CYBER MONEY LAUNDERING
(Salah satu bentuk *White Collar Crime* abad 21)

Oleh : Iskandar Wibawa
iskandar.wibawa@yahoo.com

Abstrak

Pencucian uang ("meney laundering") adalah perbuatan menyembunyikan asal usul dana yang tidak sah karena diperoleh dari suatu tindak pidana menjadi seolah sah, merupakan suatu tindak pidana sejak di undangkan Undang Undang Nomor 15 tahun 2002 jo Undang Undang Nomor 25 tahun 2003, yang kemudian diperbaharui dengan Undang Undang Nomor 8 tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Tahapan pencucian uang yang terdiri atas konversi ("placement"), pelapisan ("layering"), dan pengintegrasian ("integration") pada perkembangannya dilakukan dengan memanfaatkan dunia maya ("cyber"), sehingga merupakan "cyber crime", yang penanganannya menjadi semakin sulit dan kompleks, karena kejahatan ini bisa merupakan kejahatan lintas Negara, padahal aparat penegak hukum dalam melaksanakan kewenanagannya dibatasi yurisdiksi.Disamping itu juga dibutuhkan kompetensi dan keahlian khusus di bidang "cyber"."Cyber money laundering" merupakan keniscayaan yang harus dihadapi sebagai salah satu bentuk "white collar crime" pada era abad ke 21, sehinnga upaya untuk pencegahan dan pemberantasan tindak pidana pencucian uang dapat diaksakan secara optimal.

Kata kunci: *meney laundering, white collar crime, cyber crime, cyber money laundering.*

A. Pendahuluan.

Perbankan sebagai salah satu lembaga keuangan yang mempunyai fungsi mengumpulkan dan menyalurkan dana masyarakat semakin mendapatkan posisi penting di tengah masyarakat untuk memajukan perekonomian rakyat, yang secara langsung maupun tidak langsung turut menciptakan stabilitas nasional terutama di bkidang ekonomi.

Perbankan sebagai pengumpul dan penyalur dana masyarakat ada kemungkinan digunakan oleh sebagaian pengguna jasa bank untuk menyimpan dan menyalurkan dana yang tidak sah/tidak halal karena diperoleh dari tindak pidana

misalkan hasil korupsi dan penjualan obat terlarang, yang guna menyembunyikan asal usul dana supaya tidak dapat dilacak oleh Aparat Penegak Hukum dilakukan langkah langkah tertentu, yang sering disebut pencucian uang (*"money laundering")*.

Abad 21 saat ini yang dikenal dengan era teknologi dan informasi, perilaku "pencucian uang" semakin rumit dan sulit dilacak,karena pelaku memanfaatkan *"dunia cyber"* yang untuk melakukan transfer dana tidak lagi harus datang ke bank, namun cukup memanfaatkan fasilitas *e-banking* dan sarana *cyber* lainnya. Berkenaan dengan hal tersebut,tulisan ini mencoba memaparkan tindakan pencucian uang (*"money laundering")* melalui dunia cyber, yakni *"Cyber Money Laundering"*.

B. *Money Laundering.*

Pencucian uang (*"money laundering")* adalah upaya untuk menyembunyikan asal usul dana yang diperoleh dari tindak pidana (kejahatan) melalui berbagai transaksi,biasanya melalui Perbankan, dengan tujuan agar aparat penegak hukum sulit menelusuri harta tersebut,sehingga terkesan dana tersebut merupakan dana yang "legal".

Viena Convention On Narcotic Drug ,Council of Europa Convention on Launderingdan OAS Model Regulations menyatakan ada 3 jenis tindak pidana pencucian uang *("money laudering")* yaitu :

1. Mengubah atau memindahkan *"property"* yang diketahui berasal dari kejahatan, dengan tujuan menyembunyikan asal usul gelap *"property"* tersebut atau untuk membantu seseorang menghindari akibat-akibat hukum dari keterlibatannya dalam melakukan kejahatan;
2. Menyembunyikan keadaan sebenarnya dari *"property"* yang berasal dari kejahatan itu, baik dari sumbernya ,asal-usul, lokasi, penempatan, pembagian, pergerakan/penyaluran, maupun hak-hak yang berhubungan dengan *"property"* tersebut;
3. Menguasai,menerima,memiliki,menggunakan "property" yang diketahui berasal dari kejahatanatau dalam keikut sertaanya dalam melakukan kejahatan. (Barda Nawawi Arief, 2002: 185).

Proses pencucian uang (*"money laundering"*) dilakukan melalui 3 tahap,yakni :

1. Tahap "*placement*" yaitu konversi dari uang tunai hasil kejahatan dalam berbagai bentuk surat berharga seperti saham atau deposito, juga penukaran dan transfer ke valuta asing atau penanaman investasi pada real estate dan lain sebagainya.
2. Tahap "*layering*" yaitu tahapan "pelapisan" dengan melakukan transaksi yang sangat kompleks dan rumit,sehingga akan menyebabkan pelacakan uang menjadi sulit.
3. *Tahap "integration"*yaitu tahapan mengintegrasikan uang hasil kejahatan dengan uang halal menjadi satu kesatuan, yang antara lain untuk pembangunan *"real estate"*, sehingga bisnis tersebut seolah menjadi "legal".

Anwar Nasution, seorang pakar ekonomi nasional menyatakan bahkwa "*money laundering"*dilakukan melalui 3 tahapan,yaitu :

1) tahap *"immersion"* yakni tahap "membenamkan" uang haram tersebut melalui rekening koran, wesel pos, deposito dan langkah lain yang sah,sehingga sulit dilacak asal usulnya oleh aparat penegak hukum;
2) tahap "pensabunan/pencucian" atau "*laundering"*, dengan mengacak dan mencampur uang haram tersebut dengan uang halal; serta
3) tahap "*pengeringan"*,atau "*repatriasi"* atau *"integrasi"*,yakni uang yang telah dicuci tersebut dikembalikan dalam bentuk yang menurut aturan hukum merupakan "uang legal" (Nyoman Serikat Putra Jaya,2001: 102).

"*Money laundering*" sebenarnya merupakan kelanjutan dari tindak pidana yang pernah dilakukan sebelumnya, antara lain tindak pidana korupsi, tindak pidana yang berkaitan dengan perbankan, tindak pidana yang berkaitan dengan narkotika, penyalah gunaan psikotropika, tindak pidana ekonomi dan hasil kejahatan lainnya, sehingga sebenarnya dapat diterapkan peraturan perundangan yang mengatur tentang tindak pidana tersebut.

Indonesia telah melarang *"money laundering"* melalui Undang-Undang Nomor 15 tahun 2002 tentang Tindak Pidana Pencucian Uang. Sebagaimana telah diubah dengan Undang-

Undang Nomor 25 tahun 2003 tentang Perubahan atas Undang-Undang Nomor 15 tahun 2002 tentang Tindak Pidana Pencucian Uang, dan terakhir diamandemen dengan Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.

Undang-Undang Nomor 15tahun 2002 tentang Tindak Pidana Pencucian Uang sebagaaimana diubah dengan Undang-Undang Nomor 25 tahun 2003 tentang Perubahan atas Undang-Undang Nomor 15 tahun 2002 tentang Tindak Pidana Pencucian Uang menyatakan bahwa yang dimaksud dengan pencucian uang adalah perbuatan menempatkan, mentransfer, membayarkan, menghibahkan, menyumbangkan, dan menitipkan, membawa keluar negeri, menukarkan atau perbuatan lainnya atas harta kekayaanm yang diketahui atau patut diduga merupakan hasil tindak pidana dengan maksud untuk menyembunyikan atau menyamarkan asal usul harta kekayaan sehingga seolah-olah menjadi harta kekayaan yang sah. Pengertian pencucian uang menurut Undang-Undang Nomor 8 tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang terdapat pada Pasal 1 ayat 1 yang menyatakan bahwa pencucian uang adalah segala perbuatan yang memenuhi unsur tindak pidana sesuai dengan ketentuan undang-undang ini. Adapun yang dimaksud dengan hasil tindak pidana pencucian uang adalah harta kekayaan yang diperoleh dari tindak pidana korupsi, penyuapan, narkotika, psikotropika, penyelundupan tenaga kerja, penyelundupan migran, di bidang perbankan, di bidang pasar modal, di bidang perasuransian, kepabeanan, cukai, perdagangan orang, perdagangan senjata gelap, terorisme, penculikan, pencurian, penggelapan, penipuan, perjudian, prostitusi, di bidang perpajakan, di bidang kehutanan, di bidang kelautan dan perikanan, serta tindak pidana lain yang ancaman pidananya 4 (empat) tahun atau lebih. Ketentuan tersebut senada dengan yang diatur dalam RUU KUHP tahun 2015 pada Penjelasan Pasal 747, yang menyatakan bahwa yang dimaksud dengan hasil tindak pidana pencucian uang adalah harta kekayaan yang diperoleh dari tindak pidana : korupsi, penyuapan, penyelundupan barang, penyelundupan tenaga kerja, penyelundupan imigran, bidang perbankan, bidang pasar modal, bidang asuransi, narkotika, psikotropika, perdagangan

manusia, perdagangan senjata gelap, penculikan, terorisme, pencurian, penggelapan, penipuan, pemalsuan uang, perjudian, prostitusi, bidang perpajakan, bidang kehutanan, bidang lingkungan hidup, bidang kelautan dan tindak pidana lain yang diancam pidana penjara 4 tahun atau lebih, yang dilakukan di wilayah Negara Kesatuan Republik Indonesia dan tindak pidana tersebut juga merupakan tindak pidana menurut hukum Indonesia. Pasal 747 merumuskan tentang delik pencucian uang *("money laundering")* sebagai berikut : " Setiap orang yang menempatkan, mentransfer, mengalihkan, membelanjakan, membayarkan, menghibahkan, menitipkan, membawa ke luar negeri, mengubah bentuk, menukarkan dengan mata uang atau surat berharga atau perbuatan lain atas harta kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana pencucian uang dengan tujuan menyembunyikan atau menyamarkan asal usul harta kekayaan dipidana karena tindak pidana pencucian uang dengan pidana penjara paling lama 20 (dua puluh) tahun dan denda paling banyak Katagori V. Rumusan delik pada pasal ini secara jelas menyatakan bahwa substansi pencucian uang adalah menyembunyikan atau menyamarkan asal usul harta kekayaan. Delik pencucian uang *("money laundering")* juga dirumuskan pada Pasal 748 dan 749 sebagai berikut :

Pasal 748 : "Setiap orang yang menyembunyikan atau menyamarkan asal usul sumber , lokasi, peruntukan, pengalihan hak-hak, atau kepemilikan yang sebenarnya atas harta kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana pencucian uang dipidana karena tindak pidana pencucian uang dengan pidana penjara paling lama 20 (dua puluh) tahun dan denda paling banyak Katagori V". Substansi pencucian uang pada pasal ini adalah menyembunyikan dan menyamarkan asal usul , sumber dan lokasi harta kekayaan".

Pasal 749 :

(1) Setiap orang yang menerima atau menguasai penempatan, pentransferan, pembayaran, hibah, sumbangan, penitipan, penukaran, atau menggunakan harta kekayaan yang diketahui atau patut diduganya merupakan hasil tindak pidana pencucian uang dipidana dengan pidana penjara

paling lama 5 (lima) tahun dan denda paling banyak Katagori IV.

(2) Ketenuan sebagaimana diatur pada ayat (1) tidak berlaku bagi pihak pelapor yang melaksanakan kewajiban pelaporan. Pasal ini mengancam orang yang menerima uang hasil pencucian uang, sedangkan 2 (dua) pasal sebelumnya mengancam orang yang melakukan pencucian uang.

Ketentuan Pasal 747, 748 dan 749 ini tidak berbeda dengan rumusan pasal yang terdapat pada Undang-Undang Nomor 8 tahun 2010 tentang Pencegahan dan Pemberantasan tindak Pidana Pencucian Uang Pasal 3, d dan 5, hanya ancaman pidana dendanya yang dinominalkan dalam rupiah, yakni pidana denda Katagori V dirumuskan dengan denda paling banyak Rp. 10.000.000.000,00 (sepuluh milyar) rupiah, sedangkan denda Katagori IV dinominalkan menjadi denda paling banayak Rp. 1.000.000.000,00 (satu milyar) rupiah.

C. Cyber *Crime*

Cyber crime merupakan salah satu dimensi baru kejahatan abad 21 yang mendapatkan banyak perhatian dari masyarakat dunia, dan merupakan salah satu sisi gelap kemajuan teknologi informasi yang mempunyai dampak negatif bagi segala aspek kehidupan modern saat ini. *Cyber Crime* dapat diartikan sebagai kejahatan di dunia maya,atau menurut Barda Nawawi Arief disebut sebagai "kejahatan mayantara". *Cyber Crime* merupakan salah satu bentuk *"White Collar Crime"*, karena para pelaku kejahatan model ini dalam melakukan aktivitasnya memerlukan "kompetensi khusus" yang merupakan ciri utama pelaku *White Collar Crime.* Kompetensi khusus tersebut adalah keahlian pelaku mengoperasikan dan menguasai dunia c*yber* (mayantara). Kongres PBB X/2000 melakukan pembagian *Cyber Crime* menjadi 2 katagori,yakni (1) *Cyber Crime* dalam arti sempit (*"in a narrow sense")*dan *Cyber Crim*e dalam arti luas (*"in a broader sense")* atau "*Computer Related Crime").* (Barda Nawawi Arief,2002: 258).

Cyber Crime dalam arti sempit adalah kejahatan terhadap sistem/jaringan komputer (*"against a computer system or network");*sedangkan *Cyber Crime* dalam arti luas atau

"*Computer Related Crime" (CRC)* adalah kejahatan dengan menggunakan sarana dari sistem/jaringan komputer ("*by means of computer system or network")* dan kejahatan di dalam sistem komputer ("*in a computer system or network").*

"Computer Related Crime" (CRC") menurut laporan Kongres PBB yang dituangkan dalam dokumen A/CONF.187/15), sebagaimana dinyatakan oleh Barda Nawawi Arief mencakup keseluruhan bentuk-bentuk baru dari kejahatan yang ditujukan pada komputer, jaringan komputer dan penggunaanya, dan bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan peralatan komputer.

Perbuatan jahat yang dilakukan di lingkungan elektronik ini cukup sulit penanggulangannya, karena untuk menanganinya diperlukan keahlian khusus, prosedur investigasi serta kekuatan dasar hukum yang kemungkinan besar belum dipunyai oleh aparat penagak hukum. Kesulitan lain adalah "*cyber crime*" melampaui batas-batas negara (lintas negara) , sedangkan selama ini aparat penegak hukum dalam melaksanakan tugas dibatasi oleh wilayah territorial/jurisdiksi tertentu.

Masaki Harmano dalam tulisannya "*Comparative Study in the Approach to jurisdiction in Cyberspace",* menguraikan tentang adanya jurisdiksi berdasar prinsip-prinsip tradisional, yang terdiri atas 3 (tiga) jurisdiksi, yaitu jurisdiksi legislatif (*lkegislative jurisdiction"),* jurisdiksi judicial ("*judicial jurisdiction"),* dan jurisdiksi eksekutif (*excecutive jurisdiction").* (Barda Nawawi Arief, 2002:276). Pengertian jurisdiksi tradisional menurut Masaki Harmano dapat dimaknai berkaitan dengan batas-batas kewenanagan Negara dibidang penagakan hukum *("law enforcement"),* yaitu :

(1) kewenangan negra untuk membuat/merumuskan hukum substantief, yang juga dinamakan kewenangan pembuatan undang-undang atau kebijakan formulatif yang dipunyai oleh badan legislative, sehingga juga dinamakan kebijakan legislatif. Ini merupakan jurisdiksi formulatif atau jurisdiksi legislatif.
(2) kewenangan negara untuk mengadili atau menerapkan hukum, yang dilakukan oleh lembaga peradilan, oleh

karena itu dinamakan kebijakan yudikatif atau kebijakan aplikatif, ini merupakan jurisdiksi yudikatif;

(3) kewenangan negara untuk melaksanakan dan memaksakan berlakunya hukum serta mengeksekusi putusan pengadilan, sehingga disebut dengan kebijakan eksekutif. Ini merupakan jurisdiksi eksekutif.

Jurisdiksi tradisional, yang terdiri atas jurisdiksi formulatif/legislatif, jurisdiksi aplikatif/judikatif dan jurisdiksi eksekutif tersebut mempunyai batas-batas keberlakuan tertentu, yakni dibatasi oleh wilyah territorial negara, sehingga sering dipermasalahkan sehubungan dengan aktivias tidak terbatas di ruang "*cyber*". Sehubungan dengan hal tersebut Masaki Harmano membedakan pengertian "*cyber-jurisdiction*"dari sudut pandang "dunia maya /*cyber*" dengan dari sudut hukum."*Cyber-jurisdiction*" diartikan sebagai kekuasaan sistem operator dan para pengguna "dunia maya" untuk menetapkan aturan dan melaksanakannya pada suatu masyarakat di ruang maya/dunia virtual/*cyber.* Disini berlaku aturan yang dibuat dari mereka, oleh mereka dan untuk mereka. Mereka mempunyai hukum sendiri yang harus dipatuhi sebagai hukum yang hidup (*the living law").* Dari sisi hukum *"cyber-jurisdiction"* dimaknai sebagai kekuasaan pemerintah secara fisik dan kewenangan pengadilan terhadap pengguna internet atau terhadap aktivitas para pengguna di ruang virtual (*"physical government's power and court's authority over Netusers or their activity in cyber-space").*

David R. Johnson dan David G. Post mengemukakan 4 (empat) model tentang kewenangan di dunia maya/virtual (*"cyber-jurisdiction")* , yaitu :

(1) pelaksanaan control dilakukan oleh badan-badan pengadilan yang saat ini ada. (*"the exiting judicial forums");*
(2) penguasa nasional membuat kesepakatan internasional menegenai *"the governance of Cyberspace";*
(3) pembentukan suatu organisasi internasional baru (*"A New InternastionalOrganization"*); dan
(4) pengaturan sendiri oleh para pengguna internet (*"self governance")'*

Barda Nawawi Arief sependapat dengan Masako Harmano, bahwa jurisdiksi traditional memang mempunyai keterbatasan karena tidak mudah menjangkau pelaku tindak

pidana di ruang virtual/maya yang tanpa batas, namun tidak berarti aktivitas di ruang *"cyber"* dibiarkan tanpa hukum. Ruang *"cyber"* sesungguhnya merupakan perluasan dari lingkungan (*"environment")* dan lingkungan hidup (*"live environment")* yang perlu dipelihara dan dijaga kualitasnya. Oleh karena itu pencemaran dan perusakan informasi di dunia maya/virtual/mayantara dapat dicegah dan ditanggulangi. Oleh karena itu jurisdiksi legislative (*jurisdiction to prescribe")* tetap dapat dan harus difungsikan untuk penanggulangan *"cyber crime"* yang merupakan dimensi baru dari *"environmental crime*".(Barda Nawawi Arief, 2002: 279).

Permasalahan yang timbul berkaitan dengan hubungan antara negara dalam kebijakan /jurisdiksi legislative ini adalah bahwa kewenangan suatu negara dibidang jurisdiksi legislative ini bisa berbeda dan bahkan saling berbenturan dengan kewenangan negara lain. Sangat mungkin terjadi suatu negara merumuskan dalam kebijakan legislatifnya suatu perbuatan merupakan tindak pidana, sedangkan di negara lain dalam kebijakan legislatifnya bukan merupakan tindak pidana. Hal ini berpotensi menimbulkan masalah dalam penerapannya, terlebih apabila pelakunya berada di suatu negara yang tidak mengkriminalisasikan perbuatan tersebut, yang aktivitasnya dilakukan di dunia maya/virtual/cyber/mayantara.

Problem menjadi semakin tajam pada jurisdiksi judikatif / ajudikasi (*"jurisdiction to adjudicate"* dan jurisdiksi ekesekutif (*"jurisdiction to enforce")* karena sangat terkait dengan kedaulatan wilayah dan kedaulatan hukum masing-masing negara. Harmonisasi antar negara perlu dilakukan berupa kesepakatan dan kerjasama antara negara, supaya jurisdiksi yudikatif maupun jurisdiksi eksekutif dapat dilakukan kesefahaman.

Barda Nawawi Arief berpandangan bahwa dalam menghadapi kejahatan tanpa batas wilayah berupa "*Cyber Crime"* seyogyanya digunakan asas universal, atau prinsip *"ubikuitas"* (*"the principle of ubiquity")*, yakni prinsip yang menyatakan bahwa delik-delik yang dilakukan/terjadi sebagian di wilayah/terirorial negara dan sebagian di luar territorial suatu negara, harus dapat dibawa ke dalam jurisdiksi setiap negara yang terkait.

RUU KUHP tahun 2015 mengatur tentang jurisdiksi yang berkaitan dengan *"cyber crime"* pada Pasal 4, yakni dimasukkan sebagai bagian dari "asas territorial", sebagaimana dirumuskan sebagai berikut :

Ketentuan pidana dalam peraturan perundang-undangan Indonesiaberlaku bagi setiap orang yang melakukan :

a. Tindak pidana di wilayah Republik Indonesia;
b. Tindak pidana di dalam kapal atau pesawat udara Indonesia; atau
c. Tindak pidana di bidang teknologi informasi atau tindak pidana lainnya yang akibatnya dirasakan atau terjadi di wilayah Indonesia atau dalam kapal atau pesawat udara Indonesia.

Pada penjelasan Pasal 4 dinyatakan sebagai berikut :

Huruf a : Ketentuan ini mengandung asas wilayah atau territorial.

Huruf b : Ketentuan ini mengandung asas territorial yang diperluas. Perluasan asas territorial tidak hanya dimaksudkan untuk menjaring tindak pidana dalam kapal atau pesawat udara Indonesia, tetapi juga untuk menjaring tindak pidana di dunia maya (*"cyber crime")* yang dilakukan di luar wilayah Indonesia tetapi akibatnya dirasakan atau terjadi di Indonesia. Asas ini berlaku bagi siapa saja, tanpa melihat kewarganegaraan pembuat.

Huruf c : Yang dimaksud dengan tindak pidana lainnya seperti perakitan bom di luar negeri dikirim ke wilayah Republik Indonesiadan meledak di wilayah Republik Indonesia.

Dunia virtual/maya dengan menggunakan jaringan komputer yang bersifat terbuka memberi peluang kepada pelaku (*"offender")* untuk memilih Negara tertentu yang belum atau tidak memformulasikan suatu perbuatan sebagai tindak pidana baik di dunia nyata maupun virtual ("*CyberCrim*e") dalam Hukum Pidananya, sebagai "terminal data", sehingga "data" tetap aman di negara tersebut.

Indonesia *memformulasikan Cyber Crime* melalui Undang-Undang Nomor Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal I tentang Ketentuan Umum, pada

poin 1 menyatakan bahwa yang dimaksud dengan transaksi elektronik adalah satu atau sekumpulan data elektronik tidak terbatas, tetapi tidak terbatas pada tulisan , suara, gambar, peta, rancangan, foto, *electric data interchange (EDI),* surat elektronik (*"electronic mail")* , telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbul atau perforasi yang telah diolah yang memiliki arti atau dapat difahami oleh orang yang mampu memahaminya. Sedangkan "transaksi elektronik" diuraikan pada poin 2 nya, yaitu perbuatan hukum yang dilakukan dengan menggunakan computer, jaringan computer, dan/atau media elektronik lainnya. Pada poin 3 nya meguraikan pengertian Teknik Informasi, yaitu suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis dan atau menmyebarkan informasi. Sistem Informasi diuraikan dalam poin 5 yaitu serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan atau menyebarkan informasi elektronik.

Ketentuan lebih lanjut tentang transaksi elektronik diatur dalam Pasal 17 yang pada dasarnya mengatur tentang penyelenggaraan transaksi di ruang public maupun privat yang harus dilandasi iktikat baik.

Pasal 17 menyatakan sebagai berikut :

(1) Penyelenggaraan transaksi elektronik dapat dilakukan dalam lingkup public ataupun privat;
(2) Para pihak yang melakukan transaksi elektronik sebagaimana dimaksud pada ayat (1) wajib beriktikat baik dalam melakukan interaksi dan/atau pertukaran informasi elektronik dan/atau dokumen elektronik selama transaksi berlangsung;
(3) Ketentuan lebih lanjut mengenai penyelenggaran transaksi elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah;

Perbuatan yang dilarang oleh Undang-Undang ini dirumuskan mulai Pasal 27 sampai dengan Pasal 33 yaitu ;

1. Mendistribuskan informasi yang bermuatan melanggar kesusilan;
2. Mendistribusikan informasi yang bermuatan perjudian;

3. Mendistribusikan informasi yang bermuatan pencemaran nama baik seseorang;
4. Mendistribusikan informasi yang bermuatan pengancaman/pemerasan;
5. Menyebarkan berita bohong;
6. Menyebarkan rasa kebencian dan permusuhan bernuansa SARA.
7. Mengirimkan informasi yang bernuansa ancaman kekerasan. Atau menakut-nakuti yang ditujukan secara pribadi;
8. Mengakses data komputer orang secara tanpa hak;
9. Menjebol sistem pengamanan jaringan komputer;
10. Memasukkan informasi atau menyadap secara tanpa hak jaringan computer orang lain;
11. Melakukan perubahan jaringan komputer orang lain secara tanpa hak;
12. Memindahkan atau mentransfer informasi dari jaringan komputer orang lain;
13. Melakukan tindakan apapun yang berakibat terganggunya sisterm elektronik, sehingga tidak dapat berfungsi dengan baik;
14. Memproduksi serta mendistribusikan perangkat keras maupun lunak untuk digunakan melakukan perbuatan srebagaimana dilarang oleh Pasal 27 sampai dengan Pasal 33.

Penyelesaian sengketa menurut undang undang ini dapat ditempuh melalui 3 (tiga) jalur, yakni :

(1) Jalur perdata, dengan mengajukan gugatan, sebagaimana diatur pada Pasal 38;
(2) Penyelesaian melalui jalur arbitrase, sebagaimana diatur dalam Pasal 39; serta
(3) Jalur pidana, sebagaimana diatur dalam Pasal 45 sampai dengan Pasal 52, dengan sanksi pidana yang berfariasi, yang diancamkan secara kumulatif – alternatif berupa pidana penjara dan/atau denda.

Apabila dicermati, perbuatan yang dilarang oleh Undang Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Ekektronik, belum terdapat perbuatan yang barkaitan dengan penggunaan fasilitas elektronik untuk melakukan "*money laundering*" pada khususnya dan kejahatan yang berkaitan

dengan ekonomi/moneter/keuangan pada umumnya. Untuk itu amandemen undang-undang ini perlu dilakukan, dengan menambahkan perbuatan dilarang yang berkaitan dengan "transaksi keuangan" yang melawan hukum atau tidak sah.

D. *Cyber Money Laundering*

Cyber Money Laundering adalah pencucian uang yang dilakukan melalui dunia maya ("mayantara"), sehingga disamping melakukan tindak pidana pencucian uang (*"money laundering")* pelaku (*"offender")* juga telah melakukan tindak pidana mayantara (*"cyber crime")* yakni melakukan tindak pidana/kejahatan melalui sarana sistem/jaringan komputer.

Cyber Money Laundering juga melalui 3 tahapan aktivitas sebagaimana money laundering, yakni *placement, layering dan integration.* Aktivitas dilakukan dengan menggunakan atau melalui jaringan komputer. *Cyber Money Laundering* dengan demikian merupakan tindak pidana yang dapat dikenai Undang-Undang Nomor 15 tahun 2002 tentang Tindak Pidana Pencucian Uang; yang diperbaharui dengan Undang-Undang Nomor 25 tahun 2003, dan terakhir diamandemen dengan Undang-Undang Nomor 8 tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik sangat disayangkan belum mengatur tentang *"cyber crime"*yang berkaitan dengan transaksi keuangan yang tidak sah atau melawan hukum..

Cyber Money Laundering merupakan kejahatan yang dimungkinkan melampaui teritorial negara dan bersifat lintas negara, karenanya kerjasama antar negara untuk secara bersama-sama mangatasi *cyber money laundering* perlu terus diupayakan, karena dampaknya yang cukup signifikan terhadap perekonomian masyarakat baik di tingkat lokal,regional,nasional maupun internasional dan global.

E. *Kesimpulan*

Cyber Money Laundering merupakan kejahatan *White Collar Crime* abad 21 yang perlu diantisipasi secara serius, karena mempunyai akibat serius di bidang ekonomi di tingkat nasional maupun global.

Secara normatif, *cyber money laundering* dapat dijaring melalui Undang-Undang Nomor 15 tahun 2002 tentang Tindak Pidana Pencucian Uang yang kemudiann diperbaharui dengan Undang-Undang Nomor 25 tahun 2003, dan yang terahir diamandemen dengan Undang-Undang Nomor 8 tashun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik belum mengakomodasi tentang kejahatan mayantara (*"cyber crime")* yang berkaitan dengan transaksi ekonomi, keuangan yang melawan hukum atau tidak sah..

Sehubungan dengan hal tersebut, kesiapan aparat penegak hukum sangat penting, baik menyangkut keahlian dalam mengoperasionalkan komputer,tentang lika-liku keuangan dan Perbankan serta keahlian dalam melakukan penegakan hukum yang bersifat lintas teritorial, yang berkaitan dengan asas teritotal dengan cakupan jurisdiksi legislatif, yudikatif maupun eksekutif.

DAFTAR PUSTAKA

A. BUKU

A. Wisnubroto, 1999, "*Kebijakan Hukum Pidana alam Penanggulangan Penyalahgunaan Komputer*", Universitas Atma Jaya,Yogyakartra.

Barda Nawawi Arief, 2001, "*Antisipasi* Penanggulangan "Cyber Crime*"dengan menggunakan Hukum Pidana*"**,** makalah Seminar Nasional, STHB, Bandung.

Barda Nawawi Arief;2002**,** *Sari Kuliah Perbandingan Hukum Pidana***;** Raja Grafindo Persada, Jakarta.

Barda Nawawi Arief, 2008, "*Bunga Rampai Kebijakan Hukum Pidana*",PT Ctra Aditya Bakti, Bandung.

Nyoman Serikat Putra Jaya; 2001,*Kapita Selekta Hukum Pidana***;**BP Universitas Diponegoro, Semarang.

B. PERATURAN PERUNDANG-UNDANGAN

Undang Undang Nomor 25 tahun 2003 tentang Perubahan atas Undang Undang Nomor 15 tahun 2002 tentang Tindak Pidana Pencucian Uang.

Undang Undang Nomor 8 tahun 2010 tentang Pencegahgan dan Pembe+-rantasanTindak Pidana Pencucian Uang.

Undang Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

RUU KUHP tahun 2015.