Disiplin : Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum sumpah Pemuda
http://disiplin.stihpada.ac.id/
p-issn : 1411-0261 e-issn : 2746-394X
available online at http://disiplin.stihpada.ac.id/index.php/Disiplin/article/view/39/41
Volume 27 Nomor 2 Mei 2021 : 84 - 97
doi : doi.org/10.5281/zenodo.4979012

ANALISIS NORMATIF UPAYA PENCEGAHAN PRAKTIK PENIPUAN MELALUI MEDIA INTERNET (INTERNET FREUD) DALAM PERSPEKTIF HUKUM INTERNASIONAL DAN KENDALANYA

Firman Freaddy Busroh, Erleni, Tobi Haryadi
Sekolah Tinggi Ilmu Hukum Sumpah Pemuda
firmanbusroh@gmail.com, tobishart910@gmail.com

Abstrak

Upaya Pencegahan Praktik Penipuan Melalui Media Internet (*Internet Fraud*) Dalam Perspektif Hukum Internasional dilakukan melalui Resolusi Kongres PBB VIII/1990 di Wina mengenai *computer related crimes* mengajukan beberapa kebijakan dalam upaya mencegah praktik penipuan melalui internet (*internet fraud*) antara lain: a. Mengimbau negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif, b. Melakukan modernisasi hukum pidana materiil dan hukum acara pidana; c. Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer; d. Melakukan langkah-langkah untuk membuat peka (sensitif) warga masyarakat, aparat pengadilan dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer; e. Melakukan upaya-upaya pelatihan (*training*) bagi para hakim, pejabat, dan aparat penegak hukum mengenai kejahatan ekonomi dan cybercrime; f. Memperluas *rules of ethics* dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika; g. Mengadopsi perlindungan korban *cybercrime* sesuai dengan Deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya *cybercrime*; h. Mengimbau negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan *cybercrime*; i. Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan (*Committee on Crime Prevention and Control*/CCPC) PBB untuk : Ada beberapa hal yang menjadi kendala dalam mencegah praktik penipuan dengan menggunakan media internet (*internet fraud*) dalam perspektif hukum internasional, yaitu antara lain : a. Masyarakat dunia internasional cenderung pasif atau terbatas dalam merespon kejahatan-kejahatan *cyber* yang menimpa dirinya. Secara umum masyarakat luas tidak begitu memperhatikan ataupun mewaspadai fenomena kejahatan *cyber*. Walaupun tingkat kerugian finansial akibat kejahatan *cyber* sudah sangat besar, namun warga masyarakat tidak begitu tergerak untuk menyikapinya; b. Sumber Daya Manusia (SDM) yang masih rendah yang dimiliki oleh banyak negara; c. ego sektoral dari beberapa negara; d. hubungan diplomatik yang kurang baik; e. Sistem hukum yang berlaku di negara-negara lain saling berbeda, dimana hal ini sangat menyulitkan posisi perundingan untuk menyamakan persepsi tentang sistem hukum yang dianut mengenai tindak pidana penipuan melalui media internet (*Internet Fraud*); f. Antar negara tersebut, terkadang belum memiliki kerjasama internasional dalam menanggulangi kejahatan internasional dengan menggunakan media internet (*Internet Fraud*).

Kata kunci : penegakan Hukum, Tindak Pidana, Praktik Penipuan

Abstract

Efforts to Prevent Fraud Practices Through the Internet (Internet Fraud) In the perspective of international law, this was carried out through the Resolution of the United Nations Congress VIII/1990 in Vienna regarding computer related crimes, proposing several policies in an effort to prevent fraudulent practices through the internet (internet

fraud), including: a. Calling on member countries to intensify efforts to tackle computer abuse more effectively, b. Modernizing material criminal law and criminal procedural law; c. Develop computer security and preventive measures; d. Take steps to sensitize citizens, court officials and law enforcement, to the importance of preventing computer-related crimes; e. Conduct training efforts for judges, officials, and law enforcement officers regarding economic crimes and cybercrime; f. Expanding the rules of ethics in the use of computers and teaching them through the informatics curriculum; g. Adopt the protection of victims of cybercrime in accordance with the United Nations Declaration on Victims, and take steps to encourage victims to report the existence of cybercrime; h. Calling on member countries to increase international activities in efforts to combat cybercrime; i. Recommend to the United Nations Committee on Crime Prevention and Control (CCPC) to: There are several things that become obstacles in preventing fraudulent practices using the internet (internet fraud) in the perspective of international law, namely: a. The international community tends to be passive or limited in responding to cyber crimes that befall them. In general, the wider community does not pay much attention to or pay attention to the phenomenon of cyber crime. Although the level of financial losses due to cyber crimes is already very large, the community members are not very moved to respond; b. Human Resources (HR) are still low owned by many countries; c. sectoral egos of several countries; d. poor diplomatic relations; e. The legal systems that apply in other countries are different from each other, which makes it very difficult for the negotiating position to equalize the perception of the legal system adopted regarding the crime of fraud through the internet (Internet Fraud); f. Between these countries, sometimes do not have international cooperation in tackling international crimes using the internet (Internet Fraud).

Keywords: law enforcement, crime, fraudulent practices

A. Latar Belakang

Sejalan dengan perkembangan ilmu pengetahuan dan teknologi, aktivitas ekonomi berkembang semakin pesat, baik dari sisi ragam maupun intensitasnya. Meski di negara maju sekalipun, komputer baru dinikmati rumah tangga di tahun 1970-an, dan internet dalam bentuknya yang paling sederhana digunakan di universitas-universitas di tahun 1980-an.[1] Meski demikian, saat ini, baik di negara maju maupun berkembang, komputer dan internet sudah merupakan barang kebutuhan yang sulit dinafikkan keberadaannya. Keberadaan internet membawa kemudahan orang untuk berkomunikasi dan mencari informasi. Namun tidak disanggah bahwa lewat internet pula kejahatan seksual terhadap anak-anak, plagiarisme, *bullying*, penipuan via email hingga pencucian uang justru semakin mudah dilakukan. Hal serupa terjadi pada keberadaan telepon genggam. Di satu sisi, telepon genggam mempermudah komunikasi, di sisi lain, HP (*handphone)* sering digunakan untuk praktik penipuan, dan praktik gendam. Tentu saja jika kita hidup 20-30 tahun lalu, kita tidak akan pernah berfikir munculnya berbagai aktivitas kejahatan tersebut yang memanfaatkan kemajuan teknologi informatika tersebut.

Penjelasan di atas menunjukkan bahwa perkembangan ilmu pengetahuan dan teknologi berpengaruh langsung terhadap ragam dan intensitas kegiatan ekonomi baru. Namun demikian, kecepatan munculnya jenis aktivitas ekonomi baru ini sering kali kurang diimbangi oleh upaya Pengaturan pemerintah untuk meminimas

[1]Dr. Rimawan Pradiptyo, Penegakan Hukum dan Pencegahan Tindak Kejahatan dalam Tinjauan Ilmu EkonomiDimuat pada majalan EBNEWS Edisi 9 Tahun 2011, https://feb.ugm.ac.id/en/research/lecturer-s-article/826-penegakan-hukum-dan-pencegahan-tindak-kejahatan-dalam-tinjauan-ilmu-ekonomi, diakses pada tanggal 01 Januari 2020

potensi kejahatan yang mungkin timbul. Fenomena ini tentunya bukanlah hal yang mengherankan, karena diperlukan waktu bagi pemerintah untuk mengkaji dampak buruk dari penyalahgunaan perkembangan teknologi

Seiring dengan perkembangan kebutuhan masyarakat di dunia, teknologi informasi (*information technology*) memegang peran penting, baik di masa kini maupun di masa mendatang. Teknologi informasi diyakini membawa keuntungan dan kepentingan yang besar bagi negara-negara di dunia. Setidaknya ada dua hal yang membuat teknologi informasi dianggap begitu penting dalam memacu pertumbuhan ekonomi dunia, yaitu :

a. Pertama, teknologi informasi mendorong permintaan atas produk-produk teknologi informasi itu sendiri, seperti komputer, modem, sarana untuk membangun jaringan internet dan sebagainya;
b. Kedua, adalah memudahkan transaksi bisnis keuangan di samping bisnis-bisnis lainnya.[2]

Dengan demikian, teknologi informasi telah berhasil memicu dan memacu perubahan tatanan kebutuhan hidup masyarakat di bidang sosial dan ekonomi, yang *notabene* sebelumnya bertransaksi ataupun bersosialisasi secara konvensial menuju transaksi ataupun sosialisasi secara elektronik. Hal ini dinilai lebih efektif dan efisien. Sebagai akibat dari perkembangan teknologi yang sangat pesat tersebut, maka secara lambat laun teknologi informasi dengan sendirinya juga telah mengubah perilaku masyarakat dan peradaban manusia secara global. Di samping itu, perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial secara signifikan berlangsung demikian cepat.

Internet merupakan bukti dari perkembangan teknologi komunikasi dan informasi, yang dalam sejarahnya berkembang dengan sangat pesat dan telah menciptakan dunia baru atau *cyberspace. Cyberspace*, sebuahdunia komunikasi berbasis komputer (*computer mediated communication*) ini menawarkan realitas yang baru, yaitu realitas virtual (*virtual reality*).[3] Dengan terciptanya realitas virtual dari penggunaan internet tersebut, pengguna dimanjakan untuk berkelana menelusuri dunia *cyberspace* dengan menembus batas kedaulatan suatu negara, batas budaya, batas agama, batas geografis, politik, ras, hirarki, birokrasi dan sebagainya.[4] Dengan berkembangnya internet, semakin banyak orang menikmati realitas baru yang ditawarkan. Manusia dapat melakukan berbagai di internet layaknya di dunia nyata.[5] Aktivitas Para penikmat *cyberspace* atau disebut netizen, duduk berlama-lama di depan layar komputer, menanggalkan segala atribut dan menikmati sajian internet yang ditawarkan.

Melihat hal di atas, segala sesuatu yang berkembang tentu akan menimbulkan dampak baik berupa dampak bersifat positif maupun dampak negatif. Begitu pula halnya dengan perkembangan internet seperti pada penjelasan di atas, bahwa perkembangan internet yang sangat pesat juga membawa dampak positif dan negatif dalam kehidupan masyarakat penggunanya yang telah sampai pada tingkat global saat ini. Kejahatan sangat erat kaitannya dengan perkembangan masyarakat. Semakin maju kehidupan masyarakat, maka kejahatan juga ikut semakin maju. Kejahatan pun menjadi sebagian dari budaya itu sendiri. Hal ini berarti semakin tinggi budaya dan semakin modern suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaannya.[6] Selain hal tersebut di atas, banyak pula dampak

[2] Agus Raharjo, *Cyber Crime: Pemahaman dam Upaya Pencegahan Kejahatan Berteknologi*, Citra Aditya Bakti, Bandung, 2002,hlm. 1

[3] *Ibid, hlm. 91*

[4] *Ibid*

[5] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime*), PT Refika Aditama, Bandung, 2005, hlm. 24

[6] Abdul Wahid dan Mohammad Labib,*Kejahatan Mayantara (Cyber Crime*), Op.Cit., hlm.23.

negatif yang timbul sebagai akibat dari perkembangan dan penggunaan internet hingga saat ini. Telah dijelaskan di depan bahwa dengan semakin muktahirnya teknologi dan perkembangan fasilitas internet, semua orang dapat dengan mudah menggunakan dan menikmati setiap hal yang disajikan di internet.

Teknologi informasi dan komunikasi telah mengubah perilaku masyarakat dan peradaban manusia secara global. Di samping telah menyebabkan dunia menjadi tanpa batas (*borderless*)[7] dan menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat seperti pergeseran nilai sosial masyarakat dan cenderung menciptakan kepribadian yang individualistis, juga sekaligus membuka peluang besar bagi terjadinya tindak kejahatan melalui penggunaan dunia siber tersebut atau dikenal dengan istilah kejahatan dunia siber/maya (*cyber crime*). Dengan terjadinya perbuatanperbuatan melawan hukum tersebut, maka ruang lingkup hukum harus diperluas untuk menjangkau perbuatan-perbuatan tersebut, seperti tindak manipulasi data, *hacking* dan tindak penipuan yang menggunakan fasilitas-fasilitas di internet.

Media sosial (*social media*)[8] sebagai media komunikasi yang saat ini sedang diminati oleh hampir seluruh pengguna internet atau netizen menjadi salah satu sarana melakukan penipuan internet ini. Hal ini dapat kita lihat pada banyaknya kasus penipuan online yang terjadi, seperti pada kasus penipuan jual-beli *online* , penipuan investasi *online*, dan penipuan. Hal ini jelas sangat mengganggu jalannya kenyamanan penggunaan internet, kenyamanan privasi, mengganggu dunia bisnis, dan sebagainya dimana banyak pengguna yang sangat dirugikan serta menjadi ancaman stabilitas sistem keamanan dan ketertiban masyarakat secara nasional terlebih jika hal ini merupakan kejahatan siber yang dilakukan dalam skala transnasional.

Untuk mengatasi hal tersebut di atas, jelas diperlukan tindakan penanganan melalui peraturan perundang-undangan yang cermat mengingat suatu hal, yakni jangan sampai perundang-undangan menjadi terpaku dan ikut arus pada perkembangan teknologi sehingga membuat peraturan yang *overlegislate*, yang pada gilirannya justru akan membawa dampak negatif, baik di bidang hukum lainnya maupun di bidang sosial ekonomi baik di tingkat nasional maupun dunia internasional.

B. Permasalahan

1. Apasajakah upaya yang dapat dilakukan dalam upaya mencegah terjadinya praktik penipuan melalui media internet dalam perspektif Hukum Internasional ?
2. Apasajakah yang menjadi kendala dalam pencegahan praktik penipuan melalui internet dalam perspektif hukum internasional ?

C. Metodologi Penelitian

Selaras dengan judul dan latar belakang seperti yang telah dipaparkan diatas, maka penulis menggunakan metode penelitian normatif yaitu penelitian yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder yang mencakup bahan hukum primer, sekunder dan tersier. Sumber data yang dipergunakan dalam penelitian ini adalah data sekunder yaitu data yang diperoleh melalui penelitian kepustakaan.

D. Pembahasan

I. Upaya Pencegahan Praktik Penipuan Melalui Media Internet (Internet Fraud) Dalam Perspektif Hukum Internasional

Secara umumUndang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur tentang segala sesuatu mengenai data elektronik dan pemanfaatannya untuk kepentingan umum. Pada awal pembentukannya undang-undang ini menuai banyak kontroversi karena dianggap akan mematikan kebebasan untuk

[7] Asa Briggs dan Peter Burke, *Sejarah Sosial Media: Dari Gutenberg sampai Internet. Terjemahan oleh A. Rahman Zainuddin*, Yayasan Obor Indonesia,Jakarta, 2006, hlm. 375.

[8] *Ibid*

mengekspresikan diri di *cyberspace*. Dalam undang-undang ini secara rinci dijelaskan mengenai segala perbuatan yang digolongkan sebagai *cybercrime*, jenis-jenis perbuatan ini diatur dalam Pasal 27sampai dengan Pasal 37.

Indonesia sendiri berada di urutan kedua dalam daftar lima besar negara asal serangan kejahatan siber atau *cyber crime*, berdasar laporan *State of The Internet* 2013.[9] Dalam kurun waktu tiga tahun terakhir, tercatat 36,6 juta serangan cyber crime terjadi di Indonesia. Hal ini sesuai dengan data *Security Threat* 2013 yang menyebutkan Indonesia adalah negara paling berisiko mengalami serangan cyber crime. Sejak 2012 sampai dengan April 2015, Subdit IT/Cyber Crime telah menangkap 497 (empat ratus Sembilan puluh tujuh) orang tersangka kasus kejahatan di dunia maya. Dari jumlah tersebut, sebanyak 389 (tiga ratus delapan puluh sembilan) orang di antaranya merupakan warga negara asing, dan 108 orang merupakan warga negara Indonesia. Total kerugian *cyber crime* di Indonesia mencapai Rp 33,29 miliar, angka ini jauh lebih besar dibandingkan perampokan nasabah bank secara konvensional.[10]

Dalam kasus tindak pidana transaksi elektronik, modus yang sering dipakai terutama undian mendapatkan hadiah atau undian lewat internet, lewat iklan jual barang murah di toko online, kasus penipuan lewat rekening bank palsu dan lainnya. Kejahatan penipuan dengan menggunakan transaksi elektronik memiliki keunikan dan kekhasan karena kejahatan ini terjadi dalam ruang lingkup teknologi informasi. Modus penipuan melalui media internet dengan modus menawarkan barang-barang elektronik seperti handphone berbagai merk, kamera, laptop berbagai merk dengan harga murah di jejaring sosial *facebook*. Pelaku membuat akun *facebook* baru atau membobol akun facebook milik orang lain kemudian menambah pertemanan hingga ribuan orang. Kemudian pelaku menawarkan barang-barang elektronik dengan harga murah. Untuk meyakinkan korbannya, pelaku mengaku sebagai bagian marketing dan berusaha meyakinkan bahwa barang akan dikirim melalui jasa titipan kilat apabila *Down Payment* (DP) sudah dikirim ke rekening pelaku. Setelah DP dikirim, seolah-olah ada yang menelepon korban mengaku sebagai bagian pengiriman barang dan mengatakan bahwa barang sudah dikirim. Untuk meyakinkan korbannya, pelaku mengirimkan resi pengiriman. Keesokan harinya korban mendapat telepon mengaku bagian pengiriman dan menginformasikan bahwa telah terjadi kelebihan jumlah ítem yang dikirimkan dan mengharuskan korban untuk membayar saja kelebihan barang yang dikirimkan tersebut dengan imingiming diberikan diskon karena hal tersebut adalah kesalahan bagian pengiriman.

Korban pun banyak yang tergiur dengan penawaran pelaku kemudian dengan mudahnya mentransfer uang ke rekening pelaku. Tindak pidana penipuan dengan menggunakan sarana transaksi elektronik merupakan suatu rintangan terhadap percepatan pembangunan ekonomi di Indonesia, karena kejahatan ini dapat menimbulkan akibat kumulatif yang tidak sederhana, salah satunya adalah beralihnya investasi perdagangan berbasis *e commerce*. Kebutuhan terhadap teknologi komunikasi dan informasi pada awalnya digunakan hanya untuk saling tukar informasi tetapi kemudian meningkat dari sekedar media komunikasi kemudian menjadi sarana untuk melakukan kegiatan komersil seperti informasi, promosi, penjualan dan pembelian produk.

Terhadap adanya internet sendiri, di samping menciptakan berbagai peluang baru dalam kehidupan masyarakat, internet juga sekaligus menciptakan peluang-peluang baru bagi kejahatan. Pemerintah Indonesia secara tertulis melalui teks perunda-

[9]Ni'matul Huda, *Negara Hukum, Demokrasi & Judicial Review*, UII Press, Yogyakarta, 2005, hlm. 8.

[10] Hotma P. Sibuea, *Asas Negara Hukum, Peraturan Kebijakan & Asas-asas Umum Pemerintahan yang Baik*, Erlangga, Jakarta, 2010, hlm. 37.

ng-undangan sudah memberikan upaya perlindungan hukum dan rasa aman terhadap segala perbuatan hukum yang berhubungan dengan teknologi informasi termasuk transaksi elektronik, yaitu dengan diakomodasinya hak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia.

Tetapi, setelah hampir 12 (dua belas) tahun undang-undang ini diberlakukan, berbagai kasus penipuan dengan menggunakan transaksi elektronik tetap meningkat dan cenderung semangat pencegahan terhadap kejahatan dengan menggunakan transaksi elektronik hanya ada sebatas teks tertulis dalam undangundang tanpa disertai upaya konkret dan sistematis untuk mewujudkannya. Penipuan dengan menggunakan transaksi elektronik merupakan masalah bersama, oleh karena itu masyarakat juga pemerintah turut bertanggung jawab dengan melakukan pencegahan dari segala bentuk kejahatan yang menggunakan transaksi elektronik. Sehingga ada perubahan sikap yang mendasar dalam kehidupan bermasyarakat yang menganggap bahwa tindak pidana penipuan dengan menggunakan transaksi elektronik bukan sekedar masalah individu tetapi merupakan tanggung jawab bersama.

Kebutuhan masyarakat terhadap rasa aman dan terlindungi merupakan salah satu hak asasi yang harus diperoleh atau dinikmati setiap orang. Rasa aman dan terlindungi juga merupakan kebutuhan dasar masyarakat yang sangat penting, setelah kebutuhan akan sandang, pangan dan papan. Hak atas rasa aman dan terlindungi masyarakat tersebut, tertuang dalam UUD 1945 Pasal 28G ayat (1) yang menerangkan: "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi". Undang-undang Dasar Negara Republik Indonesia Tahun 1945 (selanjutnya disingkat UUD 1945) sebagai landasan konstitusional yang di dalamnya dijiwai oleh Pancasila, merupakan arah politik dari hukum nasional yang dimuat dalam Alinea Keempat Pembukaan Undang-undang Dasar Negara Republik Indonesia Tahun 1945, sebagai berikut: …

> "untuk membentuk suatu pemerintahan negara Indonesia yang melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteran umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial"

Dalam suatu negara hukum kedudukan dan hubungan warga dengan negara adalah dalam suasana keseimbangan, sama-sama mempunyai hak yang dilindungi oleh hukum dan sama-sama dibatasi oleh hukum.[11] Sementara itu, menurut Mochtar Kusuma atmadja, bahwa tujuan hukum tersebut pada akhirnya diarahkan untuk memberikan perlindungan kepada kepentingan manusia, yaitu kepentingan dalam melangsungkan dan memenuhi kebutuhan hidup yang layak tanpa diskriminasi. Oleh karenanya, hukum bukan hanya sekedar keseluruhan asas-asas dan kaidah-kaidah yang mengatur kehidupan manusia dalam masyarakat yang meliputi lembaga-lembaga (*institutions)* dan proses-proses (*process*), tetapi melalui hukum ini hendak diwujudkan berlakunya tujuan hukum menjadi kenyataan.[12] Hukum bukan tujuan, tetapi dibuat sebagai sarana mencapai tujuan hukum yang dapat digerakkan untuk merekayasa umat manusia menuju tujuan yang baik dan benar serta diridhai Allah SWT atau dalam istilah Roscoe Pound adalah *law as a tool of social engineering* (hukum

[11]Mochtar Kusumaatmadja, *Fungsi dan Perkembangan Hukum dalam Pembangunan Nasional*, Binacipta, Bandung, Tanpa Tahun, hlm. 3.

[12]*Ibid*

sebagai alat pembaharuan masyarakat) atau dengan perkataan lain, sebagaimana dikemukakan Mochtar Kusumaatmadja, bahwa hukum merupakan sarana pembangunan (*a tool of development*), yakni hukum dalam arti kaidah atau peraturan hukum yang difungsikan sebagai alat (pengatur) atau sarana yang mengatur pembangunan dalam penyalur arah kegiatan manusia ke arah yang dikehendaki oleh pembangunan atau pembaruan.

Demokrasi sebagai suatu sistem politik dalam negara hukum memuat atau mengandung esensi persamaan (*equity*) dan kebebasan (*liberty*) warga negara. Warga negara adalah pemilik kedaulatan, oleh karena itu hak-hak warga negara yang menjelma sebagai hak asasi harus terjamin keberadaan dan implementasinya dalam negara. Begitu juga bagi masyarakat pengguna transaksi elektronik tentunya mempunyai hak yang sama untuk mendapatkan perlindungan hukum dalam menjalankan segala perbuatan hukum melalui sarana teknologi informasi. Suatu negara yang berdasarkan atas hukum harus menjamin Konsekuensi, bahwa Indonesia negara berdasarkan hukum (*rechtsstaat*) tidak berdasarkan atas kekuasaan belaka (*machtstaat*) dan pemerintahan berdasarkan sistem konstitusi (hukum dasar) bukan absolutisme (kekuasaan yang tidak terbatas) dengan prinsip dasar yang wajib dijunjung tinggi oleh setiap warga negara adalah supremasi hukum, kesetaraan di hadapan hukum, dan penegakan hukum dengan cara-cara yang tidak bertentangan dengan hukum.

Pada dasarnya setiap manusia terlahir sebagai makhluk ciptaan ALLAH SWT, yang secara kodrati mendapatkan hak dasar yaitu kebebasan, hak hidup, hak untuk dilindungi dan hak lainnya. Hal ini senada dengan prinsip hukum alam pada abad ke-18 yaitu kebebasan individu dan keutamaan rasio, salah satu penganutnya adalah Locke, menurut Locke teori hukum beranjak dari kebebasan individu dan keutamaan rasio. Locke juga mengajarkan pada kontrak sosial, menurutnya yang melakukan kontrak sosial adalah manusia yang tertib dan menghargai kebebasan, hak hidup dan pemilikan harta sebagai hak bawaan manusia.

Menurut Locke, hak-hak tersebut tidak diserahkan kepada penguasa ketika kontrak sosial dilakukan. Oleh karena itu, kekuasaan penguasa yang diberikan lewat kontrak sosial dengan sendirinya tidak mungkin bersifat mutlak, dengan begitu kekuasaan tersebut justru untuk melindungi hak-hak kodrat dimaksud dari bahaya-bahaya yang mungkin mengancam, baik datang dari dalam maupun dari luar. Begitu juga hukum yang dibuat dalam Negara, bertugas melindungi hak-hak dasar tersebut. Hak-hak dasar yang biasa disebut sebagai hak asasi, tanpa perbedaan antara satu dengan lainnya. Dengan hak asasi manusia dapat mengembangkan diri pribadi, peranan dan sumbangannya bagi kesejahteraan hidup manusia. Prinsip perlindungan hukum terhadap tindakan pemerintah bertumpu dan bersumber dari konsep tentang pengakuan dan perlindungan terhadap hak-hak asasi manusia, karena menurut sejarah dari barat lahirnya konsep-konsep tentang pengakuan dan perlindungan terhadap hak-hak asasi manusia diarahkan kepada pembatasan-pembatasan dan peletakkan kewajiban masyakat dan pemerintah.

Dunia internasional, melalui Kongres PBB, telah melakukan Lokakarya yang diorganisir oleh UNAFEI selama kongres PBB X/2000 berlangsung telah memberikan pedoman dalam melakukan upaya pencegahan terhadap kejahatan yang berhubungan dengan jaringan komputer melalui dunia internasional, yaitu:[13]

a. *Computer Related Crime* (CRC) harus dikriminalisasikan;
b. Diperlukan hukum acara yang tepat untuk melakukan penyidikan dan penuntutan terhadap penjahat *cyber* (*cyber criminals*);

[13] *https://media.neliti.com/media/publications/3421-ID-pembuktian-terhadap-kejahatan-dunia-maya-dan-upaya-mengatasinya-menurut-hukum-po.pdf, diakses pada tanggal 02 Februari 2020*

c. Harus ada kerja sama antara pemerintah dan industri terhadap tujuan umum pencegahan dan penanggulangan kejahatan komputer agar internet menjadi tempat yang aman;
d. Diperlukan kerja sama internasional untuk menelusuri/mencari penjahat di internet;
e. PBB harus mengambil langkah/tindak lanjut yang berhubungan dengan bantuan kerja sama teknis dalam penanggulangan CRC.

Perserikatan Bangsa-Bangsa (PBB) pernah mengadakan kongres mengenai *The Prevention Of Crime and The Treatment Of Offenders* yang telah membahas masalah mengenai *cybercrime*. Masalah c*ybercrime* diagendakan pada Kongres VIII/1990 di Havana dan pada Kongres X/2000 di Wina. Resolusi Kongres PBB VIII/1990 di Wina-mengenai *computer related crimes* mengajukan beberapa kebijakan dalam upaya mencegah praktik penipuan melalui internet (internet fraud) antara lain:[14]

a. Mengimbau negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah di antaranya:
    1) Melakukan modernisasi hukum pidana materiil dan hukum acara pidana;
    2) Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer;
    3) Melakukan langkah-langkah untuk membuat peka (sensitif) warga masyarakat, aparat pengadilan dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer;
    4) Melakukan upaya-upaya pelatihan (*training*) bagi para hakim, pejabat, dan aparat penegak hukum mengenai kejahatan ekonomi dan cybercrime;
    5) Memperluas *rules of ethics* dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika;
    6) Mengadopsi perlindungan korban *cybercrime* sesuai dengan Deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya *cyberrcrime*.
b. Mengimbau negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan *cybercrime*;
c. Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan (*Committee on Crime Prevention and Control*/CCPC) PBB untuk:
    1) Menyebarluaskan pedoman dan standar untuk membantu negara anggota menghadapi cybercrime di tingkat nasional, regional, dan internasional;
    2) Mengembangkan penelitian dan analisis lebih lanjut guna menemukan cara-cara baru menghadapi problem cybercrime di masa yang akan datang;
    3) Mempertimbangkan*cybercrime* sewaktu meninjau pengimplementasian perjanjian ekstradisi dan bantuan kerja sama di bidang penanggulangan kejahatan.

Berdasarkan resolusi PBB tersebut, tindakan penanggulangan terhadap cybercrime tidak hanya melalui kebijakan hukum pidana, baik hukum pidana material maupun hukum pidana formal, tetapi juga dengan kebijakan pencegahan. Kebijakan pencegahan yang didapatkan didalam Resolusi PBB tersebut adalah upaya mengembangkan pengamanan atau perlindungan komputer dan tindakan-tindakan pencegahan

[14] *Ibid*

yang dapat dilihat dalam Resolusi PBB di atas. Hal ini terkait denganpendekatan *techno-prevention*, yaitu upaya pencegahan atau penanggulangan kejahatan dengan menggunakan teknologi. Kongres PBB menyadari bahwa *cybercrime* yang terkait erat dengan kemajuan teknologi tidak dapat ditanggulangi dengan pendekatan yuridis, tetapi juga harus dengan pendekatan teknologi itu sendiri.

Selain dari hal untuk mengamankan teknologi itu sendiri, dalam Resolusi PBB tersebut juga melihak aspek lain lain yang menarik yaitu perlu adanya pendekatan budaya atau kultural dalam kebijakan penanggulangan *cybercrime* dengan cara membangun atau membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah *cybercrime* dan menyebarluaskan atau mengajarkan etika penggunaan komputer melalui media pendidikan sesuai dengan Resolusi PBB.Selain berdasarkan Kongres PBB VIII/1990 dan Kongres X/2000, penyusunan perangkat hukum tentang *cybercrime* yang dihasilkan oleh G-8 *dalam communique* tanggal 9-10 Desember 1997 menghasilkan 10 butir asas dan 10 agenda aksi yang dapat dilakukan dalam mencegah praktik penipuan dengan media internet (Internet Fraud) melalui dunia internasional, yaitu:[15]

1. Tidak akan ada tempat perlindungan yang aman bagi mereka yang menyalahgunakan teknologi informasi;
2. Penyidikan dan penuntutan terhadap *high-tech international crime* harus dikoordinasikan di antara negara-negara yang menaruh perhatian, tanpa melihat di mana akibat yang merugikan terjadi;
3. Aparat penegak hukum harus dilatih dan dilengkapi dalam menghadapi *high-tech crime*;
4. Sistem hukum harus melindungi kerahasiaan, integritas, dan keberadaan data dan sistem dari perbuatan yang tidak sah dan menjamin bahwa penyalahgunaan yang serius harus dipidana;
5. Sistem hukum harus mengizinkan perlindungan dan akses cepat terhadap data elektronik, yang sering kali kritis bagi suksesnya penyidikan kejahatan;
6. Pengaturan *mutual assistance* harus dapat menjamin pengumpulan dan pertukaran alat bukti tepat pada waktunya, dalam kasus-kasus yang berkaitan dengan high-tech crime;
7. Akses elektronik lintas batas oleh penegak hukum terhadap keberadaan informasi yang bersifat umum, tidak memerlukan pengesahan dari negara di mana data tersebut berada;
8. Standar forensik untuk mendapatkan dan membuktikan keaslian data elektronik dalam rangka penyidikan tindak pidana dan penuntutan harus dikembangkan dan digunakan;
9. Untuk kepentingan praktis, sistem informasi dan telekomunikasi harus didesain untuk membantu mencegah dan mendeteksi penyalahgunaan jaringan, dan harus memfasilitasi pencarian penjahat dan pengumpulan bukti;
10. Bekerja di lingkungan ini harus berkoordinasi dengan pekerjaan lain di era informasi yang relevan untuk menghindari duplikasi kebijakan.

Menurut salah satu organisasi internasioal yang bernama *The Organization for Economic Cooperation and Development* (OECD), ada beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan *cybercrime* adalah :[16]

1. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya;
2. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional;

[15]Mulyana W. Kusuma, *Perspektif, Teori, Dan Kebijaksanaan Hukum*, CV. Rajawali, Jakarta, 1986, Hlm 43

[16]Dr. H. Obsatar Sinaga, *Penanggulangan Kejahatan Internasional Cyber Crime Di Indonesia*, Universitas Padjadjaran, Bandung, 2010, Hlm 23.

3. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan cybercrime;
4. Meningkatkan kesadaran warga negara mengenai masalah cybercrime serta pentingnya mencegah kejahatan tersebut terjadi;
5. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan cybercrime.

Instrumen hukum Internasional yang dapat dirujuk dalam fenomena *cyber crime* sebagai kejahatan transnasional adalah *United Nations Conventions Againts Transnational Organized Crime*, atau yang dikenal dengan *Palermo Convention*, tahun 2000. Dalam *Palermo Convention* ini ditetapkan bahwa kejahatan-kejahatan yang termasuk dalam kejahatan transnasional adalah *cybercrime* salah satunya. *Cyber Crime* merupakan bentuk perkembangan kejahatan transnasional yang cukup menghawatirkan saat ini. Konvensi ini meskipun pada awalnya dibuat oleh negara regional Eropa, tetapi dalam perkembangannya dimungkinkan untuk diratifikasi dan diaksesi oleh negara manapun di dunia yang memiliki komitmen dalam upaya mengatasi kejahatan mayantara.

II. Kendala Dalam Pencegahan Praktik Penipuan Melalui Internet (Internet Fraud) Dalam Perspektif Hukum Internasional

European Convention on Cyber Crime[17] merupakan konvensi tentang *cyber* crime yang disepakati oleh negara-negara anggota Uni Eropa, namun konvensi ini terbuka bagi negara lain di luar Uni Eropa untuk mengikutinya. Oleh karena banyak negara yang mengikuti konvensi tersebut, maka isi perjanjian ini menjadi model bagi banyak pengaturan *cybercrime* di berbagai negara. Oleh karenanya menjadi penting bagi negara kita untuk merujuk konvensi ini sebagai salah satu pembanding bagi pengaturan cybercrime di Indonesia. Dalam konvensi ini *cybercrime* diatur mulai dari pasal (*article*) 2 sampai dengan Pasal 7.

Berbicara tentang kejahatan dalam konteks *cybercrime*, maka perlu mendalami tentang pelaku kejahatan, modus kejahatan, reaksi sosial atas kejahatan, dan hukum yang berlaku. *Cybercrime* sebagai kejahatan yang menggunakan teknologi dunia maya (komputer) sudah semakin marak terjadi di semua negara di dunia. Pelakunya sangat beragam yang pasti mereka orang-orang yang, sangat profesional, dan yang semula hanya kebetulan (iseng), dan dilakukan kalangan berpendidikan cukup namun akrab dengan komputer, sampai dengan pelaku kejahatan yang sangat profesional dan berdasi (*white collor crime*).

Modus operandi kejahatan, dilakukan dengan penyamaran atau memakai identitas palsu, penipuan, pembajakan, dan penyusupan, sedangkan reaksi sosial masyarakat terhadap kejahatan dunia maya hanya terbatas kalangan tertentu yang biasa memanfaatkannya. Masyarakat luas cenderung pasif atau terbatas dalam merespon kejahatan-kejahatan *cyber* yang menimpa dirinya. Secara umum masyarakat luas tidak begitu memperhatikan ataupun mewaspadai fenomena kejahatan *cyber*. Karena barangkali pengguna atau pengakses komputer/-internet belum begitu membudaya di Indonesia. Walaupun tingkat kerugian finansial akibat kejahatan *cyber* sudah sangat besar, namun warga mssyarakat tidak begitu tergerak untuk menyikapinya.

Reaksi sosial masyarakat yang positif dalam menyikapi penegakan hukum internasional dalam masalah pidana pada kasus *cybercrime*, cenderung terbatas pada kalangan akademisi tertentu, dan jajaran penegak hukum tertentu pula. Hal itu

[17] Nani Mulyati (Tim), *Harmonisasi Hukum Pengaturan Cyber crime Dalam Undang -Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*, sumber : http://lp.unand.ac.id/?pModule=news&pSub=news&pAct=detail& detail=234 , 21 Mei 2010 , diakses tanggal 20 Oktober 2019 .

diwujudkan dengan usulan perubahan perundang-undangan agar dapat mengantisipasi semakin canggihnya kejahatan *cyber*, sekaligus kompleksitas Undang-Undang Nomor 1 Tahun 2006Tentang Bantuan Timbal Balik Dalam Masalah Pidana. Sedangkan hukum yang berlaku saat di Indonesia ini diantaranya Undang Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE), walaupun terdapat ketentuan pidana terkait *cybercrime* masih belum komprehensif. Dan RUU Tindak Pidana Teknologi Informasi, telah selesai dibuat,diantaranya merujuk pada salah satu instrumen hukum internasional yaitu EU *Convention on CyberCrime* 2001 yang dibuat tanggal 23 Nopember 2001 di kota Budapest, Hongaria oleh Uni Eropa.

Menurut Sutan Remmy Syahdeini, jutaan rekening telah dibobol. Apabila seorang pemegang kartu kecurian atau kehilangan kartu kreditnya ia memang dapat melaporkan kehilangan tersebut secepat mungkin, tetapi data tentang rekening yang akan dibobol oleh pelaku dapat disimpan selama beberapa minggu atau bulan sebelum kejahatan yang dirancang oleh pelaku itu dilaksanakan. Hal itu mengakibatkan kesulitan dalam mengidentifikasi asal muasal pembobolan tersebut. Pemegang kartu kredit dapat tidak segera menyadari tentang telah terjadinya pembobolan terhadap rekeningnya dan baru mengetahui hal itu dari billing statement yang diperolehnya dari bank beberapa lama setelah pembobolan itu terjadi.

Banyak faktor yang melatar-belakangi sulitnya memberantas penipuan melalui media internet (internet Fraud) antara lain sumber daya manusia (SDM) yang rendah, tidak renponsif, dan ego sektoral, dana, kecepatan, antar negara, hubungan diplomatik yang baik, kepentingan Indonesia menghendakinya.

Kendala yang utama dalam penerapannya berkenaan dengan sistem hukum yang berlaku di negara-negara lain saling berbeda. Hal ini sangat menyulitkan posisi perundingan untuk menyamakan persepsi tentang sistem hukum yang dianut. Belum lagi kalau menyangkut kepentingan nasional yang di dalamnya melekat kepentingan politik, dan keamanan nasionalnya.

Sebagai perwujudan kerjasama internasional antar Kepolisian baik yang diwadahi oleh Interpol maupun antar kerjasama Kepolisian Republik Indonesia dengan Kepolisian Negara lain, biasa dilakukan melalui *Handling Over* yaitu menyerahkan tersangka kejahatan melalui mekanisme deportasi plus plus. Amerika Serikat sering melakukan kerjasama dengan Indonesia, diantaranya menyerahkan tersangka/kasus David Nusa Jaya kepada Indonesia. Biasanya diserahkan di bandara suatu negara bagian Amerika Serikat. Dengan wadah Interpol, kerjasama internasional dalam penanggulangan kejahatan seluruh anggota interpol, melalui mekanisme ekstradisi, dan deportasi.

Dari apa yang telah di jabarkan diatas, maka terdapatlah beberapa hal yang menjadi kendala dalam mencegah praktik penipuan dengan menggunakan media internet (*internet fraud*) dalam perspektif hukum internasional, yaitu antara lain :

1. Masyarakat dunia internasional cenderung pasif atau terbatas dalam merespon kejahatan-kejahatan *cyber* yang menimpa dirinya. Secara umum masyarakat luas tidak begitu memperhatikan ataupun mewaspadai fenomena kejahatan *cyber*. Walaupun tingkat kerugian finansial akibat kejahatan *cyber* sudah sangat besar, namun warga masyarakat tidak begitu tergerak untuk menyikapinya;
2. Sumber Daya Manusia (SDM) yang masih rendah yang dimiliki oleh banyak negara;
3. Ego sektoral dari beberapa negara;
4. Hubungan diplomatik yang kurang baik;
5. Sistem hukum yang berlaku di negara-negara lain saling berbeda, dimana hal ini sangat menyulitkan

posisi perundingan untuk menyamakan persepsi tentang sistem hukum yang dianut mengenai tindak pidana penipuan melalui media internet (*Internet Fraud*);

6. Antar negara tersebut, terkadang belum memiliki kerjasama internasional dalam menanggulangi kejahatan internasional dengan menggunakan media internet (*Internet Fraud*).

E. Kesimpulan

1. Upaya Pencegahan Praktik Penipuan Melalui Media Internet (*Internet Fraud*) Dalam Perspektif Hukum Internasional dilakukan melalui Resolusi Kongres PBB VIII/1990 di Wina mengenai *computer related crimes* mengajukan beberapa kebijakan dalam upaya mencegah praktik penipuan melalui internet (*internet fraud*) antara lain:
   a) Mengimbau negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif,
   b) Melakukan modernisasi hukum pidana materiil dan hukum acara pidana;
   c) Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer;
   d) Melakukan langkah-langkah untuk membuat peka (sensitif) warga masyarakat, aparat pengadilan dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer;
   e) Melakukan upaya-upaya pelatihan (*training*) bagi para hakim, pejabat, dan aparat penegak hukum mengenai kejahatan ekonomi dan cybercrime;
   f) Memperluas *rules of ethics* dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika;
   g) Mengadopsi perlindungan korban *cybercrime* sesuai dengan Deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya *cybercrime*;
   h) Mengimbau negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan *cybercrime*;
   i) Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan (*Committee on Crime Prevention and Control*/-CCPC) PBB untuk :
      1) Menyebarluaskan pedoman dan standar untuk membantu negara anggota menghadapi *cybercrime* di tingkat nasional, regional, dan internasional;
      2) Mengembangkan penelitian dan analisis lebih lanjut guna menemukan cara-cara baru menghadapi problem cybercrime di masa yang akan datang;
      3) Mempertimbangkan *cybercrime* sewaktu meninjau pengimplementasian perjanjian ekstradisi dan bantuan kerja sama di bidang penanggulangan kejahatan.
2. Ada beberapa hal yang menjadi kendala dalam mencegah praktik penipuan dengan menggunakan media internet (*internet fraud*) dalam perspektif hukum internasional, yaitu antara lain :
   a. Masyarakat dunia internasional cenderung pasif atau terbatas dalam merespon kejahatan-kejahatan *cyber* yang menimpa dirinya. Secara umum masyarakat luas tidak begitu memperhatikan ataupun mewaspadai fenomena kejahatan *cyber*. Walaupun tingkat kerugian finansial akibat kejahatan *cyber* sudah sangat besar, namun warga

masyarakat tidak begitu tergerak untuk menyikapinya;

b. Sumber Daya Manusia (SDM) yang masih rendah yang dimiliki oleh banyak negara;
c. ego sektoral dari beberapa negara;
d. hubungan diplomatik yang kurang baik;
e. Sistem hukum yang berlaku di negara-negara lain saling berbeda, dimana hal ini sangat menyulitkan posisi perundingan untuk menyamakan persepsi tentang sistem hukum yang dianut mengenai tindak pidana penipuan melalui media internet (*Internet Fraud*);
f. Antar negara tersebut, terkadang belum memiliki kerjasama internasional dalam menanggulangi kejahatan internasional dengan menggunakan media internet (*Internet Fraud*).

DAFTAR PUSTAKA

Agus Raharjo, *Cyber Crime: Pemahaman dam Upaya Pencegahan Kejahatan Berteknologi*, Citra Aditya Bakti,Bandung, 2002;

Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime*), PT Refika Aditama, Bandung, 2005;

Dr. H. Obsatar Sinaga, *Penanggulangan Kejahatan Internasional Cyber Crime Di Indonesia*, Universitas Padjadjaran, Bandung, 2010;

Maskun, *Kejahatan Siber (cyber crime) Suatu Pengantar*, Kencana Prenada Media Group, Jakarta, 2013;

Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*, Rajawali Pers, Jakarta, 2012;

Romli Atmasasmita, *Pengantar Hukum Pidana Internasional*, Refika Aditama, Bandung, 1981;

B.V.A. Rolling dalam Oscar Schachter, *International Law in Theory And Practice, Martinus Nijhoff Publishers, Dodrecht,* 1991;

I Wayan Parthiana, *Hukum Pidana Internasional,* Yrama Widya, Bandung, 2006;

Georg Schwarzenberger, *The Problem of An International Criminal Law*, Steven & Son, LTD, 1950;

Cherif Bassiouni, *International Criminal Law*, Transnational Publishers, 1986, New York, yang dikutip dalam Romli Atmasasmita, Pengantar Hukum Pidana Internasional;

Ni'matul Huda, *Negara Hukum, Demokrasi & Judicial Review*, UII Press, Yogyakarta, 2005;

Hotma P. Sibuea, *Asas Negara Hukum, Peraturan Kebijakan & Asas-asas Umum Pemerintahan yang Baik*, Erlangga, Jakarta, 2010;

Mochtar Kusumaatmadja, *Fungsi dan Perkembangan Hukum dalam Pembangunan Nasional*, Binacipta, Bandung, Tanpa Tahun,

Mulyana W. Kusuma, *Perspektif, Teori, Dan Kebijaksanaan Hukum*, CV. Rajawali, Jakarta, 1986;

JURNAL :

Ujang Charda S., "*Reaktualisasi Supremasi Hukum dalam Merekonstruksi Lembaga Peradilan Menuju Indonesia Baru*", Jurnal Jurista Insentif'06, Vol. 1 No. 1, Kopertis Wilayah IV Jabar – Banten, Bandung, 2006,

INTERNET DAN WIKIPEDIA :

Dr. Rimawan Pradiptyo, Penegakan Hukum dan Pencegahan Tindak Kejahatan dalam Tinjauan Ilmu EkonomiDimuat pada majalan EBNEWS Edisi 9 Tahun 2011, https://feb.ugm.ac.id/en/research/lecturer-s-article/826-penegakan-hukum-dan-

pencegahan-tindak-kejahatan-dalam-tinjauan-ilmu-ekonomi, diakses pada tanggal 01 Januari 2020

Gamble, Teri and Michael, *Communication Work. Seventh Edition*, diakses di Wikipedia.org pada 14 September 2020 pukul 12.10 WIB

Article 1 *Definitions and Use of Terms, Draft International Convention To Enhance Protection From Cyber Crime And Terrorism* dalam https://core.ac.uk/download/pdf/77625655.pdf, diakses pada tanggal 15 Januari 2020

Wawan Andriawan, Jurnal Ilmiah-*Pertanggungjawaban Pidana Pelaku Penipuan Dalam Jual Beli Melalui Sistem*, 2013,hlm. 9 diakses di fh.unram.ac.id pada 16 September 2015 pukul 21.31 WITA dalam https://core.ac.uk/download/pdf/77625655.pdf,*https://media.neliti.com/media/publications/3421-ID-pembuktian-terhadap-kejahatan-dunia-maya-dan-upaya-mengatasinya-menurut-hukum-po.pdf, diakses pada tanggal 02 Februari 2020*

Nani Mulyati (Tim*), Harmonisasi Hukum Pengaturan Cyber crime Dalam Undang - Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*, sumber : http://lp.unand.ac.id/?pModule=news&pSub=news&pAct=detail& detail=234 , 21 Mei 2010 , diakses tanggal 20 Oktober 2019 .