TEKNOLOGI NUSANTARA
Jurnal Penelitian Fakultas Teknik UNINUS
http://ojs.uninus.ac.id/index.php/teknologinusantara

E-ISSN : 2964-4577

Optimalisasi Hukum Siber (*cyber law*) dalam Penanggulangan Kejahatan Penipuan melalui Internet dalamMenyelamatkan Kehidupan Masyarakat.

Soecipto

Teknik Informatika; Jl Soekarno Hatta no 53 Kota Bandung

soecipto@gmail.com

ARTICLE INFO

Publish : 28 November 2022

ABSTRACT

Fraud through the internet is increasingly massive in various forms. This scam targets all walks of life in large numbers. Likewise involves a very large amount of money. Various modus operandi are increasingly diverse and growing. The area of operation and the mastermind of the crime can also be in all areas outside the territory of the country. Legally, both online and conventional fraud can be treated similarly to conventional offenses regulated in the Criminal Code (KUHP). Regulations regarding the use of information and communication technology are regulated in Law (UU) Number 19 of 2016 concerning Information and Electronic Transactions (UU ITE). Law 19 of 2016 is an amendment to Law Number 11 of 2008. Law Number 11 of 2008 contains regulations for information and electronic transactions in Indonesia. The research examines the Optimization of Cyber Law in Combating Fraud Crimes through the Internet in Saving People's Lives.

ABSTRAK

Penipuan melalui internet semakin massive dengan berbagai bentuk. Penipuan ini menyasar seluruh lapisan masyarakat dalam jumlah besar. Demikian juga melibatkan uang dalam jumlah yang sangat besar. Berbagai modus operandi yang semakin beragam dan semakin berkembang. Wilayah operasi dan dalang kejahatan juga dapat berada di seluruh wilayah diluar wilayah negara. Secara hukum, baik penipuan secara online maupun konvensional dapat diberi perlakuan serupa dengan delik konvensional yang diatur di dalam Kitab Undang-Undang Hukum Pidana (KUHP). Peraturan mengenai penggunaan teknologi informasi dan komunikasi diatur dalam Undang-Undang (UU) Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE). UU 19 Tahun 2016 merupakan perubahan atas UU Nomor 11 Tahun 2008. Undang-undang Nomor 11 Tahun 2008 berisi tentang aturan informasi dan transaksi elektronik di Indonesia.

Penelitian mengupas mengenai Optimalisasi Hukum Siber (cyber law) dalam Penanggulangan Kejahatan Penipuan melalui Internet dalam Menyelamatkan Kehidupan Masyarakat

Keyword:
Cyber Law, Combating Fraud Crimes

A. INTRODUCTION / PENDAHULUAN

Beberapa pendapat mengindentikkan *Cyber Crime* dengan *Computer Crime*. The U.S. *Department of Justice* memberikan pengertian computer crime sebagai : " *.... any illegal act requiring knowledge of computer technology for its perpetration, investigation or prosecution ...*" Pemahaman tersebut sesuai dengan diberikannya *Organization of European Community Development*, yang mengartikan *Computer Crime* sebagai : " *any eillegal,unethical or unatorized behavior relating to the automatic processing and/ or the transmission of data*" Dalam dua dokumen Kongres PBB mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana, Cuba pada tahun 1990 dan di Wina, Austria pada tahun 2000, ada dua istilah yang dikenal: 1. *Cyber Crime* dalam arti sempit disebut computer crime, yaitu prilaku ilegal atau melanggar secara langsung menyerang sistem keamanan suatu komputer atau data yang diproses oleh komputer 2. *Cyber Crime* dalam arti luas disebut *computer related crime*, yaitu perilaku ilegal atau melanggar yang berkaitan dengan sistem komputer atau jaringan. Penipuan melalui media daring merupakan suatu bentuk kejahatan yang menggunakan sarana teknologi di dalam kegiatannya. Pada prinsipnya penipuan secara online memiliki persamaan dengan penipuan secara biasa atau konvensional dimana setiap persoalan penipuan pasti terdapat korban yang dirugikan dan pihak lainnya diuntungkan secara tidak sah. Perbedaan antara penipuan online dengan konvensional yakni pemakaian sistem elektronik berupa perangkat internet, media sosial dan teknologi informasi. Secara hukum, baik penipuan secara online maupun konvensional dapat diberi perlakuan serupa dengan delik konvensional yang diatur di dalam Kitab Undang-Undang Hukum Pidana (KUHP). Peraturan mengenai penggunaan teknologi informasi dan komunikasi diatur dalam Undang-Undang (UU) Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE). UU 19 Tahun 2016 merupakan perubahan atas UU Nomor 11 Tahun 2008. Undang-undang Nomor 11 Tahun 2008 berisi tentang aturan informasi dan transaksi elektronik di Indonesia.

B. STUDY LITERATURE / TINJAUAN PUSTAKA

Studi Literatur yang berkaitan dengan penelitian ini adalah teori penanggulangan adalah Kebijakan atau upaya penanggulangan kejahatan pada hakikatnya merupakan bagian integral berasal dari usaha melindungi warga negara (*social defence*) dan upaya meraih kesejahteraan (*social welfare*). Kebijakan penanggulangan kejahatan atau disebut juga sebagai politik kriminal memiliki target akhir atau target utama yaitu "perlindungan warga negara untuk meraih kesejahteraan masyarakat". Kebijakan penanggulangan kejahatan (*criminal policy*) itu sendiri merupakan bagian dari kebijakan penegakan hukum (*law enforcement policy*). Kebijakan penegakan hukum merupakan bagian yang berasal dari kebijakan social (*social policy*) dan termasuk didalam kebijakan legislatif (*legislative policy*). Politik kriminal pada hakikatnya termasuk merupakan bagian integral kebijakan sosial yaitu kebijakan atau upaya untuk meraih kesejahteraan sosial (Arif, 2008:2).

Kebijakan kriminal atau kebijakan penanggulangan kejahatan jika dicermati ruang lingkupnya, sangat luas dan sangat kompleks. Hal ini wajar dikarenakan pada hakikatnya kejahatan merupakan kasus kemanusiaan dan sekaligus kasus sosial yang membutuhkan pemahaman tersendiri. Kejahatan sebagai kasus sosial adalah merupakan tanda-tanda yang dinamis yang terus tumbuh dan memiliki hubungan dengan tanda-tanda dan struktur kemasyarakatan lainnya yang memiliki kompleksitas tinggi, hal ini merupakan permasalahan-permasalahan sosial politik.

Salah satu bentuk perencanaan dukungan sosial adalah upaya- upaya yang rasional berasal dari warga negara untuk menanggulangi kejahatan yang biasa disebut bersama politik kriminal (*criminal politic*). Sasaran akhir dari politik kriminal adalah suatu proteksi bagi masyarakat. Dengan demikianlah politik kriminal adalah merupakan bagian dari rencana melindungi masyarakat, yang merupakan bagian dari total kebijakan sosial. Upaya penanggulangan kejahatan yang dilaksanakan terhadap anak memang tidaklah jauh berlainan bersama kebijakan yang diterapkan terhadap orang dewasa. Di di dalam upaya penanggulangan kejahatan harus ditempuh dengan pendekatan kebijakan, di dalam arti: a) Adaintegrasi antara politik kriminil dan politik sosial; b) Ada integrasi antara upaya penggulangan kejahatan bersama penal maupun non penal. Upaya penanggulangan kejahatan melalui jalur "penal" lebih menitikberatkan terhadap sifat "repressive" (penindasan / pemberantasan / penumpasan) sesudah kejahatan terjadi, sedangkan jalur "non-penal" lebih menitikberatkan terhadap sifat "*preventive*" (pencegahan/penangkalan) sebelum saat kejahatan terjadi. Dikatakan sebagai perbedaan secara kasar, dikarenakan tindakan refresif terhadap hakikatnyadapat dilihat sebagai tindakan preventif di dalam arti luas.

Upaya penangulangan kejahatan dapat ditempuh dengan: a) Penerapan hukum pidana (*criminal law application*); b) Pencegahan tanpa pidana (*prevention without punishment*); c) Mempengaruhi pandangan warga mengenai kejahatan dan pemidanaan melalui media massa *(influencing views of society on crime and punishment/mass media*). tehnik pengumpulan data yang dilaksanakan di dalam penelitian ini berasal dari pendalaman dokumen/literatur, baik berbentuk referensi cetak maupun digital, dan juga pengalaman empiris penulis (Sugiyono, 2012), dalam keadaan ini pengalaman penulis disaat bertugas saat mendukung tugas penelitian pasca sarjana Fakultas Hukum Universitas Islam Nusantara. Analisis pengetahuan di dalam penelitian ini dilaksanakan melalui sistem seleksi sampai pembuatan fokus, melaksanakan penyajian data, dan juga melaksanakan penarikan resume kesimpulan (Miles, Huberman, dan Saldana 2013).

C. RESEARCH METHOD / METODE PENELITIAN

1.1. Prosedur penelitian.

Proses penelitian dilakukan secara kualitatif, sehingga sumber data di dalam penelitian ini berasal dari data dokumen (Muhadjir, 2002), yakni berbagai buku -buku yang berasal dari perpustakaan pascasarjana Hukum Universitas Islam Nusantara. Analisis data pada penelitian ini dilakukan lewat proses seleksi dan membuat fokus terhadap data yang diperoleh, melakukan analisis serta penyajian data, hingga melakukan proses penarikan simpulan (Miles, 2013).

1.2. Teknik pengumpulan data.

Teknik pengumpulan data yang dipakai dalam peneltian ini berdasarkan pada studi dokumen atau literatur, baik berupa referensi dari media cetak maupun media digital (Sugiyono, 2012), hingga dari pengalaman penulis selama kuliah, meneliti dan bergabung dengan asosiasi hukum dan Asosiasi Pendidikan Tinggi Informatika dan Komputer (APTIKOM) Universitas Islam Nusantara.

Analisis SWOT; suatu proses bertahap di dalam mengembangkan sebuah strategi, menurut hasil pengukuran internal dan eksternal (Fine, 2009). Metode EFAS dan juga IFAS dipakai untuk pemetaan posisi, tetapi periode strategi memakai metode SFAS (Riyanto, 2017). Analisis SWOT digunakan untuk menganalisis faktor yang berkontribusi , dan juga dirumuskan melalui analisis strategi yang berada di dalam sistem matriks EFAS, IFAS, dan SFAS.

Teori Manajemen Strategi; merupakan urutan keputusan yang digunakan untuk menyusun suatu rumusan dan juga menerapkan strategi di dalam meraih sasaran organisasi (Triton, 2011). Manajemen strategi adalah sistem di dalam pengambilan suatu keputusan yang memiliki ciri-ciri mendasar dan menyeluruh untuk berbagai organisasi (Dess, Lumpkin, dan Eisner, 2013). Manajemen strategi ini terdiri dari seluruh aktivitas terkait rumusan tujuan organisasi, strategi, dan pengembangan rencana, tindakan, dan juga kebijakan (Harvey, 1998). Teori manajemen strategi ini dapat digunakan sebagai analisa untuk menopang pemecahan masalah..

D. CONCLUSION / HASIL DAN PEMBAHASAN

1.1. Secara hukum, baik penipuan secara online maupun konvensional dapat diberi perlakuan serupa dengan delik konvensional yang diatur di dalam Kitab Undang-Undang Hukum Pidana (KUHP). Peraturan mengenai penggunaan teknologi informasi dan komunikasi diatur dalam Undang-Undang (UU) Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE). UU 19 Tahun 2016 merupakan perubahan atas UU Nomor 11 Tahun 2008. Undang-undang Nomor 11 Tahun 2008 berisi tentang aturan informasi dan transaksi elektronik di Indonesia. Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 (UU ITE) disahkan pada tanggal 21 April 2008 dan menjadi cyber law pertama di Indonesia. Dalam Undang-Undang Nomor 21 Tahun 2011 berkenaan tentang Otoritas Jasa Keuangan (UU OJK), wewenang dan tugas OJK adalah mengawasi Lembaga Jasa Keuangan (LJK) di bidang pasar modal, di bidang industri keuangan non bank (seperti : asuransi, dana pensiun, perusahaan pembiyaan, dll) dan mulai tahun 2014 juga dapat mengawasi sektor perbankan (Bank Umum dan Bank Perkreditan Rakyat).

Penanggulangan cybercrime membutuhkan kombinasi kebijakan penal dan non penal secara terencana, terfokus, dan professional. Tahapan kebijakan penal adalah melalui pelaksanaan kriminalisasi terhadap pelanggaran yang termasuk kedalam cybercrime, dan penalisasi telah diatur didalam hukum pidana, pembaruan hukum acara pidana, dan pembaruan hukum . Sedangkan langkah-langah kebijakan nonpenal di Indonesia, yakni melalui aktivitas sebagai berikut (Saragih, 2018).

a) Mempengaruhi pandangan penduduk mengenai kejahatan dan pemidanaan melalui media massa, yaitu bersama dengan langkah mendeskripsikan, menayangkan, meneliti, dan analisa berdasarkan kajian ilmiah mengenai cybercrime di media elektronik oleh pihak-pihak yang kompeten secara proporsional.

b) Pencegahan tanpa pakai pidana, meliputi kerjasama antar negara, kerjasama antar pelaku atau antar praktisi teknologi informasi, menambah pengamanan sistem atau jaringan komputer, mengembangkan kode etik profesi teknologi Info dan sertifikasi teknologi informasi, menambah kebijakan sosial, mengembangkan kesehatan mental masyarakat, perbaikan kesegaran mental secara nasional, peningkatan kesejahteraan sosial dan kesejahteraan anak-anak, dan optimalisasi penerapan hukum.

Operasionalisasi kebijakan hukum penal meliputi kriminalisasi, diskriminalisasi, penalisasi dan depenalisasi. Penegakan hukum pidana tersebut sangat tergantung pada perkembangan politik hukum, politik kriminal, dan politik sosial, oleh karena itu penegakan hukum tidak hanya memperhatikan hukum yang otonom, melainkan memperhatikan juga masalah kemasyarakatan dan ilmu perilaku social (Haryono, 2012).

1.2. Perusahaan atau pihak yang melaksanakan penawaran investasi ilegal hampir semua bukanlah Lembaga Jasa Keuangan (LJK) sehingga Perusahaan atau pihak tersebut tidak tercatat dan diawasi oleh OJK. Dengan demikianlah OJK tidak mampu memastikan faktor legalitas dari perusahaan tersebut. Undang-undang Nomor 9 Tahun 2016 UU tentang Pencegahan dan Penanganan Krisis Sistem Keuangan. Serta Undang-undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan.

1.3. Kementrian Kominfo sosialisasi peningkatan kecakapan literasi digital masyarakat, membuka layanan pengaduan peniapuan digital , kegiatan pemblokiran situs atau nomor yang terindikasi penipuan digital dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik

1.4. PPATK bertugas sesuai Undang- undang Republik Indonesia Nomor 8 tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang memiliki tugas menghambat dan memberantas tindak pidana Pencucian Uang. Dalam lakukan tugasnya, PPATK membawa manfaat sebagai berikut:

1). Pencegahan dan pemberantasan tindak pidana Pencucian Uang;
2). Pengelolaan data dan informasi yang diperoleh PPATK;
3). Pengawasan pada kepatuhan Pihak Pelapor; dan
4). Analisis atau kontrol laporan dan Informasi Transaksi Keuangan yang berindikasi tindak pidana Pencucian Uang dan/atau tindak pidana lain

1.5. Analisis Strategi.- Faktor Eksternal. EFAS (External Factor Analysis Summary).

No.	*KEY EXTERNAL FACTORS*	BOBOT	*RATING*	SKOR
	A. PELUANG (*OPPORTUNITIES*)			
1.	Koordinasi antar negara karena kejahatan penipuan internet merupakan kejahatan transnasional	0.091	6	0.546
2.	**Aktivitas kontinyu *social media influencer* yang mempu mempengaruhi dan mengedukasi *follower* yang banyak dan beragam dalam penanggulangan penipuan melaluiinternet**	**0.117**	**8**	**0.936**
3.	**Kecepatan aduan masyarakat pada saat mengalami kejahatan penipuan internet**	**0.105**	**8**	**0.840**
4.	Perkembangan teknologi informasi dan komunikasi terkini dapat mendukung penanggulangan penipuan online .	0.084	6	0.504
5.	**Keterbukaan pihak *Internet Service Provider* (ISP) di dalamkerja sama hingga mendukung penanggulangan penipuan melalui internet**	**0.103**	**7**	**0.721**
	Jumlah	**0.500**		**3.547**

	B. ANCAMAN (*THREATS*)			
1.	Sulitnya melacak pelaku kejahatan penipuan online dikarenakan wilayah pelaku bisa dimana saja, pelaku biasanya akan menggunakan identitas yang palsu atau juga meminjam identitas orang lain	0.086	3	0.258
2.	**Literasi digital dari netizen masih lemah, sehingga masih banyak yang mudah tertipu penipuan melalui internet;**	**0.149**	**2**	**0.298**
3.	Sikap skeptis, hoaks dan opini negatif dari sebagian publik terhadap kemampuan dan integritas Kominfo dan Polri	0.075	4	0.300
4.	**Kejahatan penyebaran penipuan melalui internet yang merupakan kejahatan transnasional, peningkatan jumlah dan jenis yang semakin massive dan luas, dengan berbagai modus.**	**0.127**	**2**	**0.254**
5.	Media mainstream dan media online masih belum intensif mendukung pelaksanaan penanggulangan penipuan online	0.063	4	0.252
	Jumlah	**0.500**		**1.362**
	Total Skor EFAS	**1.000**		**4.909**

1.6. Faktor Internal.

IFAS (*Internal Factor Analysis Summary*)

Tabel 6.6 **IFAS (*Internal Factor Analysis Summary*)**

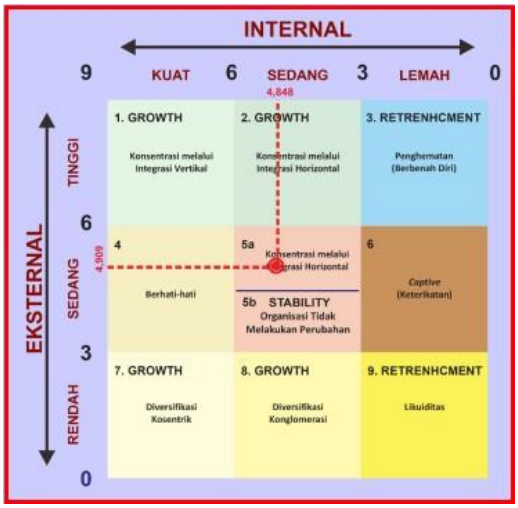
No.	*KEY INTERNAL FACTORS*	BOBOT	*RATING*	SKOR
	A. KEKUATAN (*STRENGTHS*)			
1.	**Dukungan dan komitmen Kemenkominfo, OJK, PPATK dan Polri mencegah dan menanggulangi aksi penipuanmelalui internet**	**0.117**	**8**	**0.936**
2.	Kemenkominfo, OJK, PPATK dan Polri semakin memiliki kemampuan dan pengalaman dalam pengungkapan bersama kasus penipuan melalui internet	0.086	6	0.516
3.	Kekuatan, Dedikasi, dukungan seluruh lapisan masyarakat dalam mangajukan pengaduan, melaporkan dan turut aktif dalam proses pengadilan	0.083	6	0.498
4.	**Kebijakan Kemenkominfo, OJK, PPATK dan Polri terkait dengan upaya deteksi dini, pre-emtif, preventif, represif penipuan melalui internet**	**0.102**	**7**	**0.714**
5.	**Sinergi Kemenkominfo, OJK, PPATK dan Polri dapat digunakan untuk memperkuat kerja sama pengungkapan terintegrasi.**	**0.112**	**8**	**0.896**
	Jumlah	**0.500**		**3.560**

No.	B. KELEMAHAN (*WEAKNESS*)	BOBOT	*RATING*	SKOR
1.	Sulitnya melacak pelaku kejahatan penipuan online dikarenakan wilayah pelaku bisa dimana saja, pelaku biasanya akan menggunakan identitas yang palsu atau juga meminjam identitas orang lain	0.065	4	0.260
2.	**Kompetensi personil Polri, dan Kemenkominfo, yang minim dalam mengikuti kecepatan kemampuan dan pengalaman dibidang ITE atau kejahatan cyber crime**	**0.132**	**2**	**0.264**
3.	Kurangnya kekuatan regulasi dan mekanisme dalam pelacakan pelaku dan pembukaan rekening bank	0.089	3	0.267
4.	**Kurangnya deteksi dini sehingga kasus kejahatan penipuan online baru terbongkar ketika sudah memakan korban dan membawa kerugian material sangat besar**	**0.145**	**2**	**0.290**
5.	Program penanganan dan *reward and punishment* kurang konsisten dalam penanganan penipuan internet	0.069	3	0.207
	Jumlah	**0.500**		**1.288**
	Total Skor IFAS	**1.000**		**4.848**

1.7. Posisi Organisasi.

Setelah melihat hasil perhitungan dengan cara metode IFAS maupun EFAS di atas, maka posisi organisasi OJK, PPATK dan Polri, dalam Penanggulangan penipuan melalui internet di Indonesia guna memastikan keamanan masyarakat, dapat dicermati pada gambar di bawah ini:

Gambar 6.1 Posisi Organisasi



Keterangan:

Diagram di atas memperlihatkan bahwa total skor IFAS ialah 4,848 serta total skor EFAS ialah 4,909, maka posisi berada pada kuadran 5a (Konsentrasi melalui Integrasi Horizontal), berarti memiliki kondisi yang sedang-sedang, yang mana peluang (eksternal) maupun kekuatan (internal) bersifat sedang. Respons untuk menghadapi kondisi ini (Horizontal Integration Strategy) adalah meningkatkan (*generic strategy*) koordinasi (*grand strategy*) mendukung Penanggulangan penipuan melalui internet di Indonesia guna meningkatkan keamanan siber pada Era Revolusi Industri 4.0masyarakat secara terpadu supaya mampu memberikan rasa keadilan. Kata kunci: koordinasi.

Melihat kondisi di atas, sehingga posisi tersebut dimaknai ke dalam bahasa operasional, yang mana menjadi kata kerja awal di dalam judul, yaitu “Optimalisasi”. Kemudian, mekanisme pemecahan masalah akan memakai pendekatan implementasi strategi (t*ranslation process*) secara sistematis.

1.8. Faktor Strategis.

SFAS (Strategic Factor Analysis Summary).

Tabel SFAS (Strategic Factor Analysis Summary)

No.	FAKTOR STRATEGIK KUNCI	BOBOT	PERINGKAT	SKOR	JANGKA		
					PENDEK	SEDANG	PANJANG
1.	**Aktivitas kontinyu *social media influencer* yang mampu mempengaruhi dan mengedukasi *follower* yang banyak dan beragam dalam penanggulangan penipuan melalui internet**	0.133	8	1.064			
2.	**Kejahatan penyebaran penipuan melalui internet yang merupakan kejahatan transnasional, peningkatanjumlah dan jenis yang semakin massive dan luas, denganberbagai modus.**	0.091	7	0.637			
3.	**Penguatan kerja sama Keterbukaan pihak *Internet Service Provider* (ISP) di dalam kerja sama hingga mendukung penanggulangan penipuan melalui internet**	0.123	8	0.984			
4.	**Peningkatan Kompetensi personil Kemenkominfo dan Polri dalam mengikuti kecepatan kemampuan dan pengalaman dibidang ITE atau kejahatan cyber crime**	0.071	2	0.142			
5.	**Penguatan Kebijakan Kemenkominfo, OJK, PPATK dan Polri terkait dengan upaya deteksi dini, pre-emtif, preventif, represif penipuan melalui internet**	0.079	2	0.158			
6.	**Dukungan dan komitmen Kemenkominfo, OJK, PPATK dan Polri mencegah dan menanggulangi aksi penipuan melalui internet**	0.132	8	1.056			
7.	**Penguatan Sinergi Kemenkominfo, OJK, PPATK dan Polri dapat digunakan untuk memperkuat kerja sama pengungkapan terintegrasi.**	0.119	8	0.952			
8.	**Penguatan Literasi digital dari netizen agar tidak mudah tertipu penipuan online.**	0.070	7	0.490			
9.	**Respon yang cepat atas kecepatan aduan masyarakat pada saat mengalami kejahatan penipuan internet**	0.084	2	0.168			
10.	**Penguatan deteksi dini agar kasus kejahatan penipuan online dapat terbongkar sebelum memakan korban dan membawa kerugian material sangat besar**	0.099	2	0.198			

a). Memaksimalkan upaya pengendalian pendahuluan (feedforward control) guna meningkatkan keamanan siber pada era revolusi industri 4.0 di Indonesia guna meningkatkan keamanan siberpada Era Revolusi Industri 4.0 sesuai UU RI No. 2/2002 tentang Polri, UU RI No. 19/2016 tentang ITE,

b). Memaksimalkan upaya pengendalian berjalan (concurrent control) guna meningkatkan keamanan siber pada era revolusi industri 4.0 UU RI No. 2/2002 tentang Polri,

c). Memaksimalkan upaya pengendalian umpan balik (feedback control) guna meningkatkan keamanan siber pada era revolusi industri 4.0 di Indonesia secara efektif serta mengacu pada KUHP, khususnya pasal 378 KUHP dan Pasal 28 ayat (1) Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, KUHAP, UU RI No. 2/2002 tentang Polri.

1.9. Strategi - Jangka Pendek

a). Optimalisasi strategi OJK Preventif dalam melakukan sosialisasi dan edukasi kepada masyarakat mengenai karakteristik kegiatan penghimpunan dana dan pengelolaan investasi ilegal berbagi pengetahuan dengan penegak hukum dan regulator di daerah Represif.

b). Membantu melakukan upaya koordinatif antar instansi terkait untuk mempercepat proses penanganan melalui kerangka kerjasama Satuan Tugas Penanganan Dugaan Tindakan Melawan Hukum di Bidang Penghimpunan Dana dan Pengelolaan Investasi atau yang lebih dikenal dengan Satgas Waspada Investasi.

Kasus-kasus dan pengaduan masyarakat terkait investasi ilegal yang dilaporkan ke OJK akan dikoordinasikan dengan Satgas Waspada Investasi untuk penanganannya.

c). Dalam melaksanakan fungsi pencegahan dan pemberantasan tindak pidana Pencucian Uang, PPATK berwenang:meminta dan mendapatkan data dan informasi dari instansi pemerintah dan/atau lembaga swasta yang memiliki kewenangan mengelola data dan informasi, termasuk dari instansi pemerintah dan/atau lembaga swasta yang menerima laporan dari profesi tertentu;

d). Menetapkan pedoman identifikasi Transaksi Keuangan Mencurigakan; mengoordinasikan upaya pencegahan tindak pidana Pencucian Uang dengan instansi terkait;memberikan rekomendasi kepada pemerintah mengenai upaya pencegahan tindak pidana Pencucian Uang;mewakili pemerintah Republik Indonesia dalam organisasi dan forum internasional yang berkaitan dengan pencegahan dan pemberantasan tindak pidana Pencucian Uang;

menyelenggarakan program pendidikan dan pelatihan antipencucian uang; dan menyelenggarakan sosialisasi pencegahan dan pemberantasan tindak pidana Pencucian Uang.

e). Kebijakan blokir situs atau akun yang terdeteksi melakukan penipuan melalui internet

f). Kebijakan perusahaan, organisasi atau personil untuk diumumkan terlarang oleh OJK jika melakukan kegiatan investasi atau jasa keuangan tanpa ijin/ ilegal

g). Kebijakan deteksi dan blokir aliran keuangan organisasi atau para pelaku penipuan melalui internet

h). Hukuman yang berat dan penyitaan aset oleh aparat penegak hukum untuk menimbulkan afek jera pelaku dan kemungkinan pengembalian hasil kejahatan kepada korban.

i). Pengejawantahan Kebijakan Polri terkait dengan Kamtibmas, upaya deteksi dini, pre-emtif, preventif, represif penipuan melalui internet;

j). Optimalisasi Kekuatan birokrasi dan aparat sampai tingkat desa untuk komunikasi dengan seluruh warga kelurahan/desa;

k). Optimalisasi Eksistensi social media influencer dengan follower yang banyak dan beragam bisa dipakai popularitasnya melalui penanggulangan penipuan melalui internet;

l). Penguatan Literasi digital dari netizen, sehingga netizen tidak mudah tertipu penipuan melaluiinternet;

m). Penguatan kerja sama Keterbukaan pihak Internet Service Provider (ISP) di dalam kerja sama hingga mendukung penanggulangan penipuan melalui internet

n). Peningkatan Kompetensi personil Polri, dan Kemenkominfo dalam mengikuti kecepatan kemampuan dan pengalaman dibidang ITE atau kejahatan cyber crime

o). Penguatan Kebijakan Kemenkominfo, OJK, PPATK dan Polri terkait dengan upaya deteksidini, pre-emtif, preventif, represif penipuan melalui internet

p). Penguatan Sinergi Kemenkominfo, OJK, PPATK dan Polri dapat digunakan untuk memperkuatkerja sama pengungkapan terintegrasi.

q). Respon yang cepat atas kecepatan aduan masyarakat pada saat mengalami kejahatan penipuaninternet

n). Penguatan deteksi dini agar kasus kejahatan penipuan online dapat terbongkar sebelum memakan korban dan membawa kerugian material sangat besar

r). peningkatan kecepatan respon aduan masyarakat agar korban tidak terus bertambah dankerugian tidak terus menumpuk

s). Peningkatan deteksi dini terhadap lembaga jasa keuangan dan investasi tidak berijin dan mengumumkannya ke masyarakat.

1.10. Strategi-Jangka Menengah.

a). Peningkatkan Eksistensi *social media influencer* dengan *follower* yang banyak dan beragambisa dipakai popularitasnya melalui penanggulangan penipuan melalui internet;

b). Penguatan dukungan pendanaan untuk pelatihan kompetensi TIK dan Sarana prasarana terkini Kemenkominfo, OJK, PPATK dan Polri;

1.11 Strategi- Jangka Panjang

a) Peningkatan dukungan penggiat media sosial, komunitas media sosial komunitas literasi digital, dan masyarakat;

b). Penangkalan Penipuan melalui internet yang semakin meningkat serta masif dengan berbagai modus;

E. SUMMARY / KESIMPULAN DAN SARAN

1.1. Saran

Jika melihat dari upaya pengendalian pendahuluan (*feedforward control*) guna meningkatkan keamanan masyarakat dengan tindakan deteksi dini, preemtif dan preventif belum optimal. Untuk mengoptimalkan hal tersebut, maka perlu adanya upaya strategis Kominfo, OJK, PPATK, Polri dan Kejaksaan dengan terintegrasi. Upaya ini penting mangingat kejahatan siber khususnya penipuan online merupakan kejahatan multi dimensi yang termasuk di dalamnya kejahatan ekonomi. Kejahatan ini meimbulkan dampak luas karena biasanya melibatkan jaringan dan korban masyarakat yang sangat besar dan luas. Kejahatan siber termasuk kejahatan penipuan daring juga terjadi lintas negara transnasional. Kejahatan ini terus berkembang kuantitas, kualitas, jenis dan modusnya. Metode seperti sosialisasi, diseminasi, komunikasi, gabungan kegiatan, pembentukan dan pembinaan jaringan intelijen, patroli siber, pelatihan, pengawasan, simulasi, kajian, dan lainnya secara rutin. Penanggulangan penipuan online sesuai dengan UU RI No. 19/2016 tentang Informasi dan Transaksi Elektronik . Penipuan melalui internet juga melanggar pasal 378 KUHP.

Sehingga, optimalnya pelaksanaan upaya penguatan fungsi deteksi dini, upaya pre-emtif, dan upaya preventif, akan mampu menanggulangi kejahatan siber khususnya penanggulangan penipuan melalui internet.

Jika melihat dari pengendalian berjalan (*concurrent control)* guna meningkatkan keamanan siber pada era revolusi industri 4.0 dalam memelihara stabilitas Kamtibmas masih belum optimal. Untuk mengoptimalkan maka perlu dilakukan upaya taktis Transformasi Polri Presisi dengan Pemolisiam Masyarakat serta community policing. Metode komunikasi, kolaborasi dan koordinasi serta sinergi polisionil dan lintas sektor dengan upaya pre-emtif dan preventif. Kerja sama formal maupun informasl khususnya dengan pemerintah Provinsi Sumatera Selatan dan Pemerintah Kota Palembang, Diskominfo, media elektronik serta media sosial, lembaga dan kelompok penggiat internet anti kejahatan siber. Metode diskusi, raker, seminar, kerja sama formal dan informal dan lainnya, sehingga pelaksanaan kerja sama semakin solid dan terpadu dalam penanggulangan kejahatan siber khususnya penipuan daring.

Jika melihat dari pengendalian umpan balik (feedback control) guna meningkatkan keamanan siber pada era revolusi industri 4.0 dalam memelihara stabilitas Kamtibmas pada Polrestabes Palembang masih belum optimal. Untuk mengoptimalkan hal tersebut, maka perlu dilakukan upaya strategis, seperti upaya preventif dan penegakan hukum dengan Transformasi Polri Presisi. Pengawasan dan pengendalian serta sistem manajemen kinerja penanggulangan kejahatan siber termasuk Penipuan daring melalui pembinaan, mentoring, perancangan sistem manajemen, pelatihan peningkatan pelayanan dalam pengaduan masyarakat sampai pemanfaatan teknologi informasi dengan Surat Pemberitahuan Dimulainya Penyidikan (SPDP) daring dan Surat Pemberitahuan Perkembangan Hasil Penyidikan (SP2HP) daring serta lainnya. sehingga proses manajemen efektif dalam penanggulangan kejahatan siber termasuk penipuan daring.

1.2. Rekomendasi.

1 Merekomendasikan kepada OJK, kemenkominfo dan Polri agar ada patroli siber gabungan untuk deteksi dini kejahatan siber dibidang ekonomi salah satunya penipuan online. Hal ini untuk mencegah dari awal indikasi penipuan daring sehingga dampaknya dapat dicegah dari awal.

2. Merekomendasikan kepada OJK, kemenkominfo dan Polri , serta pembina fungsi terkait lainnya agar dapat melaksanakan pelatihan berkala berbasis kompetensi bagi seluruh stafnya. Pelatihan profesional ini khususnya arah pengembangan kompetensi Teknologi dan komunikasi terkini untuk penanggulangan kejahatan siber termasuk penipuan melalui internet.

3 Merekomendasikan kepada OJK, kemenkominfo, PPATK dan Polri, serta pembina fungsi terkait lainnya agar dapat mengembangkan kerja sama, bersama media sosial dan media elektronik serta kelompok masyarakat penggiat anti kejahatan siber / internet sehat dan aman. Penerapan sistem pengukuran kepuasan masyarakat akan penanganan tindak pidana kejahatan siber termasuk penipuan melalui internet.

4. Merekomendasikan kepada OJK, kemenkominfo, PPATK dan Polri, serta pembinafungsi terkait lainnya untuk peningkatan kapasitas sumber daya untuk menghadapikecepatan perkembangan kejahatan siber termasuk penipuan melalui internet.

5. Merekomendasikan kepada, OJK, kemenkominfo, PPATK dan Polri, serta pembina fungsi pengawasan dan pembina fungsi terkait terkait lainnya untuk memberi waktu bagi pemaparan kepala lembaga Meminta ijin untuk pendukungan penuh terhadap program kerja dan menjadikannya sebagai sistem penilaian kerja dalam menanggulangi kejahatan siber termasuk penipuan melalui internet. Merekomendasikan sistem pengawasan dan pengendalian kinerja penanganan kejahatan siber terhadap seluruh personil.

REFERENCE / DAFTAR PUSTAKA [Times New Roman, 12 bold, space 1.5]

Adami Chazawi, Tindak Pidana Informasi & Transaksi Elektronik, Bayumedia Publishing, 2011.Abdul Wahid, Kejahatan Mayantara, PT Refika Aditama, Bandung, 2005.
Soerjono Soekanto, Pengantar Penelitian Hukum, UII Press, Jakarta, 1982.

Sutrisno Hadi, Metodologi ReseacrhJilid 1, Andi Offset, Yogyakarta,1989. Burhan Ashshofa, Metode PenelitianHukum, Rineka Cipata, Jakarta, 2004. J.E.Sahetap

y, Kapita Selekta Kriminologi, PT. Citra Adtya Bakti, Bandung, 1979