab yang kemudian dengan sengaja membuat keributan dengan keahlian khusus yang dimilikinya, sebagai dampak adanya dari pelanggaran kejahatan tersebut berimplikasi pada sebuah ancaman secara global ke seluruh dunia, khususnya kepada orang perorangan, badan hukum, dan instansi pemerintah. Penelitian ini menggunakan metode yuridis normatif, yaitu, penelitian yang menitik beratkan pada studi literatur seperti, buku, karya ilmiah/jurnal, perundang-undangan dan bahan hukum lainya yang mendukung dalam peneltian ini kemudian diimplikasikan dalam studi kasus yang terjadi didalam dunia maya. Sejauh ini dampak atau implikasi adanya pelanggaran kejahatan didalam dunia maya tidak hanya menyesatkan bagi pembaca informasi elektronik, tetapi juga mengancam kedaulatan nasional dan lambatnya pertumbuhan ekonomi. Kejahatan didalam dunia maya yang tidak mengenal ruang dan waktu, apabila tidak segera disiapkan payung hukum dalam menegakan hukum dan tercapinya keadilan bagi masyarakat, hal itu berpotensi semakin meningkatnya tingkat pelanggaran kejahatan yang sudah mulai masuk pada era Revolusi Industri 4.0 dan akan bertransformasi di era 5.0 yang mengedepankan sisi digital sebagai alat komunikasi teknologi yang semakin berbahaya bagi generasi muda yang akan datang, jika tidak segera diantisipasi oleh regulasi sebuah sistem hukum yang lebih memadahi dan lebih dinamis. Meskipun saat ini Indonesia sudah memiliki UU ITE No. 11/2008 dan sebagian telah diperbaruhi dengan keluarnya UU No. 16/2016 tetapi hal itu masih belum cukup dalam menghadapi arus global lintas negara.
Kata Kunci: *Cycerspace; Revolusi Industri; Legal Sistem; Dinamis.*

1. Pendahuluan

Teknologi digital yang berbasis pada budaya sosial masyarakat modern saat ini cenderung lebih mengutamakan alat teknologi sebagai alat komunikasi yang paling ideal, super cepat sesuai dengan perubahan zaman. Tetapi disisi lain, kebiasaan itu justru menyebabkan adanya perubahan konvergensi tatanan hukum atau sistem hukum yang mengupdate tuntutan itu guna untuk menyesuaikan perkembangan globalisasi secara dinamis. Sebagaimana eksistensi teori hukum konvergensi merupakan pemahaman tentang variabel konseptual teknologi, ekonomi, dan budaya hukum menjadi satu kesatuan yang saling berkaitan dan hubungan yang paling intim bagi manusia dan masyarakat dalam menghadapi transformasi Revolusi Industri 4.0, baik dalam lingkup nasional, regional maupun internasional. Peran teknologi dan beberapa implikasi teknologi informasi terhadap komunikasi tidak hanya memberikan perubahan yang signifikan dalam penggunaannya, tetapi juga memfasilitasi adanya eksplorasi pelanggaran kejahatan yang mengancam keselamatan setiap orang, terutama dalam melindungi data penting baik secara individu, badan hukum, ataupun instansi pemerintah.

Penelitian yang dilakukan di AS, "*America Online dan National Cyber Security Alliance*" yang menyatakan bahwa, pengguna internet di rumah tidak senyaman yang mereka yakini selama ini. Adanya peryataan itu tentu memiliki akibat hukum yang harus diperhatikan dengan serius. Dengan meningkatnya penetrasi penggunaan internet saat ini, tentu kita juga perlu memahami adanya kepentingan relatif dari berbagai factor, sosio-demografis yang mempengaruhi kerentanan setiap individu terhadap terjadinya pelanggaran kejahatan berbasis internet. Tren masa kini menunjukkan bahwa, kejahatan tradisional seperti pelecehan, penipuan, dan pencurian identitas dan lain sebagainya, kini dilakukan dengan menggunakan kecanggihan alat pendukung berbasis internet (Tejaswini Herath, 2012) Berbagai macam cara kejahatan memfokuskan pada pengguna internet yang lemah dalam pengamanan dalam akun konten yang dimiliki, sehingga hal itu menjadikan pengguna internet sebagai sasaran kejahatan di ruang publik. Sedangkan sejauh ini definisi tentang tindak kejahatan di dunia maya yang tunggal masih belum ada kecocokan dan kesepakat yang sama dalam mendefinisikan pandangan tersebut.

Dalam hal pandangan tentang definisi tersebut, sejauh ini telah banyak sejumlah pakar dan pakar industri ditawarkan oleh beberapa definisi yang telah dirumuskan di pemerintah federal. Banyaknya macam-macam definisi tampaknya memiliki variasi dalam tingkatannya yang lebih khusus dan umum. Misalnya, salah satu perusahaan keamanan komputer terbesar, *Symantec Corporation*, mendefinisikan pelanggaran kejahatan dunia maya sebagai "kejahatan apa pun itu yang telah dilakukan menggunakan bantuan komputer atau jaringan, atau perangkat keras. Terlepas dari definisi tersebut, konseptualisasi kejahatan dunia maya juga melibatkan sejumlah elemen dan pertanyaan kunci, termasuk di mana kejahatan itu dilakukan di dalam dunia nyata maupun dunia digital, dan teknologi apa yang dipakai atau dilibatkan. Sejumlah pertanyaan lain juga juga ikut mewarnai, mengapa aktivitas kejahatan dimulai, dan siapa yang terlibat di dalam melakukan tindakan jahat itu (Finklea, 2012) Nampaknya perkembangan teknologi digital dan informasi elektronik tidak hanya memberikan kontribusi positif dan spesifik bagi peningkatan kesejahteraan masyarakat tetapi juga sekaligus menjadi sarana percepatan informasi global dalam membangun jaringan dan peradaban, namun disisi lain selain menjadi sarana media yang efektif dalam meningkatkan kesejahteraan masyarakat justru banyak aktivitas yang dilakukan dalam hal perbuatan melawan hukum. Universalitas, *Universal Interest Jurisdiction* memberikan pandangan bahwa, setiap negara memiliki hak untuk menangkap dan menghukum pembajakan, yang dapat diperluas menjadi kejahatan terhadap kemanusiaan, genosida, pembajakan pesawat, semua itu dapat diperluas menjadi: privasi internet, *hacking*, *cracking*, virus yang sengaja dikirim untuk merusak sistem, semua itu termasuk dalam pelanggaran kejahatan sangat berat yang berkembang menjadi yurisdiksi ekstra teritorial (Partodiharjo, 2008)

Perlunya pendekatan hukum yang berbasis teknologi untuk dapat mengantisipasi pelangaran kejahatan terhadap perubahan sosio-teknologi. Maka berbagai kebijakan yang mengatur keamanan siber khusus di Indonesia telah dirintis sejak tahun 2007 yang dikeluarkan oleh Menteri Komunikasi dan Informatika Nomor 26 / PER / M.Kominfo / 5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Internet Protocol yang kemudian direvisi dengan keluarnya Peraturan Menteri Komunikasi dan Informatika No.16 / PER / M.KOMINFO / 10/2010 dan kemudian diperbarui dengan Peraturan Menteri Komunikasi dan Informatika No.29 / PER / M.KOMINFO / 12/2010 (Ardiyanti, 2014) semua upaya itu dilakukan guna dalam menjamin adanya perlindungan hukum kepada pengguna teknomogi digital. Kemudian pendapat lain juga menyatakan bahwa, hukum dan teknologi menunjukkan tanda-tanda menuju masa depan, ketika dampak teknologi tertentu berada di bawah "mikroskop" hukum. Apabila menurut **Heidegger** bahwa, teknologi itu bukan hanya sejumlah mesin tetapi sebagai upaya mendasar untuk menyatakan dunia sebagaimana adanya (Budhijanto, 2018)

Perubahan perilaku yang mengatasnamakan orang lain atau dengan membuat akun palsu yang seolah-olah itu asli milik orang tersebut atau dengan sengaja mengubah teks konten media orang lain yang dapat merugikan korban vandalisme konten, mengubah pada tampilan *website* tanpa seizin atau sepengetahuan pemilik akun, tentunya tindakan tersebut melanggar ketentuan hukum yang berlaku. Seperti yang terjadi pada artikel Arteria Dahlan (Rahmayunita, 2019) adanya perubahan biodata yang sengaja diubah *hacker* dalam wikipedia, masih banyak jenis vandalisme konten yang telah diacak-acak dengan konten yang dikenal sebagai *cyber vandalism*, contoh, lain seperti akun Twitter palsu dengan narasi tertulis @htmnparis akan membawa *boyband* terkenal Korea, BTS dan EXO, setelah Corona Pandemi, di narasi yang berisikan memberikan sejumlah hadiah yang akan dibagikan. Kedua contoh ini tidak hanya merusak citra orang yang bersangkutan, tetapi juga menyesatkan orang lain yang membacanya.

Menurut buku *Ethics and Technology*: *Controversies, Questions, and Strategy for Ethical Computing, pelaku cyber vandalism* juga dapat melakukan kerusakan pada file elektronik dengan membuat *malware* atau menghapus *disk drive* untuk menonaktifkan sistem komputer (KumparanNews, 2019) Tentunya hal tersebut sangat merugikan pihak lain. Maka urgensi dalam hal ini mestinya harus ada intervensi hukum sebagaimana yang dikemukakan oleh **Boele Woelki** yang berpandangan bahwa, keterlibatan langsung pemerintah dan hukum sebagai solusinya dalam menangani adanya pelanggaran kejahatan pada dunia maya merupakan hal yang sangat dibutuhkan, terutama dalam menyelesaikan sengketa yang timbul di bidang telematika (Maskun, 2014) Jika kita menyadari bahwa kecanggihan teknologi tidak terlepas dari peran manusia, maka kita dapat menurunkannya sebagai prinsip yang diterapkan pada manusia di belakang mesin, artinya mesin yang menjalankan program dan itu diperbolehkan, tetapi jika mesin itu dibuat, dan diprogram untuk melakukan kejahatan yang dikendalikan oleh manusia dengan mental motif kejahatan. Maka prinsip ini menyatakan bahwa, tanggung jawab tetap pada orang yang mengendalikannya. Adapun keterlibatan alat yang digunakan adalah, alat media yang akan menjadi subjek hukum saat terjadi pelanggaran kejahatan tersebut.

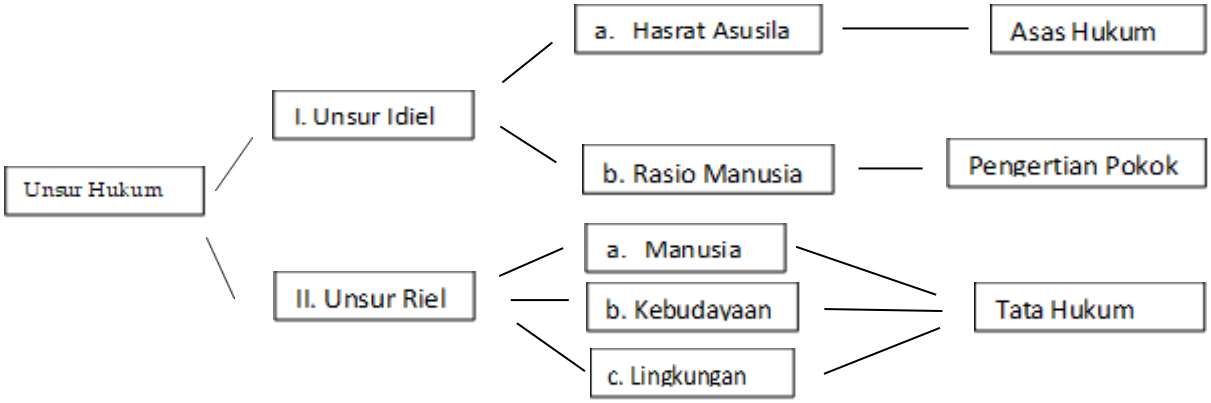
2. Tujuan Penelitian

Penelitian ini tidak lain memiliki tujuan edukasi yang bersifat ilmiah, adapun tujuan khusus dari penelitian ini merupakan sebagai bentuk tanggung jawab moral sebagai intelektual yang memiliki kewajiban turut mencerdaskan anak bangsa, sedangkan tujuan umum diharapkan penelitian ini bermanfaat bagi pembaca yaitu, masyarakat, akademisi, praktisi dan instansi pemerintah.

3. Metode

Penelitian ini merupakan penelitian yuridis normatif dengan menggunakan bahan pustaka, hukum, buku, jurnal, media online / internet. Penelitian hukum normatif meliputi asas-asas hukum, sistematika hukum, derajat sinkronisasi vertikal dan horizontal, hukum komparatif, serta sejarah hukum (Soerjono Soekanto, 2015) Untuk lebih memahami hubungan antara ilmu hukum dan hukum

positif, diperlukan kajian tentang unsur hukum atau *'gegeven van het recht*'. Unsur hukum meliputi unsur idiil dan unsur nyata. Dengan demikian, sistem secara visual adalah sebagai berikut:



4. Hasil Penelitian

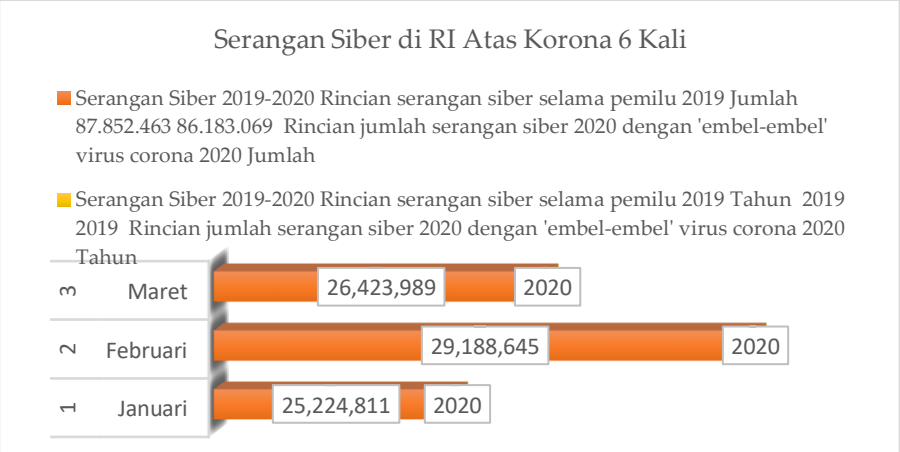
4.1 Vandalisme Konten Media

Berbagai model kejahatan yang kerap terjadi seiring dengan perkembangan teknologi yang semakin maju menuntut kesadaran kritis terhadap masyarakat untuk menjaga perilaku di ruang media social, baik berupa menulis teks pada kolom media sosial ataupun saat memberikan komentar terhadap orang lain, karena dalam hal ini merupakan suatu keharusan. Mengapa setiap orang dituntut untuk kritis. Setidaknya ada tiga alasan yang menjadi dasar adanya sikap ini. *Pertama*, rentan hilangnya hak masyarakat atas suatu informasi yang benar. *Kedua*, adanya kelompok kepentingan (ekonomi dan politik) yang menjadikan sosial media yang mendominasi sebuah gagasan. Dominasi teks yang selama ini secara tidak langsung menjadikan masyarakat sebagai objek manipulasi gagasan dari otoritas media. *Ketiga*, adanya popularitas konten media yang mengarah pada keseragaman selera di masyarakat. Keragaman ini menjadi suatu penghalang dari adanya erosi beragam tindakan komunikatif di masyarakat (Abdul Wahid, 2017) Termasuk juga dalam tindakan vandalisme konten di media sosial, tindakan itu mengarah dan melibatkan pada penghancuran atau perusakan yang disengaja untuk dilakukan terhadap properti publik atau pribadi. Pengertian lain dari vandalisme yang memungkinkan adanya suatu perbedaan perilaku bermusuhan yang ditujukan untuk merusak atau menghancurkan suatu objek, perilaku instrumental yang terdiri dari kerusakan atau kehancuran yang disebabkan oleh suatu objek sebagai sarana untuk mencapai tujuan lain (perampasan harta benda orang lain, sabotase), dan perilaku yang dimotivasi dalam bentuk menyesatkan oleh keinginan orang yang tidak bertanggung jawab untuk dapat mengekspresikan diri melalui degradasi objek dan vandalisme bermain. Vandalisme sendiri terkadang dianggap sebagai salah satu kejahatan umum yang tidak terlalu dianggap serius, tetapi hal itu bisa menjadi sangat serius dan merepotkan jika dilakukan secara masif dan meluas, dengan bentuk kekerasan, atau sebagai ekspresi kebencian dan intimidasi dalam ruang *cyberspace*.

Berikut contoh kasus yang sering terjadi baik di Indonesia maupun di negara lain:

1) Akun palsu, Facebook, Instagram, Twitter
   Media sosial jenis ini banyak digunakan oleh masyarakat dan tokoh masyarakat yang memiliki banyak pertemanan dan follower. Salah satu pelanggaran kejahatan yang diikuti dengan vandalisme konten adalah pengkloningan media sosial orang lain. Modus seperti ini biasanya dilakukan oleh mereka dengan meminta sejumlah tebusan uang kepada pemilik akun dan meminta transfer melalui rekening yang sudah disiapkan.
2) Serangan dunia maya di Indonesia

Selama pandemi global Covid-19, National *Siber and Coding Agency* (BSSN) mencatat sedikitnya berjumlah 80.837.445 kasus serangan siber pada periode Januari-Maret 2020. Jika dibandingkan dengan kasus pada tahun 2019 saat pemilu, tentu lebih banyak kasus yang terjadi disaat pandemi global Covid-19. BSSN selama ini juga mencatat setidaknya terdapat kasus sebanyak 159 serang terhadap situs *website* yang sengaja ditujukan untuk merusak situs pemerintah. BSSN menunjukkan sejumlah data konkret bahwa, telah terjadi serangan jahat pada layanan konferensi video Zoom yang menggunakan pengkodean yang berisi modul *metasploit*, *adware*, dan *hiddenad/hiddad* (Indonesia, 2020)



Gambar: 1, Sumber: data yang telah diolah dari situs CNNIndonesia

4.2. Kategori Kejahatan Dunia Maya

Sebagaimana telah kita ketahui, bahwa kejahatan yang terjadi di ruang media sosial dengan melibatkan bantuan seperangkat alat canggih untuk dapat melakukan tindakan pelanggaran kejahatan secara konvensional tentang kejahatan siber telah menetapkan 4 (empat) kategori bentuk yang dapat dikatakan sebagai kejahatan siber, yaitu:

1) Pelanggaran kerahasiaan, integritas dan ketersediaan data pada sistem komputer.
2) Pelanggaran dengan merusak sistem komputer.
3) Pelanggaran yang terkait dengan muatan konten.
4) Pelanggaran yang berkaitan dengan pekerjaan dan hak terkait lainnya.

Sebagaimana pembahasan *cybercrime* dalam kongres PBB yang bertajuk membahas tentang pencegahan kejahatan dan perlakuan terhadap pelanggar di Havana, Cuba pada tahun 1990 dan di Wina, Austria pada tahun 2000, memberikan dua catatan istilah penting yang harus diketahui:

1) *Cybercrime* yang dalam artiannya merupakan kejahatan komputer adalah tindakan ilegal dengan menyerang sistem pada keamanan komputer atau data yang terdapat di dalam komputer dan diakses tanpa izin dari pemiliknya.
2) Kejahatan dunia maya, dalam arti luas, disebut kejahatan terkait komputer, yang menunjukkan perilaku ilegal atau melanggar yang terkait dengan sistem atau jaringan komputer (Ketaren, 2016)

Kategorisasi diatas yang menunjukkan bahwa kejahatan siber, jika ditelisik lebih dalam masih banyak model-model kejahatan siber yang juga terbagi menjadi dua yaitu: adanya berpotensi kekerasan, dan non-kekerasan (Fauzan, Riadi, & Fadlil, 2016) masing-masing memiliki kategorisasi tersendiri yaitu:

- Kekerasan/berpotensi kekerasan:
  1) *Cyberterrorism*, yaitu suatu model kejahatan yang lebih mengarah pada kejahatan teroris dengan menggunakan basis dunia maya.
  2) *Cyber bullying*, yaitu suatu model serangan yang acap kali memperlakukan korbannya dengan cara menakut-nakuti/intimidasi bahkan juga mempermalukannya

di depan umum dengan kata lain yaitu menyerang suatu kehormatannya yang merendahkan harkat martabat orang lain.

3) Ponografi anak, yaitu suatu rangkain kegiatan yang melibatkan beberapa kelompok orang dengan tugas yang berbeda-beda yaitu: tugas membuat konten kreatif, tugas untuk pendistribusian dan tugas untuk mengakses konten materi.

- Tanpa kekerasan:
  1) *Cybertrespass*, munculnya dari pemahaman tentang internet di mana properti berwujud itu adalah sebagai dasar prinsip pengorganisasian utama (Collins, 2006) yang sering menjadi sasaran peretas dan kemudian diaksesnya secara ilegal.
  2) *Cyber Threat,* yaitu merupakan bagian dari kelompok kejahatan peretas untuk mencuri data perusahaan, membajak sistem dan jaringan pihak ketiga. Perhatian departemen Kehakiman telah lama berargumen bahwa jika sebuah perusahaan mengakses jaringan komputer pihak lain tanpa izin, untuk tujuan apa pun, itu melanggar hukum (Matthews, 2013)
  3) *Plagiarisme*, yaitu pengakuan secara sepihak atas karya orang lain dengan mengakuinya bahwa itu adalah kepunyaannya atau hak ciptaannya sendiri.
  4) Pembajakan, yaitu penyalahgunaan perangkat lunak dalam penelitian ini berarti merusak atau menyalin perangkat lunak milik orang lain, dan menggunakan perangkat lunak yang disalin, atau mendistribusikan perangkat lunak yang disalin tanpa izin (Timothy Paul Cronan, C. Bryan Foltz, 2006)
  5) *Cyber Fraud*, yang sering dikaitkan dengan kejadian penipuan dalam ruang cyber atau Internet, *Center for Internet Fraud*. Departemen Kehakiman AS mendefinisikan penipuan dalam ruang internet sebagai jenis dari semua jenis skema penipuan yang menggunakan satu atau lebih komponen internet, seperti ruang obrolan, email, papan pesan, atau situs web untuk mengirimkan aplikasi kepada calon korban yang akan ditipu dengan melakukan transaksi penipuan, atau mengirimkan hasil penipuan ke lembaga keuangan atau orang lain yang terkait dengan skema itu (Ebenezer, 2014)
  6) Kejahatan merusak, yaitu kejahatan merusak yang bekerja secara alami atau simulasi yang sengaja dibuat (Kapoor, 2016)
  7) Kejahatan lainnya, yang meliputi beberapa poin yaitu: 1) *Recreational Hacker*, 2) *Cracker* (*Criminal Minded Hacker*), 3) *Political Hacker*, 4) *Denial of Service a Attack* (DoS), 5) Virus, 6) Perjudian, 7) *Cyber* Menguntit (Partodiharjo, 2008)

4.3. Pengaturan Hukum Dalam Dunia Maya

Istilah dunia maya yang dipopulerkan oleh **William Gibson** dalam karyanya yang berjudul *Neuromancer* (p. 128) mengartikan bahwa dunia maya sebagai berikut:

> "*Halusinasi konsensual dialami setiap hari oleh milyaran operator yang sah, di setiap negara, anak-anak diajari konsep matematika. Representasi grafis dari data yang diabstraksi dari bank setiap komputer dalam sistem manusia. Kompleksitas yang tak terbayangkan. Garis-garis cahaya berputar di sekitar ruang pikiran, kelompok dan konstelasi data*".

Oleh karena itu, definisi **William Gibson** yang dikomentari oleh **Dr. Edmon Makarim, S.Kom., S.H., LL.M**. dalam Disertasinya sebagai calon Doktor, dengan pembahasan "Penyelenggara Tanggung Jawab *Good Governance* Dalam Penyelenggaraan Sistem Elektronik (*Good Electronic Governance*)". Pada intinya adalah sebuah halusinasi virtual yang menekankan pada ruang baru yang mempertemukan hasil perkabelan kabel listrik dengan perangkat komputer, yang dalam hal ini keberadaan kata '*space*' dalam istilah '*cyberspace*' secara teknis berbeda sifatnya dari kata tersebut. 'ruang' dalam 'dirgantara', karena makna ruang dalam 'dirgantara' adalah alam semesta tanpa batas yang diciptakan oleh penciptanya, sedangkan ruang dalam 'dunia maya' merupakan ruang komunikasi ciptaan manusia yang dibatasi, walaupun jumlah penggunanya juga akan terbatas atau terus meningkat dari waktu ke waktu sesuai dengan dinamika masyarakatnya (Kurnia, 2018)

Sebagaimana pengaturan hukum yang mengatur adanya tindak pidana siber melalui UU No. 11/2008 ITE sebagaimana telah diubah dengan UU No. 19/2016 tentang Perubahan Atas UU No. 11/2008 ITE, memiliki implikasi terhadap pengaturan hukum acara pidana terutama mengenai, 1) alat bukti, 2) kewenangan penyidik melakukan penggeledahan, 3) penyitaan dan kerjasama internasional, 4) peran ahli teknologi di bidang teknologi informasi dan komunikasi (Suseno, 2012) sehingga pengaturan hukum secara umum dalam hal ini KUHP jika terjadi pelanggaran di ruang media sosial, maka yang digunakan adalah *lex specialis*. Oleh karena itu, *rule of law* yang akan mengatur kegiatan di dunia maya harus didasarkan pada sintesis antara hukum positif (*the existing law*) dan *lex informatica*. Apabila menurut **Orin S. Kerr** dalam memberantas adanya tindak pidana siber disamping perlu adanya pengaturan hukum pidana materiil juga diperlukan ketentuan-ketentuan baru dalam mengatur hukum acara pidana, karena dalam tindak pidana siber menunjukkan adanya fakta baru yang akan membutuhkan hukum acara pidana yang baru pula.

Table 1. Klasifikasi menurut Convention on Cybercrime

1.	**Crimes regarding illegal activities of the ITE Law**	**UU ITE**
	a. Distribusi, transmisi, akses, konten ilegal	• Tindakan yang dilarang, Pasal 27 ayat (1) Kesusilaan. • Tindakan yang dilarang, Pasal 27 ayat (2) Perjudian. • Pencemaran nama baik / fitnah, Pasal 27 ayat (3). • Tindakan yang dilarang, Pasal 27 ayat (4) Pemerasan / ancaman. • Perbuatan yang dilarang, Pasal 28 ayat (2) Berita yang berbohong dan merugikan konsumen. • Tindakan yang dilarang, Pasal 28 ayat (2) Menumbuhkan kebencian dan intoleransi rasial.
	b. Setiap upaya / metode akses ilegal, Pasal 30 UU ITE	
	c. Penyadapan / intersepsi ilegal atas informasi atau dokumen elektronik dalam sistem elektronik, Pasal 31 UU ITE 19/2016	• Tindakan yang dilarang, Pasal 29 ayat (29) Informasi yang berisi ancaman dan intimidasi ditangani secara tertutup
2.	**Kejahatan yang terkait dengan gangguan (intervensi)**	
	a. Tindakan yang dilarang, Pasal 32 adalah gangguan terhadap informasi atau dokumen elektronik (gangguan data)	
	b. Tindakan yang dilarang, Pasal 33 adalah gangguan pada sistem elektronik (gangguan sistem)	
3.	**Tindak pidana yang ikut memfasilitasi perbuatan terlarang, Pasal 34 UU ITE**	
4.	**Kejahatan yang memanipulasi informasi dokumen elektronik, Pasal 35 UU ITE**	
5.	**Tindak pidana tambahan (akses) Pasal 36 UU ITE, dan**	
6.	**Hambatan terhadap ancaman pidana, Pasal 52 UU ITE**	

Seperti halnya pengaturan kejahatan siber formal di Indonesia, selain mengatur kejahatan siber yang bersifat material, peraturan tersebut juga mengatur tentang tindak pidana siber formal,

khususnya di bidang penyidikan oleh aparat penegak hukum yang bertugas membujuk barang bukti, penjelasannya diuraikan dalam Pasal 42 UU ITE bahwa penyidikan tindak pidana berdasarkan ketentuan UU Acara Pidana Nomor 8 Tahun 1981.

4.4. Pendekatan Statistik Mempelajari Kejahatan

Mempelajari kejahatan dengan pendekatan statistik tentunya tidak terlepas dari Adolpe Quetelet, seorang ahli di bidang statistika Belgia dan Profesor Astronomi di Brussel yang berhasil menjadikan statistika sebagai suatu ilmu, sekaligus menciptakan pola dasar statistika praktis (Efendi, 2017) Quetelet menggunakan data kejahatan di Perancis untuk pertama kalinya untuk membuktikan bahwa kejahatan, seperti banyak kejadian dalam interaksi sosial lainnya, bukanlah gejala dari tindakan individu, tetapi juga merupakan fenomena massal, sehingga statistik kriminal menjadi metode yang lebih efektif daripada yang lain. metode. untuk dapat mempelajari kejahatan massal, yaitu dengan menemukan perintah, kecenderungan dari hukum sosial.

Statistik kejahatan menyajikan angka dalam bentuk angka yang menunjukkan jumlah kriminalitas yang tercatat pada waktu dan tempat tertentu. Statistik kriminal ini kemudian menampilkan data kriminal yang terekam, baik yang resmi maupun yang direkam sendiri. Statistik resmi dapat diperoleh dari tiga sumber atau biro publik, yaitu:

1) Polisi, selain mencatat kejahatan, polisi umumnya juga mencatat umur, kebangsaan dan jenis kelamin para pelaku kejahatan yang menjadi bagian dari statistik kepolisian.
2) Pengadilan, statistik yang dibuat oleh pengadilan tentang hal-hal yang berkaitan dengan jumlah pelanggaran yang dituntut, jumlah hukuman dan tata cara yang digunakan dalam memberikan hukuman, jumlah yang tidak terpidana serta alasan prosedur persidangan untuk melepaskan masalah tersebut. dan siapa yang bertanggung jawab.
3) Fasilitas Pemasyarakatan, di Amerika, penjahat dewasa dipenjara di penjara negara dengan sedikit pengecualian, sedangkan untuk penjahat minor pada umumnya disediakan fasilitas di wilayah provinsi, sehingga statistik mengenai tahanan jarang sekali dalam kondisi yang dapat digunakan karena tidak memiliki ayah sama sekali secara tertulis yang dapat dipertanggungjawabkan atau perkiraan yang dapat diandalkan tentang jumlah narapidana di setiap provinsi.

Keberadaan statistik pidana dimaksudkan untuk menghomogenkan data tentang pelaku tindak pidana dan jenis tindak pidana dalam jumlah yang diterima dari instansi resmi berdasarkan pencatatannya, dikalsifikasi, ditabulasi, dan dianalisis dengan tujuan menjalin hubungan antara klasifikasi dan faktor yang ditabulasikan. kemudian dipublikasikan secara rutin.

Berikut sebagai penjelasan Teknis (Badan Pusat Statistik, 2014)

(1) Angka Indeks Kejahatan (It)

$$\text{It} = \frac{\text{Jumlah peristiwa kejahatan pada tahun t}}{Jumlah\ peristiwa\ kejahatan\ pada\ tahun\ t}\ x\ 100$$

(2) Angka Kejahatan per 100.000 Penduduk (crime pate)

$$= \frac{\text{Jumlah peristiwa kejahatan pada tahun t}}{Jumlah\ penduduk}\ x\ 100.000$$

(3) Skala Waktu Kejahatan Tahun t (crime clock)

$$= \frac{365 \text{ x } 24 \text{ x } 60 \text{ x } 60}{Jumlah\ peristiwa\ kejahatan\ tahun\ t}\ x\ (detik)$$

(4) Persentase Penyelesaian Peristiwa Kejahatan (crime clearence)

$$= \frac{\text{Jumlah peristiwa kejahatan yang diselesaikan}}{Jumlah\ peristiwa\ kejahatan\ pada\ dilaporkan}\ x\ 100\ (\%)$$

4.5. Prinsip Dasar Forensik Digital

Prinsip paling dasar harus dipahami terlebih dahulu oleh seorang ahli forensik digital sendiri. Banyak pedoman internasional juga tertarik untuk membahas hal ini lebih dalam. Aparat penegak hukum sebagai acuan dalam bertindak dituntut sesuai dengan prosedur yang telah ditetapkan dalam investigasi kejahatan komputer dan kejahatan terkait komputer, dalam hal pemeriksaan dan analisis barang bukti. Beberapa ketentuan yang menjadi rujukan para profesional forensik digital lebih diterima dan aplikatif yaitu:

1) Panduan praktik yang baik untuk alat bukti elektronik berbasis komputer, ketentuan ini dikeluarkan oleh Association of Chief Police Officers (ACPO) yang merupakan asosiasi pimpinan polisi di Inggris, yang telah bekerja sama dengan 7 Safe.
2) Pemeriksaan forensik bukti digital: panduan penegakan hukum, ketentuan ini dikeluarkan oleh National Institute of Justice di bawah kendali Departemen Kehakiman AS.
3) Penyelidikan TKP elektronik: Panduan untuk penanggap pertama, juga dikeluarkan oleh National Institution of Justice di bawah kendali Departemen Kehakiman AS.

Prinsip dasar forensik digital menurut ACPO yang dikutip dari pedoman dapat dilihat sebagai berikut:

1) tindakan yang diambil oleh aparat penegak hukum atau aparatnya yang harus mengubah data yang disimpan di komputer atau media penyimpanan yang kemudian dapat diandalkan di pengadilan.
2) Dalam keadaan dimana seseorang merasa perlu untuk mengakses data asli yang disimpan di komputer atau di media penyimpanan, orang tersebut harus kompeten untuk melakukannya dan dapat memberikan bukti yang menjelaskan relevansi dan implikasi dari tindakan mereka.
3) Jejak audit digital atau catatan lain dari semua proses yang dapat diterapkan pada bukti elektronik harus dibuat dan disimpan di tempat yang benar-benar aman. Pihak ketiga, atau pihak independen harus dapat memeriksa proses ini dan mencapai hasil yang sama untuk menyinkronkan hal-hal terkait.
4) Dalam kasus apa pun, tanggung jawab Seseorang untuk investigasi memiliki tanggung jawab keseluruhan untuk memastikan bahwa hukum dan prinsip-prinsip ini dipatuhi (Al-Azhar, 2012)

Table 2. Forensic Digital Classification

Classification	Description
Computer Forensics	• Terkait dengan pemeriksaan dan analisis bukti perangkat keras elektronik berupa komputer PC, laptop, netbook dan tablet yang kemudian pemeriksaan bukti biasanya terkait dengan file recovery
Mobile Forensics	• Mobile forensik berkaitan dengan jenis alat bukti elektronik berupa handphone atau smartphone. Pemeriksaan ini terkait dengan informasi digital yang masih tersimpan dalam barang bukti. Seperti: log panggilan, masuk, keluar, tidak terjawab, SMS, email, video.
	• Hal ini berkaitan dengan rekaman suara yang berkaitan dengan pelaku kejahatan. Rekaman ini biasanya

Audio Forensics	diperiksa untuk pengenalan suara, kemudian dianalisis suara untuk dibandingkan dengan perbandingan suara yang relevan untuk mengetahui identik atau tidak identik.
Forensic Video	• Untuk memperdalam hasil pemeriksaan dan analisis terkait video forensik berupa cuplikan video, ahli forensik kemudian melakukan analisis dengan screenshot wajah tersangka
Forensic Image	• Suatu citra / foto yang berkaitan dengan jenis barang bukti berupa file citra digital, diperiksa dan dianalisis untuk mengetahui peralatan apa yang digunakan juga termasuk untuk mengetahui waktu pengambilan dan kemudian dipastikan apakah berkas tersebut masih asli atau sudah direkayasa. .
Cyber Forensics	• Terkait dengan itu semua, kasus-kasus tersebut terkait dengan jaringan komputer internet atau LAN, kemudian melacak IP mana yang digunakan dalam melakukan tindak pidana tersebut.

Kesimpulan

Peningkatan penetrasi pengguna internet yang cukup signifikan, tentunya diikuti dengan ancaman tindak pidana yang terus mengintai, hal tersebut disebabkan oleh persaingan yang tidak sehat baik secara individu, bisnis korporasi bahkan antar negara. Keamanan siber yang selama ini diserang oleh pihak luar masih cukup untuk menangkalnya, hal ini juga disebabkan oleh kurangnya sumber daya manusia yang mendasarinya, dan juga aparat penegak hukum saat menerima laporan kejahatan di dunia maya juga kurang tanggap dalam menanganinya. Urgensi perlindungan hukum bagi pengguna media sosial internet, selain harus memiliki regulasi yang sudah ada, yakni UU ITE 11/2008 atau yang telah diubah menjadi UU ITE 9/2016 masih mensyaratkan adanya tambahan regulasi yang mengatur waktu terjadinya tindak pidana, baik disaat siang maupun malam, juga harus memperhatikan waktu efektif saat orang sibuk bekerja mengoperasikan sistem komputer. Aturan hukum tambahan akan lebih ditekankan melihat kondisi dan waktu. Hal ini diperlukan untuk mengantisipasi kerugian ekonomi, juga kelalaian setiap orang saat istirahat atau penanggung jawab pengawasannya. Selain itu, perlindungan konsumen diberlakukan kepada pemilik platform media yang banyak digunakan, guna menjamin keamanannya sendiri bagi pengguna media sosial dari ancaman atau kejahatan di dunia maya, sehingga pemilik platform juga harus bertanggung jawab dalam mengganti kerugian. timbul.

Ucapan Penghargaan

Kami ucapkan terima kasih banyak kepada rekan M. Adhi Prasnowo, S.T., M.T., IPM., ASEAN Eng, juga kepada rekan-rekan Komunitas UMAHA Publikasi dan juga kepada pihak publisher yang telah membantu dalam proses penerbitan karya ilmiah ini.

Konflik Kepentingan

Demi menjaga eksistensi disiplin ilmu dan etika dalam penulisan karya ilmiah ini maka perlu dipertegas bahwa, penelitian ini bertujuan sebagai pengetahuan terbuka dalam menambah ilmu pengetahuan dan juga perlu diketahui bahwa penelitian ini bukan hasil dari plagiat.

Referensi

Abdul Wahid, D. A. P. (2017). *Masyarakat dan Teks Media* (Pertama). Malang: UBPress.

Al-Azhar, M. N. (2012). *Digital Forensic Practical Guidelines for Computer Investigation*. 1–292.

Ardiyanti, H. (2014). Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. *Politica*, *5*(1), 95–110.

Badan Pusat Statistik. (2014). Statistik Kriminal. In *Bps.Go.Id* (p. 14). Jakarta: Badan Pusat Statistik. Retrieved from http://www.bps.go.id/linkTabelStatis/view/id/1720

Budhijanto, D. (2018). *Teori Hukum Dan Revolusi Industri 4.0* (Pertama). Bandung: Logoz Publishing.

Collins, K. E. (2006). Cybertrespass and Trespass to Documents. *Cleveland State Law Review*, *54*(41), 41–68.

Ebenezer, J. A. (2014). Cyber Fraud , Global Trade And Youth Crime Burden : Nigerian Experience. *Afro Asian Journal of Social Sciences*, *5*(4), 1–21.

Efendi, T. (2017). *Dasar-Dasar Kriminologi* (Pertama). Malang: Setara Press.

Fauzan, A., Riadi, I., & Fadlil, A. (2016). Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime. *Annual Research Seminar (ARS)*, *2*(1), 159–163. Retrieved from http://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/832/752

Finklea, K. M. (2012). Cybercrime : Conceptual Issues for Congress. *Congressional Research Service*, 1–26. Retrieved from http://fas.org/sgp/crs/misc/R42547.pdf

Indonesia, C. (2020). BSSN: Serangan Siber di RI Selama Corona Naik 6 Kali Lipat. Retrieved April 24, 2020, from CNN Indonesia website: https://www.cnnindonesia.com/teknologi/20200423160048-185-496626/bssn-serangan-siber-di-ri-selama-corona-naik-6-kali-lipat

Kapoor, J. K. D. K. (2016). Development of latent prints exposed to destructive crime scene conditions using wet powder suspensions. *Egyptian Journal of Forensic Sciences*, *6*(4), 396–404. https://doi.org/10.1016/j.ejfs.2016.06.003

Ketaren, E. (2016). Cybercrime, Cyber Space, Dan Cyber Law. *Jurnal TIMES*, *5*(2), 35–42.

KumparanNews. (2019). Seputar Vandalisme "Bacot" di Laman Wikipedia Arteria Dahlan. Retrieved April 5, 2020, from Kumparan website: https://kumparan.com/kumparannews/seputar-vandalisme-bacot-di-laman-wikipedia-arteria-dahlan-1s2aeVIdDdy

Kurnia, A. J. (2018). Perbuatan-perbuatan Pidana dalam Cyberspace. Retrieved August 14, 2018, from HukumOnline.com website: https://www.hukumonline.com/klinik/detail/ulasan/cl3509/perbuatan-perbuatan-pidana-dalam-icyberspace-i

Maskun. (2014). *Cyber Crime* (Kedua). Jakarta: Kencana Prenada Media Group.

Matthews, C. M. (2013). Support Grows to Let Cybertheft Victims ' Hack Back '. *The Wall Street Journal*, 1–4.

Partodihardjo, S. (2008). *Tanya Jawab Sekitar UU No. 11 Tahun 2008 tentang Informasi Transaksi Elektronik*. Jakarta: PT. Gramedia Pustaka Utama.

Rahmayunita, I. S. | H. (2019). Profil Arteria Dahlan Dirusak, Admin Wikipedia Naik Pitam. Retrieved October 20, 2020, from Suara.com website: https://www.suara.com/news/2019/10/10/134057/profil-arteria-dahlan-dirusak-admin-wikipedia-naik-pitam

Soerjono Soekanto, S. M. (2015). *Penelitian Hukum Normatif Suatu Tinjauan Singkat* (17th ed.). Jakarta: RajaGrafindo Persada.

Suseno, S. (2012). *Yuridiksi Tindak Pidana Siber* (Cet-1). Bandung: PT. Refika Aditama.

Tejaswini Herath, H. R. R. U. (2012). Internet Crime: How Vulnerable Are You? Do Gender, Social Influence and Education Play a Role in Vulnerability? In *Cyber Crime: Concepts, Methodologies, Tools and Applications* (p. 9). United States of America: Information Science Publishing (an imprint of IGI Global).

Timothy Paul Cronan, C. Bryan Foltz, T. W. J. (2006). Piracy, Computer "Crime" and Is Misuse at The University. *COMMUNICATIONS OF THE ACM*, *49*(6), 84–90.