LAPORAN HASIL PENELITIAN

Problematika Hukum Perkembangan *Electronic Money* Dalam Kerangka Pencegahan Pencucian Uang Menurut Undang-undang No. 25 Tahun 2003

Oleh:

Dr. Ignasius Sumarsono Raharjo, S.H.,M.Hum.

Fakultas Hukum
Universitas Atma Jaya Yogyakarta
2008

LAPORAN HASIL PENELITIAN

Problematika Hukum Perkembangan *Electronic Money* Dalam Kerangka Pencegahan Pencucian Uang Menurut Undang-undang No. 25 Tahun 2003

Oleh:

Dr. Ignasius Sumarsono Raharjo, S.H.,M.Hum.

Fakultas Hukum
Universitas Atma Jaya Yogyakarta
2008

LEMBAR IDENTITAS DAN PENGESAHAN LAPORAN AKHIR

PENELITIAN MANDIRI

1.a. Judul Penelitian : **Problematika Hukum Perkembangan *Electronic Money* Dalam Kerangka Pencegahan Pencucian Uang Menurut Undang-undang No. 25 Tahun 2003**

1.b. Kategori Penelitian : III.

2. Peneliti
2.a. N a m a : Dr. Ignasius Sumarsono Raharjo, S.H.,M.Hum.
2.b. Bidang Keahlian : *Cyberlaw*
2.c. Pangkat dan jabatan/gol: Penata/Ass. Ahli/IIIB.
2.d. Tempat Penelitian : Jakarta dan DIY
2.e. Waktu Penelitian : 15 jam perminggu
2.f. Unit Kerja : Fakultas Hukum Universitas Atma Jaya Yogyakarta
2.g. Alamat surat : Jln. Mgr. Sugiyapranata 08, Klaten Utara, Klaten
Telepon : (0272) 323945, HP: 0815 7834 9007.

3. Jumlah Peneliti : Penelitian Mandiri

4. Lokasi Penelitian : Yogyakarta, Jakarta, dunia maya

5. Jangka waktu penelitian: 6 (enam) bulan

6. Biaya yang diperlukan : Rp. 2.850.000,00 (Dua Juta Delapan Ratus Lima Puluh Ribu Rupiah)

Mengetahui,
Ketua Bagian Keperdataan

Iswantiningsih, S.H.,M.S.

Yogyakarta, 20 Agustus 2008
Peneliti,

Dr. Ign. Sumarsono Raharjo, S.H.,M.Hum.

Menyetujui,
Dekan Fakultas Hukum,

B. Hestu Cipto Handoyo, S.H.,M.Hum.

Ketua LPPM

01 SEP 2008

Ir. B. Kristyanto, M.Eng.,Ph.D.

PRAKATA

Syukur dan terima kasih yang berlimpah perlu saya lambungkan kepada Bapa yang mahakasih dan bertahta di kerajaan sorga, karena berkat kelimpahan-Nya penelitian ini dapat diselesaikan, biarpun dalam hal tertentu mengalami kesulitan karena harus menunggu beberapa literatur yang langka didapatkan.

Kebahagiaan ini bertambah sempurna seiiring dengan ucapan terima kasih saya yang tidak terhingga kepada yang terhormat:

1. Dekan Fakultas Hukum Universitas Atma Jaya Yogyakarta;
2. Ketua LPPM Universitas Atma Jaya Yogyakarta;
3. Rekan-rekan yang berkantor di PPATK yang membantu mencarikan bahan hukum pendukung untuk alat recheck penelitian ini;
4. Semua saja yang membantu selesainya penelitian ini yang tidak mungkin saya sebut satu per satu;

Akhirnya menyadari setulusnya sebagai hamba Tuhan, *servio Dei*, maka dengan sujud syukur dan mengakui bahwa karya penelitian ini sangat tergantung kepada Tuhan, saya kembalikan karya yang kecil ini kepada Tuhan dan untuk kemanfaatan kepada sesama di dalam negeri tercinta dan masyarakat global pada umumnya. Amin.

Yogyakarta, 20 Agustus 2008

Peneliti,

Dr. Ign. Sumarsono Raharjo, S.H.,M.Hum.

ABSTRAK

Ign. Sumarsono Raharjo

Problematika Hukum Perkembangan *Electronic Money*
Dalam Kerangka Pencegahan Pencucian Uang
Menurut Undang-undang No. 25 Tahun 2003

Dugaan FATF tentang pencucian uang cenderung mengatakan bahwa sarana e-money untuk pencucian uang mengalami perkembangan yang pesat. Oleh karena itu nilai strategis penelitian ini adalah untuk menganalisis dua perkembangan hukum yaitu perkembangan hukum nasional Indonesia dan perkembangan global sehubungan dengan obyek penelitian karena pelanggaran ini bersifat borderless, paperless, anonym dan menggunakan sarana teknologi informasi yang berkembang revolusioner. Melalui penelitian normatif dengan pendekatan analisis *statute approach* dan *comparative approach*, ditemukan bahwa Undang-Undang No. 25 Tahun 2003 dan peraturan pelaksanaannya termasuk peraturan yang dibuat oleh PPATK, PBI, Undang-Undang ITE tidak cukup untuk mencegah pelanggaran tindak pencucian uang di *cyber* karena disamping pola *smurfing* atau *structuring* masih tetap dilegalkan tetapi juga penting bahwa *e-money* dapat dilakukan tidak hanya oleh lembaga perbankan pemerintah tetapi juga dilakukan oleh lembaga keuangan lainnya. *E-money* mempunyai 'karakter' dapat dilakukan dimanapun di dunia sebagai konsekuensi globalisasi serta kapanpun juga baik untuk mengirim transaksi maupun menerima transaksi, sifat anonimitas, sehingga relatif sulit dilakukan pelacakan, biarpun pengaturan prinsip mengenal nasabah sudah ditegakkan. Berkembangnya tindak pencucian uang melalui sarana *electronic money* adalah suatu keniscayaan. Maka, hukum juga harus berkarakter sibernetis yaitu *variety, circularity, process* dan *observation*. Hukum sibernetis adalah hukum yang fungsional, dalam arti, hukum berfungsi melindungi dan sebagai tempat menuntut keadilan dengan relasi ketergantungannya dengan suatu sistem dan faktor lingkungan dari sistem hukum di dunia maya yang menciptakan *lex informatica* sehingga menjadi hukum bagi para pihak di dalam aktivitasnya di dunia maya. Pencegahan *cyberlaundering* hanya dapat dilakukan melalui kebijakan hukum yang berkarakter sibernetis yaitu harus cepat berubah, fungsional dan disesuaikan kebutuhan.

Keywords: E-money, cyber laundering, money laundering.

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan transaksi-transaksi global dengan menggunakan elektronik telah mendorong pula pertukaran uang dan transfer uang melalui *Electronic Money* karena hal tersebut telah ditunjukkannya sebagai bentuk kinerja keuangan yang mempunyai efisiensi dan efektivitas luar biasa. Perkembangan internet telah memacu hal tersebut karena sistem transfer dana melalui *cyber-money* meningkatkan efisiensi dan efektivitas perbankan. Namun, dengan kemajuan transfer dana *online* yang luar biasa tersebut telah pula memunculkan permasalahan yang juga bertumbuh antara lain pencucian uang dengan menggunakan sarana transfer dana *online* karena sifat *borderless* dan *paperless* sehingga relatif pelacakan dan identifikasi adanya pencucian uang menjadi lama dan sulit dilakukan yang berarti pelaku akan lebih mudah untuk menentukan sikap dan penyelundupan hukum melalui anonimitas data pribadi.

FATF (*Financial Action Task Force*) sudah lama yaitu sejak tahun 1996 melaporkan bahwa tipologi pencucian di Asia (di luar bekas negara Uni Soviet) selaras dengan awal berkembangnya transfer dana melalui elektronik. FATF melaporkan bahwa karakteristik di negara-negara ini adalah:[1]

> "1. Ekonomi Asia sangat *cash intensive* dan pada umumnya tidak memiliki mekanisme untuk melacak transaksi-transaksi tunai yang jumlahnya besar;
> 2. *Underground banking* yang dikenal sebagai sistem *hundi*, *chit* atau *fei-chien*, tergantung pada wilayah dan kelompok etnis yang tersangkut dengan sistem itu, merupakan tradisi yang bersejarah panjang di bagian dunia ini. *Underground*

[1]Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 1999-2000,p.10.

banking memberikan layanan cepat, murah, efisien dan cara-cara yang anonim untuk memindahkan uang;

3. Beberapa negara yang bukan anggota FATF di Asia memiliki undang-undang pencucian uang tetapi tidak diterapkan dengan sungguh-sungguh."

Disamping itu, pola perdagangan narkoba (*drug trafficking*) melalui segitiga emas (*Golden Triangle*) di Asia Tenggara (Myanmar, Laos dan Thailand) dan negara-negara Afghanistan dan Pakistan (*Golden Crescent*) telah diidentifikasi sebagai salah satu sumber utama hasil kejahatan di wilayah Asia yang penghasilannya dicuci dengan menggunakan celah-celah peraturan di bidang *electronic money* dan pencucian uang *online*.

Banyak permasalahan yang muncul sehubungan dengan berkembangnya transaksi-transaksi yang dilakukan melalui internet dan cara-cara pembayaran menggunakan *electronic money*. FATF telah merintis adanya 40 rekomendasi yang harus dilaksanakan oleh anggotanya sebagai kerangka dasar bagi upaya-upaya anti pencucian uang dan dirancang sebagai harmonisasi hukum untuk diaplikasikan ke dalam hukum-hukum nasional negara-negara anggota dan ditujukan sebagai pengaturan universal. Oleh karena itu, karena Indonesia sebagai salah satu negara anggota tentunya memerlukan penyesuaian-penyesuaian sehubungan dengan perkembangan *electronic money* yang rentan terhadap praktek pencucian uang tersebut. Undang-Undang No. 25 Tahun 2003 tentang Tindak Pidana Pencucian Uang, ternyata telah mengalami ketinggalan zaman setelah berkembangnya *online transaction* dan *electronic funds transfer*. Undang-Undang No. 25 Tahun 2003 diduga telah mengalami stagnasi setelah berkembangnya *E-money* atau *E-cash*. Identifikasi permasalahan diharapkan dapat membangun suatu konfigurasi masalah sehingga dapat dicarikan alternatif

penyelesaian hukum dengan berpijak dari "fungsi hukum" dalam perkembangan teknologi informasi di masyarakat.

Fokus pada aspek *electronic money* khususnya pencegahan penggunaan *electronic money* untuk tindakan pencucian uang menjadi masalah serius. Padahal apabila dilihat secara holistik, aspek yang muncul adalah multi aspek meliputi yurisdiksi, *virtual juries*, hukum yang diberlakukan, jangkauan dan efektivitas Undang-undang No. 25 Tahun 2003. Dengan memfokuskan diri pada aspek-aspek yuridik perkembangan *electronic money* yang potensial digunakan untuk tindak kejahatan pencucian uang maka diharapkan dapat dilakukan pengkajian yang mendalam terhadap pelanggaran atau kejahatan melalui penyalahgunaan *electronic money* dalam bisnis *online*. Fungsi hukum dalam hukum modern yang *"...a tool of social engineering"* perlu dikaji kembali karena tidak tepat dalam kondisi perkembangan yang revolusioner atas teknologi informasi terutama sistem pembayaran yang global dan mengindikatorkan adanya uang tanpa kebangsaan. Sebaliknya fungsi hukum yang responsif perlu dipertajam dalam konteks aplikasinya sehingga efektivikasi hukum terjamin.

B. Perumusan Masalah.

1. Bagaimanakah implementasi UU No. 25 Tahun 2003 dengan berkembangnya *electronic money* untuk mencegah pelanggaran yang bersangkutan dengan tindak pencucian uang?
2. Kebijakan hukum apakah yang dapat ditempuh berkenaan dengan diduganya berkembang tindak pencucian uang melalui sarana *electronic money*?

BAB II

TINJAUAN PUSTAKA

A. Perkembangan Transaksi Elektronik dan *Electronic Money*

Menurut *Electronic Commerce Expert Group* (ECEG) seperti dikutip oleh Melissa De Zwart,[2] *Electronic-commerce (E-com)* adalah:

> "a broad concept that covers any commercial transaction that is effected via electronic means and would include such means as facsimile, telex, EDI, internet, and telephone. For the purpose of this report the term is limited to those trade and commercial transactions involving computer to computer communications wether utilising an open or closed network."

Pengertian yang dikutip oleh Melissa ini menunjukkan perbedaan dengan pengertian *E-com* khususnya media yang dipergunakan yaitu membatasi diri pada komunikasi komputer ke komputer baik menggunakan jaringan terbuka maupun tertutup sehingga apabila media yang dipergunakan adalah Telex, Fax, telekopi, telepon bukan merupakan *E-com*.

Pengertian lain tentang *E-com* yang dimaksudkan untuk menampung perkembangan hubungan perdagangan internasional diberikan oleh UNCITRAL melalui *UNCITRAL Model Law on Electronic Commerce*. Menurut *Model Law on Electronic Commerce*, *E-com* adalah perdagangan yang dilakukan dengan menggunakan *data messages*,[3] yaitu:

> "the term 'commercial' should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of

---

[2] http://www.unsw/lawjournal.html (Melissa De Zwart, "Electronic Commerce: Promises, Potential and Proposals,")

[3] Data messages adalah information genereted, sent, recieved or stored by electronic, optical or similar means including; but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy.

> commercial nature include, but are not limited to, the followong transactions: any trade transactions for the supply or exhange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road."

Interpretasi UNCITRAL tersebut di atas cukup luas karena mencakup seluruh hubungan-hubungan sifat perdagangan baik yang bersifat kontraktual maupun tidak, dengan memberikan cakupan luas. yaitu memerinci secara enumeratif sebagai cara untuk menampung perkembangan perdagangan dunia. Diskripsi tersebut di atas juga menggambarkan bahwa media yang dominan digunakan adalah elektronik (termasuk digital) dalam suatu jaringan baik tertutup maupun terbuka. Hal ini sangat berbeda dengan perdagangan konvensional yang *paper-based* dan keharusan kontak-kontak phisik para pihak diperlukan.

Berbagai definisi tentang *E-com* tersebut telah memberikan pemahaman adanya aksentuasi bahwa *E-com* tidak semata-mata perdagangan melalui internet tetapi cukup luas yaitu tidak hanya melakukan praktek penjualan dan pembelian saja tetapi juga pelayanan nasabah dan mengkolaborasi dengan partner bisnis dan melakukan transaksi elektronik (dan digital) ke dalam suatu organisasi atau individu. Dalam perkembangannya sekarang, *E-com* merupakan bagian dari *Electronic business* (E-bis) yang menjadi genusnya atau dengan kata lain *electronic commerce is a part of electronic business*. Hubungan antara *E-com* dan *E-bis*, ditegaskan oleh Lou Garstner IBM,s CEO yaitu bahwa *E-business is all*

about time cycle, speed globalization, enhanced productivity, reaching new costumer and sharing knowledge across institutions for competitive advantage.[4]

Dekade pertengahan tahun 1990 terdapat dua pembidangan besar dalam hubungan bisnis *E-com* yaitu kontak antar bisnis *(business to business)* yang menggunakan sarana EDI *(Electronic Data Interchange)* untuk *E-com* dan pemakaian individu/perorangan yang menggunakan internet dan WWW. Pada Tahun 1995, internet mulai digunakan secara serius sebagai basis perdagangan dunia.[5] Keuntungan menggunakan EDI adalah:[6]

1. A large volume of repetitive standard actions;
2. Very tight operating margins;
3. Strong competition requiring significant productivity improvement;
4. Operational time constraints;
5. Trading partners request for paperless exchange of documents."

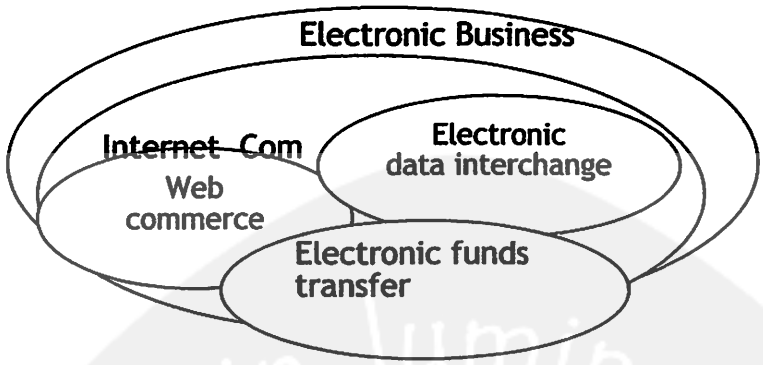
Sekarang, pertumbuhan *E-com* telah menunjukkan perkembangan yang mengagumkan, dan munculnya pembidangan yang jelas dengan terminologi-terminologi baru. Terminologi tersebut dimulai dengan *electronic business,* yang merupakan hubungan bisnis yang paling luas dan umum dan meliputi *E-com, internet commerce, Web Commerce,* EDI dan EFT. Penjelasan secara rinci tentang pembidangan tersebut dapat dijelaskan dalam **Figure 1** sbb:

---

[4]Efraim Turban, et.al., Turban, Efraim et.al., **Electronic Commerce A Managerial Perspective**, New Jersey, Prentice Hall, 2000, p.4.

[5]Sidney L. Huff, et.al., **Cases In Electronic Commerce**, The McGraw-Hill Companies, Boston AS. 2000,p.4.

[6]Kamlesh K Bajaj & Debjani Nag, **E-Commerce: The Cutting Edge of Business**, Tat McGraw-Hill Publishing Limited, New Delhi, 2000, p.15.



"The largest oval is labeled "electronic business". Simply put, this includes everything having to do with the application of information and communication technologies (ICT) to the conduct of business between organizations or from company to consumer. Within the electronic business oval is smaller oval labeled 'electronic commerce'. This highlights the fact that there are numerous forms of business-related ICT - based interactions that can accur between businesses, or between a business and an end consumer, which do not directly concern buying and selling (i.e., 'commerce). Only those forms of interaction having to do with commerce are included in the electronic commerce oval. This includes advertising of products or services, electronic shopping, and direct after sales support. It would not include such things as interoganizational collaboration, using ICT-based collaboration systems, for the development of a new product.

Within the electronic commerce oval is a smaller oval labeled 'Internet commerce.' This reflects the fact that electronic commerce need not be conducted only over the Internet. In fact a great deal of business-to-business electronic commerce is still today conducted over private networks, using primarily traditional EDI channels and value-added network (VAN) service providers. This is changing, as more and more companies adopt the Internet for some or all of their busines-to business electronic commerce, but it will be many years before the Internet largely displace the VANs.

Within the Internet commerce domain lies an even smaller subset, termed "web commerce". This is the component of electronic commerce conducted strictly over the World Wide

> Web. The WWW is not the only way of using the Internet for commercial interactions. Electronic mail, for example, serves well for certain forms of electronic commerce. Software may be conveniently sold over the Internet using the file transfer protocol (FTP) for product distribution. Nevertheless, the Web is clearly the dominant medium for the large majority of Internet commerce today. Furthermore, since modern web browsers incorporate other Internet applications, including electronic mail and file transfer via FTP, all under one hood, users today have the perception that they are relying solely on the Web even as they send and receive e-mail, transfer files, and conduct other forms of Internet application that used to be conducted using separate application programs.
>
> There are two other important domains represented in Figure 1. One is labeled "electronic data interchange." It is shown to lie fully within the electronic commerce realm, but it overlaps the other domains of web commerce, Internet commerce and electronic funds transfer. As discussed earlier, EDI precedes modern-day electronic commerce by almost two decades. It is clearly a type of electronic commerce, since EDI comprises standard formats for a variety of business commercial transactions such as orders, invoices, shipping documents, and the like. But EDI can be conducted either over private networks or over the Internet. If conducted over the Internet, it may not make use of the WWW. Also, it may or may not involve aspects of electronic funds transfer.
>
> Finally, the oval labeled 'electronic funds transfer,' or EFT, bears much the same relationship with the other domains as does EDI. It is an aspect of electronic commerce, hence is represented as falling fully within the electronic commerce oval. It can be conducted over the Internet or over private networks, and if over the Internet, it may or may not be conducted over the Web. Also, EFT may be executed using EDI standards or alternately may be done in non-EDI fashion ..."[7]

Disamping tersebut di atas, *electronic business* juga termasuk di dalamnya: **(1).** *Electronic advertising*; (2). *Electronic buying and selling*; (3). *Electronic distribution*; (4). *Direct client interaction for marketing and customer service*;

[7]Sidney L. Huf, Op.cit., p.4-6.

(5). *Groupware, e-mail, electronic collaboration*; (6). *Workflow, automated forma distribution*; (7). *Secure X.400 (e-mail) business transactions.*

Penjelasan yang terperinci tersebut di atas, menunjukkan bahwa *E-com* mempunyai banyak aplikasi yaitu mulai dari belanja di mall dan toko yang melayani fasilitas *E-com, home banking, online-stock* pembelian barang dan jasa, *auction*, kolaborasi elektronik untuk proyek pembangunan serta penelitian yang membutuhkan dukungan informasi, sistem dan infrastruktur organisasi yang efisien dan efektif dalam melakukan pekerjaan.

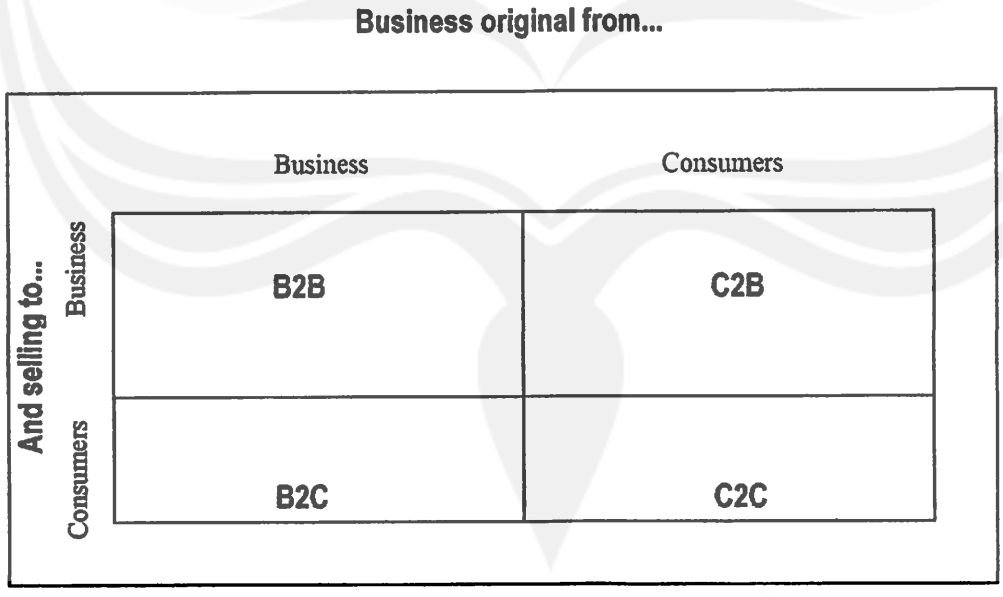
Pengertian-pengertian tentang *E-com* serta luas lingkupnya di atas, setidaknya memberikan pemahaman bahwa *E-com* adalah merupakan bagian dari *E-business* yang berdemensi *luas*. Pemahaman *E-com* sebagai perdagangan melalui internet adalah tidak tepat. *E-com* merupakan seluruh aktifitas bisnis yang dilakukan melalui media elektronik dan digital. Popularitas *E-com* sebagai perdagangan yang hanya menggunakan internet dan WWW karena *E-com* berkembang dengan pesat setelah menggunakan sarana internet dan WWW sehingga menjanjikan efisiensi dan efektivitas perdagangan. Sifat global, *borderless, paperless* dan disertai teknologi yang memungkinkan untuk itu, sangat menekan beaya-beaya *(low cost)* seperti misalnya: iklan, pembuatan, pemrosesan, pendistribusian, penyimpanan segala informasi. Interaksi yang tidak mengenal waktu (24 jam) serta komunikasi dapat dilakukan bersama-sama oleh jutaan orang dari berbagai negara di dunia adalah keunggulan *E-com*. Disamping itu, *E-com* sangat efektif dan efisien untuk memperluas pasar yang tidak mengenal istilah nasional dan internasional karena sifat globalnya. Baku mutu produk dapat dijamin dengan baik karena individu-individu dan perusahaan-

perusahaan dapat dengan cepat dan mudah untuk mendapatkan *supplier, customer, partner* yang dikehendaki sesuai dengan kualifikasi yang diinginkan.

Terdapat empat perbedaan kategori dalam E-com yang diidentifikasi sebagai hubungan antar pebisnis (*business to business*/B2B), pebinis dengan konsumen (*business to consumer*/B2C), konsumen dengan konsumen (*consumer to consumer*/C2C) dan konsumen dengan pebisnis (*consumer to business*/C2B). Hubungan antar para pihak tersebut selanjutnya dapat dijelaskan sbb:

> "...Business to business refers to the full spectrum of e-commerce that occurs between two organizations. Many of the same activities that occur in business-to-business also occur in the business-to-consumer context, except transactions relating to the "back office" of the customer that are often not tracked electronically. Consumer-to-consumer activities include auction- exchanges, classified ads, games, bulletin boards, and personal services. Consumers can also band together to form buyer groups in a consumer-to-business relationship..."

Penjelasan tersebut di atas dapat digambarkan ke dalam figure 2 sbb:[8]



[8]Jeffrey F. Rayport & Benard J. Jaworski, Cases in E Commerce, New York, McGraw Hill, 2002., p.3.

Kombinasi hubungan-hubungan antara para pihak dalam *E-com* yang variatif dan kompleks menunjukkan bahwa dalam model ekonomi baru (*New Economy*) ini *E-com* sebagai "*...unique in several respects...*". Hal ini karena *E-com* mempunyai beberapa cirikhas lain yaitu:[9]

> "a. Core strategi decisions are technology-based. Technology has been an increasing part of business strategy; in the New Economy, it is interlinked with strategy decisions as opposed to being a secondary, support activity;
>
> b. There is real-time competitive responsiveness. Competitors are easy to find, track, and compare. This transparency of activity leads to unprecedented speed in cometitive responses;
>
> c. The store is always open. It is not necessary to retool the factory or close down for a face interaction;
>
> d. The customer interface shifts from a traditional, face to face interaction to a screen-to-face interaction;
>
> e. The customer controls the interacti on. Certainly the online business attempts to shift and influence consumer has increasing control of the interaction.
>
> f. On the firm side, e-businesses are able to track behavior to an unprecedented level-noting where the consumer visited, how long he or she stayed, and so on;
>
> g. Businesses benefit from network effects. Namely, the value of the service increases as the number of other users use the service. But network effects place increased burdens on online firms to become the "standard" for the category;
>
> h. e-commerce uses nontraditional evaluation metrics and emergent valuation models. Cash flow will continue to be the single most important indicator of the value of a business, but the logic of valuation has become more complex (i.e., real options theory). Moreover, the "scorecard" that one uses to judge the progress of business is also changing."

[9]Ibid., p.2.

Berbagai pendapat yang variatif tentang *E-com* tersebut di atas adalah hal yang wajar karena masing-masing penulis memberikan penekanan pada aspek-aspek tertentu. Penulis berpendapat bahwa *electronic commerce* adalah sistem perdagangan global yang menampung sebagian besar aktivitas bisnis dengan menggunakan media informasi elektronik (yaitu EDI, E-mail, EBB [Electronic Bulletin Boards], EFT, Internet, WWW atau teknologi jaringan lainnya, telepon, teletex, telegram, fax, telekopi serta teknologi elektronik lainnya) untuk sarana hubungan-hubungan kontraktual ataupun bukan kontraktual, dalam penyediaan barang, jasa atau pengambil-alihan hak. Oleh karena itu maka *E-com* pada prinsipnya adalah berbasis pada hubungan hukum yang sebagian besar kontraktual tetapi dapat juga dimungkinkan bukan kontraktual dan menampung sebagian besar hubungan bisnis. Disamping itu, hubungan bisnis tersebut dalam lingkup sistem perdagangan global melalui teknologi jaringan maka dalam kontrak sebaiknya disebut yurisdiksi yang dipilih apabila terjadi sengketa. Informasi elektronik dalam bentuk data, message, record, dokumen adalah merupakan bentuk tertulis, sebagaimana diakui dalam Pasal 6 UNCITRAL *Model Law on Electronic Commerce,* sehingga mempunyai akibat hukum dan kekuatan hukum sehingga kepenuhan syarat hukum bukti tertulis dapat dipenuhi.

B. Perkembangan Pencegahan Pencucian Uang Menurut Undang-undang No. 25 Tahun 2003

Electronic Money adalah merupakan pengertian yang tidak tunggal. E-money juga sering disebut sebagai *electronic cash* atau digital cash atau *digital cash*. Sistem keuangan (*financial systems*) dunia karena perkembangan internet memungkinkan untuk suatu nilai ekonomis dinyatakan secara digital atau elektronik melalui pola elektronik. Art. I Sec. 3 (b) dari *Directive 2000/46/EC of*

the Europen Parliament and of the Council of 18 September 2000, menguraikan mengenai *electronic money* sbb:

> "electronic money shall mean monetary value as represented by a claim on the which is:
> (i). Stored on an electronic device;
> (ii). Issued on receipt of founds of and amount not loss in value than the monetary value issued;
> (iii). Accepted as mean of payment by undertakings other than the issuer."

Disamping tersebut di atas, istilah lain yang digunakan yaitu *E-cash*, menurut Mark Bortner adalah:

> "Electronic cash, or digital money, is an electronic replacement for cash. Digital cash has been defined as a series of numbers that have an intrincit value to same form of currency. Using digital cash, actual assets are transferred through digital communicatrion in the form of individually identified representations of bills and coins - similar to serial members on hard currency."

Definisi-definisi di atas maka *E-money* dimaksudkan sebagai pengganti uang logam dan uang kertas (*banknote*) untuk tujuan melakukan pembayaran secara elektronik. *E-money* dapat berfungsi sebagai *"medium of exchange, a unit of account and a store of value"*. *E-money* dapat dibawa dalam sejumlah peralatan-peralatan elektronik (*electronic devices*) termasuk *magnetic swipe card, smart card, computer memory, mobile phone, personal digital assistant*, dan *digital TV set*. *E-money* dapat diambil dari suatu rekening bank pada ATM atau dengan menggunakan *"smart phone"*. *E-money* dapat pula di-*downloaded* dari internet melalui PC atau melalui *mobile phone*.Cara yang utama memperoleh *e-money* adalah dengan membeli *card* yang telah dapat digunakan langsung untuk melakukan pembayaran terhadap suatu pelaku usaha (*merchant*) atau dapat ditransfer ke *hard drive* dari suatu PC dengan melakukan *keying* ke dalam nomor seri yang khusus dalam card tersebut. Begitu *e-money* diperoleh, maka *e-money*

tersebut dapat dipakai untuk melakukan pembayaran-pembayaran yang berjumlah kecil, sekalipun dalam jumlah beberapa *cent* saja dan akan menguntungkan baik untuk pelaku usaha yang menerima pembayaran, maupun bagi penerbit *digital cash* tersebut.[10] Penggunaan *e-money* dapat dilakukan dengan cara-cara:[11]

- memasukkan (inserting) suatu kartu pada suatu terminal;
- menggunakan contactless wireless technology untuk mentransfer nilai (value) yang ada dalam suatu card ke suatu terminal; atau
- melakukan transmitting nilai (value) melalui internet dari suatu PC.

Dibandingkan dengan uang tradisional/konvensional, ada beberapa kelebihan dari *e-cash*. Kelebihan-kelebihan tersebut adalah:[12]

a. E-cash lebih memberikan kemudahan (*convenient*) dan lebih luwes (*flexible*) daripada uang yang tradisional;
b. Dapat digunakan oleh konsumen maupun oleh para pelaku usaha;
c. Dapat digunakan untuk membeli barang dan jasa apapun juga sepanjang para pihak menggunakan dan menerima e-cash sebagai alat pembayaran.
d. Memiliki pecahan sampai sen (cent) sehingga tidak ada pihak yang dirugikan karena pembulatan yaitu karena pembayar tidak memiliki uang sen untuk pembayaran atau penerima tidak memiliki uang sen untuk kembalian.
e. Pembayaran dapat dilakukan tanpa harus menggunakan atau melalui intermediasi, misalnya tidak perlu ada campur tangan bank di antara pembayar dan penerima pada waktu pembayaran itu dilakukan, kecuali para pihak menggunakan rekening-rekening yang ada di bank mereka masing-masing.
f. Pembayaran dapat dilakukan seketika dan sifatnya realtime.
g. Tidak perlu dibawa-bawa secara fisik, apalagi bila jumlahnya besar dan memerlukan jumlah lembaran yang banyak. Bila ingin dibawa dapat disimpan dalam suatu smart card yang besarnya sama dengan suatu kartu kredit. Dengan demikian dalam menyimpan e-cash menjadi mudah dan aman.

---

[10]Financial Service Authority, **Deregulation of Electronic Money Issuers**, December 2001, Consultation Paper 117, p.16

[11]Geoffrey Turk, **Money and Currency in the 21 Century**, Juli 1997, http://www.info.goldmoney.com

[12]Sutan Remy Sjahdeini, **Seluk Beluk Tindak Pidana Pencucian Uang dan Pembiayaan Terorisme**, Grafiti Pers, Jakarta, 2004, h.59-60.

h. Menjamin privasi (privacy) atau kerahasiaan dari pihak-pihak yang bertransaksi yaitu karena anonim (anonymous). Dengan demikian juga tidak dapat dilacak oleh siapapun (untraceable). Dari aspek ini sama halnya dengan uang yang tradisional.
i. Bagi bank-bank yang menerbitkan e-cash biayanya lebih murah daripada menangani cek dan keharusan untuk melakukan pencatatan sebagaimana hal itu biasanya dilakukan dalam menangani uang yang tradisional.
j. Penerbitan e-cash tidak bersifat penciptaan yang menambah jumlah uang yang beredar, karena untuk memperoleh e-cash dari penerbitnya harus dengan cara membeli atau menukar dengan uang tradisional, baik yang berupa uang kartal maupun uang giral.

Disamping kelebihan-kelebihan tersebut, *e-cash* juga mempunyai kekurangan-kekurangan yaitu sbb:[13]

a. penyimpanan e-cash pada PC dapat terancam apabila sistemnya mengalami crash.
b. E-cash dapat meningkatkan kecemburuan sosial dari masyarakat miskin terhadap masyarakat kaya, karena mereka yang memiliki akses langsung ke sistem e-cash, sedangkan mereka yang tidak memiliki PC, yang sebagian besar adalah konsumen yang berpenghasilan sangat rendah, tidak memiliki akses tersebut.
c. Pencucian uang dan penghindaran pajak (tax evasion) dapat marak dilakukan dalam sistem e-cash yang tidak berkewarganegaraan (stateless e-cash system) karena para penjahat dapat menggunakan e-cash yang tidak dapat dilacak untuk menyembunyikan kekayaan mereka.
d. Uang-uang tradisional palsu yang berhasil dipakai untuk memperoleh (membeli) e-cash akan menyulitkan bagi otoritas pemberantas pemalsuan uang karena e-cash yang diperoleh dari uang-uang tradisional palsu tersebut telah bercampur dengan e-cash yang diperoleh dari uang-uang tradisional yang tidak palsu dalam sistem e-cash tersebut.
e. Apabila computer hackers atau penjahat-penjahat lain berhasil masuk ke dalam sistem e-cash, mereka dapat seketika meraup kekayaan elektronik tersebut dalam jumlah ribuan bahkan jutaan dollar milik pemilik e-cash yang tidak berdosa. Sistem pengamanan yang baik dapat memberikan perlindungan yang diharapkan oleh para pemilik e-cash di dalam sistem tersebut.
f. Pertumbuhan sistem e-cash dapat menambah beban tugas dari otoritas yang berkewajiban mengawasi sistem keuangan.

[13]Ibid., h.61.

Spesifikasi *e-money* adalah dapat diterbitkan oleh lembaga keuangan yang bukan bank sentral, baik lembaga tersebut adalah bank atau lembaga bukan bank. Berbeda dengan *banknotes* yang hanya dapat diterbitkan oleh suatu bank sentral atau oleh lembaga negara yang berfungsi sebagai penerbit *banknote*. Dalam perkembangannya kemudian maka terdapat mata uang yang diterbitkan oleh bank sentral disebut *government currency* dan mata uang yang diterbitkan oleh badan-badan swasta (bank-bank atau lembaga-lembaga keuangan bukan bank) disebut sebagai *private currency* yang dapat berupa *electronic money*.

Penyalahgunaan Electronic Money untuk Pencucian Uang

Sebelum adanya *virtual world*, pencucian uang dilakukan sebagai *physical transportation of hard cash*. Setelah makin populernya penggunaan transaksi online dengan pembayaran online yaitu melalui transfer dana elektronik dengan cara apapun yang memungkinkan terutama melalui E-bank, maka mulailah marak penyalahgunaan *electronic banking* tersebut untuk sarana pencucian uang. Pencucian uang yang dilakukan dengan cara menggunakan sarana *online* biasa disebut *cyberlaundering* dan merupakan teknik paling mutakhir pencucian uang. Salah satu ciri dari transfer yang bersifat digital (*digital transfer*) adalah bahwa transfer tersebut dapat dilakukan dengan anonim. Undang-undang No. 25 Tahun 2003 tentang Tindak Pidana Pencucian Uang dan berbagai peraturan perundangan di negara-negara lain yang mengharuskan bank-bank untuk membuat dan menyampaikan laporan kepada otoritas yang berwewenang atas transaksi-transaksi yang mencurigakan (*suspectious transactions*), menjadi tidak berarti dan bermakna karena bank-bank yang diwajibkan melapor itu tidak mengetahui darimana asal-usul uang yang masuk ke dalam suatu rekening. Laporan transaksi keuangan hanya

berguna apabila transaksi itu dapat dilacak sampai kepada suatu rekening yang spesifik. Dengan demikian pemecahan jumlah transaksi yang disebut *structuring of transaction*, dengan maksud untuk menghindari ketentuan-ketentuan pelaporan transaksi keuangan menjadi sangat kecil sekali risikonya apabila dana-dana yang mengalami *restructuring* tersebut praktis tidak dapat dilacak (*untraceable*).

Menurut Departemen Kehakiman Kanada (1988), potensi penyalahgunaan *e-money* oleh para pencuci uang adalah karena dua alasan menarik yaitu:

a. transaksi-transaksi yang dimaksud tidak dapat dilacak (*untraceable*);
b. transaksi-transaksi tersebut bergerak sangat cepat (*highly mobile*).

Bloomberg.co.uk pada tanggal 2 Februari 2002 memuat berita dengan judul *"Internet Banks Are Money Laundering Havens, OECD Report Says."* dikatakan bahwa:

> Internet banks are a heaven for money laundering and should face tighter regulatory controls, the Time of London reported, citing a report by the Organization for Economic Cooperation and Development.
> Internet banking is a money-launderer's dream. Andrew Clarke, a partner and money-laundering expert at Price Waterhouse Coopers told the paper.
> Money launderers are able to hide behind the anonymity of the Internet to create false identities, the paper said.

Berkenaan dengan sangat rawannya penggunaan Internet Banking untuk dipakai melakukan pencucian uang, maka *Financial Action Task Force's 1999-2000 Money Laundering Typologies Report* telah memasukkan Internet Banking sebagai salah satu dari masalah-masalah *money laundering* yang utama yang perlu mendapat perhatian global. Internet banking memungkinkan akses langsung ke rekening-rekening (*accounts*), lembaga-lembaga keuangan (*financial institution*) tidak mungkin melakukan verifikasi bahwa orang-orang yang mengakses rekening

tersebut yang tercatat di bank. Hal ini, bersama-sama dengan tersedianya internet secara global, memungkinkan dilakukannya akses dari manapun juga secara online yang anonim dan tidak terbatas ke rekening-rekening bank tersebut. Menurut laporan tersebut, kelompok-kelompok kejahatan, termasuk *Colombian Black Market Peso Exchange, Indian "Hawala"* dan *Chinese "Fliying Money"* makin sering menggunakan jaringan perbankan tersebut untuk memindahkan uang hasil kejahatan mereka. Laporan tersebut lebih jauh mengemukakan bahwa sistem itu merupakan cara yang murah (*inexpensive*), memberikan kemudahan (*convinient*), dan dapat diandalkan untuk memindahkan uang dari satu lokasi ke lokasi lainnya di luar sistem peraturan perundang-undangan nasional di bidang keuangan dan tanpa melakukan pemindahan fisik dari uang tersebut. Sistem tersebut melibatkan hanya sedikit *paperwork*, menyulitkan upaya untuk melacak aliran uang haram yang dicuci itu melewati batas-batas internasional.[14]

FATF dalam laporannya dua tahun berturut-turut mengemukakan keprihatinannya kepada negara-negara anggotanya mengenai kerentanan internet yang mungkin dipakai untuk kegiatan pencucian uang. Menurut FATF ada tiga faktor yang menimbulkan kerentanan tersebut yaitu:

a. ease of access to account through the internet;
b. absence of face to face transactions between the online bank and the customer;
c. the immediacy of electronic transactions.

Masalah ini menjadi semakin rumit karena beberapa server tidak menggunakan*"log files"* untuk dapat melacak asal dari komputer yang melakukan

[14]Alert Global Media, Inc., FATF Experts sepouse strict laundering controls for cyberbanking. An article from the April 2000 issue of Money Laundering Alert. http://www.moneylaundering.com

transaksi tersebut, sehingga *internet protocol number* dari server yang bersangkutan dan tanggal serta waktu terjadinya hubungan tidak dapat disimpan dalam *electronic file*. Akar dari transmisi-transmisi tersebut disimpan secara pribadi dan praktis tidak mungkin dilacak.[15]

[15]Ibid.

BAB III

TUJUAN DAN MANFAAT PENELITIAN

A. Keaslian Penelitian

Buku tentang *Money Laundering* pernah ditulis oleh Prof.Dr. Sutan Remy Syahdeini, berjudul "Seluk Beluk Tindak Pidana Pencucian Uang dan Pembiayaan Terorisme" Tahun 2007, dan beberapa penulis lain Namun, penelitian ini menitik beratkan pada *electronic money* potensinya sebagai sarana pencucian uang sehingga secara spesifik menganalisis tentang korelasi antara Undang-Undang No. 25 Tahun 2003 tentang Tindak Pidana Pencucian Uang dengan electronic money dan potensi-potensi kerawanan didalamnya. Dalam penelitian yang berjudul : Problematika Hukum Perkembangan *Electronic Money* dalam Kerangka Pencegahan Pencucian Uang Menurut Undang-undang No. 25 Tahun 2003, menganalisis secara komprehensif perkembangan electronic money, praktek pencucian uang dan problematika hukumnya bagi UU No. 25 Tahun 2003. Implikasi-implikasi serta urgensi reinterpretasi beberapa Pasal dalam UU No. 25 Tahun 2003 untuk mengantisipasi pesatnya perkembangan *electronic money*, menjadi fokus utama. Isu-isu hukum yang muncul adalah masalah yurisdiksi, obyek *electronic money* yaitu *cyber money* mealui sarana-sarana transaksi perbankan, undang-undang tersebut apakah dapat menyelesaikannya. Berbagai kasus telah terjadi di Indonesia yang mendorong untuk dilakukannya reinterpretasi berbagai Pasal dalam UU itu.

Berlakunya UU No. 25 Tahun 2004 yang ketika diundangkannya relatif masih baru, pada saat itu seharusnya dapat mengantisipasi perkembangan electronic money karena pada saat diundangkannya juga sedang berkembang

praktek-praktek pencucian uang melalui *cybermoney*. Kondisi ini menurut Myrdal, menunjukkan bahwa negara Indonesia adalah negara *soft state* yang cenderung menciptakan undang-undang yang cacat[16]. Hal ini jelas terlihat dengan undang-undang yang tidak ditujukan untuk mengantisipasi perkembangan ke depan. Oleh karena itu UU No. 25 Tahun 2004 terbuka kesempatan untuk dianalisis dari sisi *ius constitutum* yang meliputi analisis bahan hukum, metode dan kritik ideologikal terhadap hukum[17], dalam hal ini antisipasi terhadap praktek pencucian uang menggunakan sarana electronic money.

B. Manfaat Hasil Penelitian

1. Penelitian ini diharapkan memberikan alternatif solusi atas isu-isu hukum atas Undang-Undang No. 25 Tahun 2003 dengan berkembangnya transfer dana dengan menggunakan *E-money* yang berpotensi digunakan untuk tindak pencucian uang hasil suatu kejahatan;
2. Bahwa transaksi-transaksi melalui *online* dengan pembayaran melalui *cybercash* telah terbukti meningkatkan kinerja perusahaan-perusahaan secara luar biasa dari sisi efisiensi dan efektifitas serta bagi konsumen atau nasabah juga searah dengan hal itu. Namun, disisi lain penyalahgunaan sarana teknologi informasi tersebut berpotensi besar, sehingga diperlukan sarana hukum yang memadai atau setidak-tidaknya apabila peraturan perundangan tidak dapat mengikuti, diperlukan interpretasi hukum atas suatu peraturan perundangan. Penelitian ini diarahkan untuk menganalisis hal itu sebagai jalan pintas mengisi kekosongan hukum.

---

[16] Gunar Myrdal, 1970, h.219-220.

[17] Arief Sidharta, Bernard, **Refleksi Tentang Struktur Ilmu Hukum**, Mandar Maju, Bandung, 1999, h.122.

C. Tujuan Penelitian

Fungsi hukum untuk pengembangan teknologi informasi (internet) sehingga bermanfaat bagi sebesar-besarnya kesejahteraan manusia mempunyai arti penting. Maka dalam penelitian yang mengkaji permasalahan penggunaan electronic money yang semakin meningkat karena ditawarkan oleh bank-bank dunia melalui jasa internet banking (*electronic banking* atau *cyberbanking*) sekaligus telah meningkatkan pula pencucian uang. *Wire transfers system* memungkinkan organisasi-organisasi kejahatan maupun bisnis yang sah dan nasabah-nasabah perbankan yang sah untuk memindahkan dengan cepat dana dari rekening (*account*) mereka dari satu bank ke bank lain ke seluruh dunia. *Cyberlaundering* menjadi marak karena sarana *electronic money* memungkinkan untuk itu. Maka penelitian ini bertujuan mencari *sinergi* fungsi hukum instrumen-instrumen hukum UU No. 25 Tahun 2003 dan konvensi-konvensi internasional disatu sisi dan perkembangan *electronic money* disisi lain. Dalam hal ini maka dikaji dan diamati perkembangan kebijakan hukum dan peraturan yang melingkupi money laundering meliputi: peraturan mengenai pencucian uang serta studi perbandingan berbagai peraturan mengenai pencucian uang di level internasional. Penelitian ini juga bertujuan untuk mengidentifikasi dan mendiskripsikan prospek *electronic money* dan permasalahan hukum yang muncul sehubungan dengan kemampuan yang terbatas UU No. 25 Tahun 2003 serta alternatif penyelesaian permasalahan tersebut.

Disamping itu, penelitian ini dimaksudkan sebagai pengembangan ilmu hukum khususnya yang berkaitan dengan hukum teknologi informasi/hukum cyber khususnya transfer dana melalui *electronic money* yang bagi Indonesia sebagai

area yang belum dikerjakan dengan maksimal, padahal era sekarang adalah era informasi dan komunikasi. Undang-undang No. 25 Tahun 2003 yang merupakan revisi Undang-undang No. 15 Tahun 2002 dimaksudkan untuk mengikuti standar internasional yang berjumlah 40 oleh FATF, namun, undang-undang ini tidak antisipatif terhadap perkembangan electronic money. Oleh karena itu interpretasi terhadap berbagai pasal dalam UU No. 25 Tahun 2003 bertujuan utuk menangkal kejahatan yang ditimbulkan oleh pelanggaran melalui internet khususnya transfer dana secara elektronik, sehingga penelitian ini diharapkan sebagai salah satu instrumen input UU No. 25 Tahun 2003 untuk mencegah penyalang gunaan electronic money yang secara efektif dan efisien sedang berkembang serta disukai oleh pebisnis untuk dijadikan sarana pencucian uang.

D. Kontribusi Penelitian

Penelitian ini diharapkan dapat memperoleh hasil yang bermanfaat bagi kemungkinan perbaikan/revisi UU No. 25 Tahun 2003 tentang Tindak Pidana Pencucian Uang pasca berkembangnya *electronic money* berkenaan dengan diduga dan diindikasikan semakin meningkatnya cyberloundering yang berkarakter berbeda dengan berkembangnya hukum di suatu negara karena hukum tidak dapat berkembang sedinamis transaksi-transaksi online. Kecenderungan terjadinya pelanggaran melalui penyalahgunaan transaksi-transaksi *online* melalui *E-com* yang semakin meningkat karena tidak memadainya perlindungan hukum dan lemahnya perangkat hukum yang menyelesaikan pelanggaran di dalam transaksi online, membutuhkan kebijakan hukum yang memadai dan menyimpang dari fungsi hukum yang konvensional. Disatu sisi transaksi melalui E-com dimaksudkan untuk menghindari hambatan-

hambatan yang terjadi seperti halnya pada transaksi konvensional misalnya masalah kecepatan negosiasi, proses pelaksanaan kontrak, levering barang sehingga terjadi suatu akselerasi dalam penyelesaian pelaksanaan kontrak, namun disisi lain, transaksi online menumbuhkan masalah hukum baru.

Bagi perkembangan ilmu pengetahuan adalah untuk memberikan keluasan wawasan dan pendalaman pemahaman tentang perkembangan transaksi *online* dan bagaimana UU No. 25 Tahun 2003 tentang Tindak Pidana Pencucian Uang seharusnya meng-*cover* perkembangan tersebut. Maka, perbaikan-perbaikan terhadap undang-undang tersebut mutlak diperlukan untuk mengantisipasi dan memberikan fungsi fasilitatif suatu peraturan dalam perkembangan binsis *online* melalui E-bank pada khususnya atau *Electronic Business* pada umumnya. Hukum Indonesia sangat ketinggalan bila dibandingkan dengan negara-negara tetangga (seperti misalnya: Singapura, Malaysia, Philipina) khususnya dalam mengantisipasi perkembangan transaksi-transaksi *online* ini.

BAB IV

METODE PENELITIAN

A. Tipe Penelitian

Penelitian ini diarahkan untuk menganalisis asas-asas hukum yang menjadi dasar bagi sahnya dan berkembangnya transaksi *online* dan *electronic money*. Namun sehubungan dengan maraknya pelanggaran pencucian uang, *electronic money* mempunyai potensi besar menjadi sarana untuk digunakan sebagai pencucian uang melalui *cyberloundering*. Melalui pendekatan dogmatik hukum dan teori hukum. Problematika hukum tersebut dianalisis sehingga didapatkan paradigma baru untuk pencegahan *cyberlaundering*. Dogmatik hukum menggunakan metode normatif, sedangkan teori hukum menggunakan metode normatif pula dengan disinggung tentang kondisi dalam praktek hukum melalui pendekatan sosio-legal.

Fungsi dogmatik hukum digunakan untuk diskripsi, sistematisasi dan sinkronisasi terhadap aturan hukum yang berhubungan dengan pengaturan transaksi *online* dan *electronic money* dan pelanggaran pencucian uang yang difokuskan pada UU No. 25 Tahun 2003 tentang Pencucian Uang dan bahan-bahan hukum yang sama dari negara-negara yang menjadi negara pembanding yaitu AS dan Singapura untuk menemukan persamaan dan perbedaan dalam pengaturan hukumnya.

Teori hukum digunakan untuk menganalisis pengaturan dan implementasi doktrin-doktrin serta asas-asas hukum universal yang dimaksudkan untuk menciptakan pengaturan *money loundering* dalam *electronic money* yang globalistik sehingga diperlukannya harmonisasi dan unifikasi hukum. Oleh karena

electronic money mempunyai sifat yang *boderless* dan *paperless* maka bantuan teori hukum sebagai ilmu eksplanasi yang berkarakter interdisipliner sehingga dapat digunakan disiplin ilmu teknik informatika untuk eksplanasi hukum.

B. Pendekatan Masalah

Sehubungan dengan tipe penelitian yuridis normatif maka pendekatan yang dilakukan adalah pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*) dan pendekatan perbandingan (*comparative approach*). Pendekatan perundang-undangan dilakukan untuk menganalisis UU No. 25 Tahun 2003 tentang Pencucian Uang serta peraturan yang terkait sehingga memungkinkan pencegahan *cyberloundering* dikaitkan dengan Konvensi yang berkaitan dengan *moneyloundering*. Pendekatan konseptual digunakan untuk menganalisis konsep-konsep *electronic money* dan *moneyloundering* yaitu apakah *moneyloundering* dapat dicegah atau setidaknya diminimalisir melalui atau menggunakan UUTPP yang mempunyai spesifikasi-spesifikasi dan keterbatasan sehingga diharapkan tidak terjadi ambiguitas dan tercipta aturan yang memfasilitasi *electronic money*. Sedangkan pendekatan komparatif dimaksudkan untuk mendalami bagaimana dengan pengalaman negara lain mengantisipasi perkembangan *cyberloundering*.

C. Bahan Hukum

1. Bahan hukum primer yakni bahan hukum yang terdiri dari aturan hukum yang diurut berdasar hirarki peraturan perundang-undangan yang berlaku di Indonesia serta bahan hukum asing sebagai bahan pembanding sehingga ditemukan kecenderungan variasi penggunaan arbitrase online yang membantu untuk pertimbangan hukum yang bersifat *ius constituendum*.

2. Bahan hukum sekunder adalah bahan hukum yang diperoleh dari *texbooks*, jurnal-jurnal ilmiah baik dalam negeri maupun luar negeri, pendapat-pendapat para ahli hukum/doktrin, jurisprudensi dan atau kasus-kasus hukum, hasil-hasil penelitian ilmiah atau pertemuan-pertemuan ilmiah para ahli hukum terkait dengan pembahasan arbitrase *online* dan arbitrase pada umumnya.
3. Bahan hukum tersier adalah bahan hukum yang diperoleh sebagai pentunjuk atau penjelasan yang cukup bermakna terhadap bahan-bahan hukum primer dan sekunder, misalnya seperti kamus-kamus hukum, ensiklopedi, manual-manual, model-model hukum, dan lain-lain.

D. Prosedur Pengumpulan Bahan Hukum

Bahan-bahan hukum primer dan sekunder, dikumpulkan, disistematisir, diklasifikasikan dengan sistem kartu dan atau juga menggunakan sistem bola salju kemudian dikaji secara komprehensif sehingga diharapkan mendapatkan suatu pemahaman (*verstehen*) dan pemecahan atas isu-isu hukum di bidang teknologi internet karena kompleksitas masalah hukum yang ada dalam perkembangan arbitrase online.

E. Pengolahan dan Analisis Bahan Hukum

Bahan-bahan hukum yang berasal dari peraturan-perundangan, *lex mercatoria, lex informatica,* studi kepustakaan, diuraikan, dihubungkan sehingga membentuk pemahaman dan pendalaman dalam alur logika hukum. Pengolahan bahan hukum dengan menggunakan metode logika deduktif yakni menarik kesimpulan dari situasi permasalahan yang bersifat umum terhadap permasalahan yang bersifat konkrit. Selanjutnya bahan-bahan hukum yang ada dianalisis untuk melihat pola kecenderungan *cyberloundering* dibandingkan dengan *money loundering* yang konvensional tersebut sehingga pelanggaaran

cyberloundering dapat dicegah dengan menggunakan instrumen hukum yang ada yaitu UU No. 25 Tahun 2003 tentang Pencucian Uang serta peraturan yang terkait serta Konvensi yang berkaitan dengan *money loundering*

F. Pertanggungjawaban Sistematika

Penelitian ini disusun berdasarkan sistematika yang terbagi dalam enam bab. Masing-masing bab terdiri dari sub-sub bab guna lebih memperjelas ruang lingkup dan cakupan permasalahan yang diteliti. Adapun urutan dan tata letak masing-masing bab serta pokok-pokok pembahasannya adalah sebagai berikut.

1. Bab I (Pendahuluan) berisi uraian latar belakang masalah munculnya problematika hukum implementasi UU No. 25 Tahun 2003 tentang Arbitrase Tindak Pidana Pencucian Uang sehubungan dengan berkembangnya penggunaan electronic money untuk cyberlaundering akibat bertumbuhnya transaksi-transaksi online. Selanjutnya ditentukan rumusan masalah yang menentukan arah penelitian dan ruang lingkup pembahasannya.
2. Bab II menguraikan kajian pustaka tentang electronic money pada umumnya dan berkembangnya penggunaan teknologi online untuk dimanfaatkan untuk tindak pelanggaran cyberlaundering yang berpotensi untuk sulit terlacak. Ditegaskan bahwa pencegahan cyberlaundering menemukan masalah karena sifatnya yang borderless dan paperless anonim, transaksi bisa dilakukan dimanapun juga dan dikirm kemanapun juga sepanjang teknologi tersebut sudah ada sehingga sulit terlacak dengan pengaturan hukum yang sudah ada.
3. Bab III menguraikan tentang jaminan keaslian penelitian bahwa penelitian ini adalah murni hasil karya sendiri tanpa plagiat, pengutipan dilakukan dengan menunjuk sumber yang jelas, penekanan penelitian yang jelas, tujuan penelitian dilakukan yaitu untuk pengembangan ilmu pengetahuan dengan

memecahkan permasalahan cyberlaundering yang mendasarkan pada UU No. 25 Tahun 2008, serta kontribusi penelitian adalah untuk penyempurnaan atau revisi peraturan perundangan yang berlaku.

4. Bab IV tentang metode penelitian yang kualifikasinya sebagai yuridis normatif dengan pendekatan *statute approach, comparative approach* dan *conceptual approach*. Semua bahan-bahan hukum dianalisis dengan metode logika deduktif. Karena bersangkutan dengan teknologi informatika maka penelitian ini juga interdisipliner dalam analisisnya.
5. Bab V merupakan analisis terhadap permasalahan yang diteliti yaitu dengan pendekatan statute approach UU No.25 Tahun 2003 dianalisis untuk menunjukkan interpretasi hukum yang dapat dilakukan berkenaan dengan berkembangnya e-money dan cyberlaundering, perbandingannya dengan negara AS dan Kanada, serta perkembangan internasional yang merupakan kecenderungan harmonisasi dan unifikasi hukum sehubungan dengan lembaga-lembaga yang menangani cyberlaundering; Analisis permasalahan yurisdiksi dan keamanan serta pencegahan cyberlaundering
6. Akhirnya, dalam Bab VI dikemukakan rangkuman dari penelitian dan analisis bab-bab terdahulu dapat suatu kesimpulan mengenai perlunya revisi UU No. 25 Tahun 2003 di Indonesia dengan mengikiti perkembangan internasional atau global dibidang e-money yang berpotensi untuk cyberlaundering. Saran yang disampaikan merupakan bentuk sumbangan pemikiran ilmiah yang diharapkan dapat memberikan masukan untuk integrasi kebijakan hukum secara global atau kekurangan hukum terhadap peraturan perundangan yang berlaku melalui interpretasi hukum .

BAB V

ANALISIS PENELITIAN

A. Implementasi UU No. 25 Tahun 2003 Dengan Berkembangnya *Electronic Money* Untuk Mencegah Tindak Pencucian Uang

Money laundering menjadi isu yang semakin penting dan menjadi cara melakukan pelanggaran yang meresahkan akhir-akhir ini, terlebih dikaitkan dengan isu terorisme. Dalam beberapa report PPATK, kepolisian dan Interpol mengindikasikan bahwa jaringan maupun tindakan terorisme mendapatkan dana yang sangat besar untuk membeayai kegiatan mereka dengan cara melakukan pencucian uang. Organisasi teroris sangat bergantung pada hasil sumber kejahatan yang menghasilkan uang, misalnya perdagangan gelap narkotika, penyelundupan barang dalam jumlah besar, dan kejahatan keuangan antara lain pemalsuan kartu kredit. *Money laundering* telah dikenal sejak tahun 1930 di Amerika Serikat. Saat itu kejahatan *money laundering* dilakukan oleh organisasi mafia melalui pembelian perusahaan-perusahaan pencucian pakaian (*Laundry*) yang kemudian digunakan oleh organisasi tersebut sebagai alat untuk pencucian uang yang dihasilkan dari kegiatan *illegal* atau hasil kejahatan sehingga menjadi uang yang sah. Indikasi dari pencucian uang paling banyak berasal dari pengedaran narkoba dan kejahatan keuangan. Bahkan kegiatan pencucian uang tersebut, berkaitan erat dengan tindak pidana korupsi, sehingga saling melengkapi, menyatu dan kejahatan seperti ini menjadikan pola kejahatan semakin nisbi.

Kasus Arthur H. Samish di California, Amerika Serikat merupakan contoh yang konkrit dimana berbagai modus kejahatan dilakukan. Arthur H. Samish adalah seorang pengusaha bir di California dan ladang perminyakan di Indiana

dan Texas, AS, yang dapat menghindar dari penyelidikan pajak, sebagai agen pengumpul dana untuk membeayai kampanye dan kegiatan yang menyangkut persoalan kenegaraan dan ia dikenal sebagai seorang lobbies di Parlemen California sejak tahun 1938. Menilik bahwa *money laundering* dikenal sejak tahun 1930, besar kemungkinan, apa yang dilakukan berkaitan dengan *money laundering* juga, karena melalui berbagai segmen kegiatan usaha mulai dari perusahaan bir, penyelundupan pajak, usaha illegal lain seperti obat bius dan peran sebagai lobbies yang mempunyai kekuatan untuk menggarap persoalan kenegaraan yang dapat berpengaruh kepada tugas kegiatan referendum, pemilihan calon senator dan anggota dewan perwakilan serta dapat mengendalikan pegawai jawatan pajak untuk bekerjasama menggelapkan pajak perusahaan. Diketahui pula bahwa pada bulan Mei 1950, ia menerbitkan selebaran pungutan dana dan mengeluarkan lembaran cek senilai @ $ 10.000 dan $ 40.000 yang diberikan kepada komite kampanye.[18] Kegiatan ini sangat merugikan negara, mengobrak-abrik demokrasi yang sangat diagungkan di AS dan sistem keuangan AS sehingga dituntut melanggar *"Federal Corrupt Practice Act"*, karena tindakan yang ia lakukan meliputi berbagai kejahatan korupsi di bidang politik, ekonomi, keuangan dan sosial.

Di Indonesia diyakini bahwa sumber utama dari uang yang dicuci berasal dari tindak pidana, yang berakar dari penyelundupan dan berasal dari pengedaran narkoba, prostitusi, judi dan korupsi. Penyelundupan merupakan sumber pelanggaran yang paling sering terjadi karena Indonesia adalah merupakan Negara yang terbuka bagi kegiatan penyelundupan karena luas daerah, pegawai beacukai yang korup, sarana/prasarana yang sangat terbatas

[18]Roesli DMB, The Kefauver Committee Report on Organized Crime, by Senator Ertes Kefauver, Didier Publisher, New York, 1952, p.131-138.

> market and globalization of organized crime have led to a collective raised awareness with regard to the problem of money laundering.

Dari definisi tersebut nampaklah bahwa *money laundering* adalah suatu kegiatan yang sama tuanya dengan kejahatan itu sendiri, karena melekat dengan penjahat yang menginginkan uang hasil kejahatannya tersebut harus aman dan masuk secara wajar dalam sistem perekonomian suatu Negara dan hubungan internasional yaitu dengan cara mencuci uangnya tersebut untuk dimasukkan dalam sirkulasi ekonomi. Pencucian uang tersebut dengan cara melalui suatu sasaran operasi, yang mana pada umumnya berlangsung dalam beberapa langkah, yaitu atas suatu asset dan/atau modal yang secara tidak sah diperoleh nampak seolah-olah mereka diperoleh dari suatu sumber sah, dan memasukkan/menyisipkan asset/modal tersebut ke dalam peredaran ekonomi. Perbankan Swiss dalam hubungan perbankan internasional dikenal sebagai sorga bagi para pencuci uang. Hal ini dapat dilihat dalam kutipan sbb:[20]

> Due to its stability, the quality of services offered and its bank secrecy, the Swiss financial hub, like other foreign financial market places, was used by criminals who wished to shield money generated by their illegal activities.

Namun, dunia perbankan sekarang tidak lagi menjadi tempat aman untuk menyimpan uang hasil *money laundering*. Hakim dapat memerintahkan untuk membuka rekening seseorang atau badan hukum bila diperlukan untuk penyelidikan melalui forum pengadilan. Oleh karena itu para pencuci uang mengalihkan perhatian pada investasi berbagai kegiatan ekonomi dan yang

[20] Ibid.

penting uang hasil kejahatannya secara aman masuk dalam sirkulasi ekonomi suatu negara. Hal ini dapat dijelaskan melalui kutipan sbb:[21]

> "The banks are not the only pawn used to conceal the criminal origin of capital assets. Since all bank transactions can be reconstituted and the criminal judge can conduct investigations on them, they are not particularly suited for money laundering. That is why money launders tend to operate through fictive companies, casinos, restaurants, jewelry stores, car dealers and art agents, as well as import-export operations."

Oleh karena itu maka dalam skema pelanggaran pencucian uang tersebut meliputi segmen yang sangat luas karena hampir semua potensi investasi yang dapat dimasuki dan secara aman dapat digunakan untuk memasukkan uang hasil kejahatan akan digunakan oleh para pencuci uang. Hal ini mengingat bahwa kejahatan/pelanggaran pencucian uang digunakan oleh para penjahat yang mempunyai jaringan luas bahkan global, mempunyai teknologi, mempunyai tenaga ahli dari berbagai bidang sehingga kelengkapan itu menimbulkan kompleksitas masalah yang kadang bahkan sering aparat penegak hukum akan selalu ketinggalan dengan kinerja yang mereka lakukan karena kebebasannya dalam menggunakan infrastruktur yang dimiliki, system jaringan yang rapi. Aparat penegak hukum sendiri mempunyai keterbatasan yang mencolok seperti mereka dibatasi oleh hukum yang harus dipatuhi, hukum yang memiliki keterbatasan untuk berlakunya ataupun kadang tidak lengkap, yurisdiksi Negara, kelengkapan teknologi yang sangat terbatas. Di Kanada, *money laundering*

[21] Ibid.

mempunyai pengertian agak berbeda karena tidak hanya transfer tetapi juga konfersi yaitu sbb:[22]

> "Money laundering is the conversion or transfer of property, knowing that such property is derived from criminal activity, for the purpose of concealing the illicit nature and origin of the property from government authorities.
>
> Any crime that generates significant profit - extortion, drug trafficking, arms smuggling and some kinds of white collar-crime - may create a "need" for money laundering."

Pada umumnya, dalam melakukan pencucian uang, metode yang dapat digunakan untuk melakukan *money laundering* dapat dijelaskan sbb:[23]

> "Money Laundering Methods:
> a) **Structuring ("smurfing")**: Smurfing is possibly the most commonly used money laundering method. It involves many individuals who deposit cash into bank accounts or buy bankdrafts in amounts under $10,000 to avoid the reporting threshold.
> b) **Bank Complicity**: Bank complicity occurs when a bank employee is involved in facilitating part of the money laundering process. Bank complicity is becoming increasingly difficult for criminals to use following the introduction of the Canadian Bankers Association's policy, procedures and training (see Canadian Bankers Association).
> c) **Money Services and Currency Exchanges**: Money services and currency exchanges provide a service that enables individuals to exchange foreign currency that can then be transported out of the country. Money can also be wired to accounts in other countries. Other services offered by these businesses include the sale of money orders, cashiers cheques, and travellers cheques.

---

[22]Department of Justice Canada, Solicitor General Canada, **ELECTRONIC MONEY LAUNDERING: An Environmental Scan,October, 1998, p.1.**

[23]The Royal Canadian Mounted Police, Proceeds of Crime Branch, **Money Laundering - A Preventive Guide, *A Preventive Guide for Small Business & Currency Exchanges in Canada* 2006, p.1.**

d) **Asset Purchases with Bulk Cash:** Money launderers may purchase high value items such as cars, boats or luxury items such as jewelry and electronics. Money launderers will use these items but will distance themselves by having them registered or purchased in an associate's name.

e) **Electronic Funds Transfer:** Also referred to as a telegraphic transfer or wire transfer, this money laundering method consists of sending funds electronically from one city or country to another to avoid the need to physically transport the currency.

f) **Postal Money Orders:** The purchase of money orders for cash allows money launderers to send these financial instruments out of the country for deposit into a foreign or offshore account.

g) **Credit Cards:** Overpaying credit cards and keeping a high credit balance gives money launderers access to these funds to purchase high value items or to convert the credit balance into cheques.

h) **Casinos:** Cash may be taken to a casino to purchase chips which can then be redeemed for a casino cheque.

i) **Refining:** This money laundering method involves the exchange of small denomination bills for larger ones and can be carried out by an individual who converts the bills at a number of different banks in order not to raise suspicion. This serves to decrease the bulk of large quantities of cash.

j) **Legitimate Business / Co-mingling of Funds:** Criminal groups or individuals may take over or invest in businesses that customarily handle a high cash transaction volume in order to mix the illicit proceeds with those of the legitimate business. Criminals may also purchase businesses that commonly receive cash payments, including restaurants, bars, night clubs, hotels, currency exchange shops, and vending machine companies. They will then insert criminal funds as false revenue mixed with income that would not otherwise be sufficient to sustain a legitimate business.

k) **Value Tampering:** Money launderers may look for property owners who agree to sell their property, on paper, at a price below its actual value and then accept the difference of the purchase price "under the table". In this way, the launderer can, for example, purchase a $2 million dollar property for $1 million, while secretly passing the balance to the seller. After holding the property for a period of time, the launderer then sells it for its true value of $2 million.

l) **Loan Back:** Using this method, a criminal provides an associate with a sum of illegitimate money and the associate creates the paperwork for a loan or mortgage back to the criminal for the same amount, including all of

> the necessary documentation. This creates an illusion that the criminal's funds are legitimate. The scheme's legitimacy is further reinforced through regularly scheduled loan payments made by the criminal, and providing another means to transfer money."

Segmen yang luas metode pencucian uang sampai dengan *electronic money*, memberikan peluang semakin sulitnya pelacakan dan pencegahan pencucian uang karena sifat *borderless* dan *paperless*, tidak mengenal waktu, sifat anonimitas pola kerja transaksi *online*. Apabila definisi *electronic money* diartikan sebagai:[24]

> "By its decentralized, distributive nature, electronic money has the same potential for transforming economic structure as personal computers did for overhauling management and communications structure."

Maka, sistem keuangan sedang memunculkan suatu nilai ekonomi untuk diwakili secara digital oleh pola kerja elektronik. Ini yang dikatakan sebagai uang elektronik atau *e-money*, dapat ditukar melalui penggunaan 'kartu cerdas' (smards card) yaitu ATM dan sejenisnya atau transaksi pembayaran melalui internet atau *online*. Tidak sama dengan kartu dimana nilai disimpan, *e-money* dapat lewat dengan seketika antara kedua transaksi *on-line*, tanpa kebutuhan akan suatu perantara (e.g., e-cash [oleh/dengan] Digicash Inc.). *E-Money* akhirnya diharapkan untuk bekerja secara baru menggantikan atau setidaknya sebagai alternatif yang efisien dan efektif atas uang kertas, risiko relative kecil, tidak menyenangkan dalam hal beaya dihubungkan dengan penanganan, mengatur dan melindungi mata uang tradisional.

---

[24]Birch, Dave & Neil McEvoy. "DIY Cash."***Wired Magazine*, 2, April, 1996"**, 1996, p.-

Kegiatan transfer dana itu sendiri saat ini banyak dilakukan dengan menggunakan teknologi, semacam *wire transfer*, ATM, dan masih banyak lagi. Bahkan saat ini metode transfer dana yang banyak digunakan karena sangat cepat adalah dengan menggunakan RTGS (*Real Time Gross Settlement*).

Transfer dana seperti tersebut di atas, menciptakan kejahatan baru yaitu bahwa transfer dana itu digunakan untuk sarana pencucian uang. Dugaan ini merupakan cara logika yang digunakan untuk mencegah bahkan mengantisipasi *money laundering*. Terdapat kesulitan yang cukup untuk memberikan bukti adanya *electronic money laundering* seperti uraian sbb:[25]

> "What does e-money mean for the money launderer?
>
> E-money laundering is thought to be negligible, for now:
> To date, G-10 countries have not seen evidence of this activity in connection with electronic money products; if such products come to be used on a large scale, it is conceivable that criminals may seek to explore their potential for transferring illicit funds.
>
> Indeed, criminals are always looking for "a new type of detergent which allows for cleaner laundry"[26].
>
> They have been quick to exploit each new method of financial transfer. In the 1980s and 1990s wire transfers became a popular method for moving money in both the legal and illegal sectors. By 2000 we may see the same situation with e-money.[27]"

Penyalahgunaan *e-money* untuk pencucian uang menjadi suatu masalah penting di masa datang sebab system *e-money* sebagai alat pencucian uang karena dua pertimbangan: (a). transaksi-transaksi boleh jadi tidak bisa terlacak

---

[25]"G7 Groups Frets Over Electronic Money Laudering." The Nando Times. 6 Feb. 1997, **http://www.nando.net/newsroom/ntn/info/020697/info8_2320.html.**

[26]Bortner, R. Mark. "Cyberlaundering: Anonymous Digital Cash and Money Laundering." 1996. University of Miami Law School, **http://www.ovnet.com/~dckinder/documents/cyberlaunder.htm**

[27]Department of Justice Canada, Solicitor General Canada, **Opcit,** p.6.

(*transactions may become untraceable*); dan (b). transaksi mobilitasnya tidak dapat dibayangkan karena kecepatannya (*transactions are incredibly mobile*). Profil tidak terlacaknya suatu transaksi *online* dan mobilitas uang yang ditransaksikan dapat dijelaskan sbb:[28]

> **Untraceability**
> The use of e-money systems will mean fewer face-to-face financial transactions. The anonymity of e-money will make "knowing your customer" much more difficult.
> E-money systems also allow the parties to the transaction to deal with each other directly, without the assistance of a regulated financial institution. Thus, there may not be a traditional audit trail.

Electronic Money yang mempunyai cirikhas yaitu sifat anonimitas dan bisa melakukan hubungan langsung tanpa bantuan lembaga keuangan perbankan sehingga dapat dikirim dimanapun di dunia maupun dana bisa datang dari manapun di dunia ini, menjadikan tidak berartinya hokum konvensional yang mengatur tentang bagaimana memonitor atau mengenal seorang nasabah. Maka, Peraturan Bank Indonesia No: 5/21/PBI/2003 Tentang Perubahan Kedua Atas Peraturan Bank Indonesia Nomor 3/10/PBI/2001 Tentang Penerapan Prinsip Mengenal Nasabah (*Know Your Customer Prinsiples*), khususnya Pasal 9 sbb:

> "(1) Bank wajib memiliki sistem informasi yang dapat mengidentifikasi, menganalisa, memantau dan menyediakan laporan secara efektif mengenai karakteristik transaksi yang dilakukan oleh Nasabah Bank.
> (2) Bank wajib melakukan pemantauan atas transaksi yang dilakukan oleh Nasabah Bank, termasuk mengidentifikasi terjadinya Transaksi Keuangan Mencurigakan."

terasa tidak terlalu berfungsi lebih-lebih saat ini, metode transfer dana yang banyak digunakan sangat cepat berfungsinya untuk eksekusi suatu transaksi-transaksi dana yang besar yaitu dengan menggunakan RTGS (*Real Time Gross*

[28]**Ibid.**, p.9.

Settlement). Kecepatan transaksi dan transfer uang yang datang darimanapun di dunia dan transfer ke manapun di dunia, sekarang sudah menggunakan hitungan detik/*second* sehingga uang sekarang menjadi tanpa kebangsaan karena begitu tinggi pergerakannya, dan "mampir" di suatu Negara untuk mendapatkan suatu keuntungan rente atau sejenisnya. PBI No: 5/21/PBI/2003 lebih tepat hanya digunakan untuk transaksi-transaksi konvensional bukan untuk *e-money*. Oleh karena itu perlulah diatur secara khusus bagaimana transaksi *e-money* mendapatkan perlindungan hukum dalam arti transaksi melalui *e-money* tersebut Negara tidak dirugikan untuk perbuatan yang tidak bertanggung jawab serta para pengguna mendapatkan perlindungan hak dan kewajibannya menurut hukum bukan untuk digunakan sebagai penyelundupan hukum. Transaksi-transaksi melalui *e-money* akhirnya akan terbentur juga dengan masalah yurisdiksi di *cyber, choice of forum* dan *choice of law*, apabila dilihat dari sisi hukum konvensional.

Mobilitas uang atau dana yang menggunakan *e-money* menunjukkan kompleksitasnya sehingga sangat rentan menjadi sumber pencucian uang, terdapat perbedaan mencolok antara transfer atau transaksi dana di bank konvensional atau lembaga keuangan lainnya dengan transfer atau transaksi dana yang dilakukan dengan menggunakan elektronik atau *online* dan dapat dijelaskan sbb (cetak miring dan garis bawah menjadi penting untuk diperhatikan):[29]

> **"Mobility**
> Hypothetically, *e-money could come from anywhere in the world, and be sent anywhere in the world*. Thus, e-money systems may offer instantaneous transfer of funds over a network that, in effect, *is not subject to any jurisdictional restrictions*.
> The problem may be illustrated by separating the process of money laundering into three basic steps - *placement, layering*

[29]Ibid.

and integration - and then comparing traditional money laundering systems with cyber-systems.

The first step in money laundering is the physical disposal of cash. Traditionally, *placement* might be accomplished by depositing the cash in domestic banks or other kinds of financial institutions. Or the cash might be smuggled across borders for deposit in foreign accounts, or used to buy high-value goods, such as artwork, airplanes, or precious metals and gems, that can then be resold with payment by cheque or bank transfer.

With e-money laundering, cash may be deposited into an unregulated financial institution. Placement may be easily achieved using a smart card or personal computer to buy foreign currency, goods, etc. Powerful encryption may be used to guarantee the anonymity of e-money transactions.

The second step, *layering*, involves working through complex layers of financial transactions to distance the illicit proceeds from their source and disguise the audit trail. This phase traditionally involves such transactions as the wire transfer of deposited cash, the conversion of deposited cash into monetary instruments (e.g., bonds, stocks, travelers' cheques), the resale of high-value goods and monetary instruments, and investment in real estate and legitimate businesses, particularly in the leisure and tourism industries. Shell companies, typically registered in offshore havens, are a popular device in the traditional layering phase. These companies, whose directors are often local attorneys acting as nominees, protect the identity of the real owners. These owners also benefit from restrictive bank secrecy laws and attorney-client privilege

In an electronic-money system, layering can be done through a personal computer. There is usually no audit trail. In addition, e-money systems allow for instantaneous transfer of funds over a system that, in effect, has no borders.

The last step is to make the wealth derived from crime appear legitimate. Traditionally, *integration* might involve any number of techniques, including using front companies to "lend" the money back to the owner or using funds on deposit in foreign financial institutions as security for domestic loans. Another common technique is over-invoicing, or producing false invoices for goods sold - or supposedly sold - across borders.

In e-money laundering the criminal may be able to achieve integration by using a personal computer to pay for investments or to buy an asset, without having to call on the services of an intermediary financial institution.

In short, the temptation of electronic forms of money for the criminal may be the potential for untraceable, mobile wealth."

Menurut *Report on Money Laundering and Terrorist Financing Typologies* 2003-2004 yang dikeluarkan oleh *Financial Action Task Force on Money Laundering* (FATF), salah satu tipologi *money laundering* adalah melalui sistem *wire transfer*. *Wire Transfer* proses berjalannya ada pada setiap transaksi keuangan yang dilakukan oleh seseorang melalui sebuah institusi keuangan dengan menggunakan perangkat elektronik yang menyediakan sejumlah uang untuk seseorang di institusi keuangan lain. *Wire Transfer* meliputi pula transaksi keuangan yang terjadi melewati batas nasional, antara satu negara dengan negara lainnya. *Wire Transfer* adalah cara yang sangat cepat dan efisien untuk memindahkan dana dari satu institusi keuangan ke institusi keuangan lainnya, dari satu negara ke negara lainnya.

Berhubungan dengan analisis di atas, kemajuan dalam teknologi sistem pembayaran ini, saat sekarang memiliki dua dampak yang terkait dengan potensi penyalahgunaan keuangan yaitu *money laundering*. Di satu sisi, sistem pembayaran elektronik menyediakan keamanan yang lebih besar untuk transaksi dengan mengizinkan kemampuan yang lebih besar untuk melacak transaksi individu melalui catatan elektronik yang terbuat secara otomatis. Disisi yang lain, kemajuan ini, juga menciptakan karakteristik yang mungkin menarik bagi pelaku pencucian uang untuk berbagai jenis kegiatan kejahatan yang bersifat transnasional. Kejahatan ini dapat dilakukan oleh semua orang yang mempunyai kemampuan teknologi ini, tidak hanya terbatas pada teroris, sindikasi perdagangan illegal seperti obat bius, uang palsu, minuman keras, perjudian, dan lain-lain. Sebagai contoh, volume *wire transfer* yang meningkat, seiring dengan kurangnya pendekatan yang konsisten dalam pencatatan informasi kunci

dalam transaksi semacam itu, dalam menyimpan catatan tersebut dan dalam menyampaikan informasi yang penting dalam transaksi tersebut, merupakan sebuah hambatan untuk memastikan transaksi tersebut dapat dilacak oleh otoritas yang memiliki kewenangan menyelidiki dari setiap transaksi individu. FATF menyatakan bahwa skema *wire transfer* yang lebih rumit dapat melibatkan *multiple wire transfer* untuk menciptakan jejak transaksi keuangan yang kompleks dan membingungkan dengan tujuan untuk menghindari deteksi. Dan ini mesti akan dilakukan karena kejahatan yang menggunakan teknologi informasi akan selalu didepan perkembangan hukum yang mengatur tentang teknologi informasi. Oleh karena itu, *e-money (e-cash)* mempunyai kekurangan-kekurangan dan potensi bahaya, yang dijelaskan oleh Sutan Remy Syahdeini sbb:[30]

1. Penyimpanan *e-cash* pada PC dapat terancam apabila sistemnya mengalami *crash*;
2. *E-cash* dapat meningkatkan kecemburuan sosial dari masyarakat miskin terhadap masyarakat kaya, karena mereka yang memiliki PC dapat memiliki akses langsung ke sistem *e-cash*, sedangkan mereka yang tidak memiliki PC, yang sebagian besar adalah konsumen yang berpenghasilan sangat rendah, tidak memiliki akses tersebut.
3. Pencucian uang dan penghindaran pajak (*tax evasion*) dapat marak dalam sistem *e-cash* yang tidak berkewarganegaraan (*stateless e-cash system*) karena para penjahat dapat menggunakan *e-cash* yang tidak dapat dilacak untuk menyembunyikan kekayaan mereka.
4. uang-uang tradisional palsu yang berhasil dipakai untuk memperoleh (membeli) *e-cash* akan menyulitkan bagi otoritas pemberantasan pemalsuan uang karena *e-cash* yang diperoleh dari uang-uang tradisional palsu tersebut telah tercampur dengan *e-cash* yang diperoleh dari uang-uang tradisional yang tidak palsu di dalam sistem *e-cash* tersebut.
5. apabila *computer hackers* atau penjahat-penjahat lain berhasil masuk ke dalam sistem *e-cash*, mereka dapat seketika meraup kekayaan elektronik tersebut dalam jumlah ribuan bahkan jutaan dolar milik pemilik *e-cash* yang tidak berdosa. Sistem pengamanan yang baik dapat memberikan perlindungan yang diharapkan oleh para pemilik *e-cash* di dalam sistem tersebut.

[30]Sutan Remmy S, Op,cit., p.61.

6. pertumbuhan sistem *e-cash* dapat menambah beban tugas dari otoritas yang berkewajiban mengawasi sistem keuangan.

Dari sisi teknologi, risiko juga terjadi yang dapat dihadapi oleh setiap para penerbit *e-money (e-money issuers)* yaitu berupa:[31]

- Unauthorized creation, transfer or redemption of e-money (i.e. fraud);
- Incorrect attribution of funds within the system;
- Hardware or software errors leading to loss of e-money value or loss of function of the e-money system; and
- Use of the e-money system for financial crime or as a tool to subvert or misuse financial systems.

Financial Services Authority selanjutnya juga memberikan pedoman bagi para penerbit *e-money* yaitu bahwa penerbit harus memiliki managemen yang sehat dan berhati-hati (*sound and prudent management*), prosedur administrasi dan akunting yang baku (*administrative and accounting procedures*) dan mekanisme kontrol internal yang memadai (*adequate internal control mechanisms*).[32]

Perlulah direkomendasikan bahwa untuk mengantisipasi pengalahgunaan *e-money*, yang perlu dilakukan pengawasan adalah lembaga penerbit yaitu bank dan lembaga keuangan bukan bank oleh otoritas tertentu melalui sistem pelaksanaan Penerapan Prinsip Mengenal Nasabah (*Know Your Customer Prinsiples*) dalam arti luas.

Antisipasi Terhadap Pencucian Uang Menurut Hukum Indonesia

Menghadapi pelanggaran hukum yang kompleks secara global dengan tingkat pergerakan sangat tinggi antar negara yang tiap-tiap negara mempunyai sistem hukum sendiri, sungguh merupakan pelanggaran yang membutuhkan kerjasama internasional antar negara, perlu adanya akselerasi *rechtschepping*, seperti yang dilakukan oleh FATF atau UNCITRAL melalui *uniform laws* atau

[31]Financial Services Authority, Op.cit., p.18.
[32]Ibid.

uniform rules yang dibuat oleh ICC (*International Chamber of Commerce*) dan menjadi pedoman bagi negara-negara untuk melakukan harmonisasi dan sinkronisasi hukum di dunia dan diabsorbsi ke dalam sistem hukum masing-masing negara. FATF juga telah membuat kriteria standar internasional suatu Negara dapat dikategorikan sebagai Negara yang memerangi pencucian uang. Sejak tahun 1990 dan akhirnya direvisi tahun 1996, telah dikeluarkan *Forty Recommendation* yaitu *the basic framework for anti-money laudering efforts* dan sengaja dirancang untuk keberlakuan secara global. Rekomendasi meliputi pemetaan tentang *criminal justice system, law enforcement, financial system* dan *international co-operation*. Di dunia standar ini telah menjadi standar global bagi negara-negara yang menjadi anggota FATF. Dalam konteks *cyberlaundering*, maka kebutuhan semacam ini mutlak karena *cyberlaundering* dapat ditekan karena untuk menghapus *cyberlaundering* jelas tidak mungkin. Setiap negara-negara anggota FATF harus mempunyai komitmen untuk saling mengawasi dan secara kontinu melakukan internal audit dengan teknik yang selalu diubah disesuaikan dengan perubahan.[33]

Tingkat nasional (termasuk Indonesia), salah satu jalan pintas untuk menanggulangi pelanggaran pencucian uang adalah bagaimana hukum Indonesia digunakan untuk pencegahan pencucian uang yang sekarang bersifat sibernetik. Indonesia melalui UU No. 25 Tahun 2003 Pasal 1 angka 8 dijelaskan bahwa transaksi keuangan adalah:

> "Transaksi keuangan yang dilakukan secara tunai adalah transaksi penarikan, atau penitipan yang dilakukan dengan uang

[33]Dijelaskan oleh FATF bahwa: "all member countries have their implementatioans of the Forty Recommendations monitored true two-pronged approach: an annual self-assessment exercise and the more detailed mutual evaluation process under which each member country is subject to an on-site examination. In addition the FATF carries out cross country reviews of measures taken to implement particular Recommendations."

tunai atau instrument pembayaran lain yang dilakukan melalui Penyedia Jasa Keuangan"

Dari definisi tersebut di atas, harus ditafsirkan bahwa transaksi tersebut tidak hanya berupa transaksi dengan menggunakan uang tunai saja, tetapi juga termasuk di dalamnya adalah transaksi-transaksi yang dilakukan dengan menggunakan instrumen pembayaran lain yaitu menggunakan cek, *traveller's ceques, certificate of deposit, ATM, bilyet giro, credit card,* sampai dengan *wire transfer* dan jenis baru dari wire transfer yaitu *multiple wire transfer,* RTGS (*Real Time Gross Settlement*) serta bentuk-bentuk baru transaksi dana yang baru berdasarkan perkembangan teknologi informasi.

Peluang transaksi keuangan yang dibuka meluas seperti dalam Pasal 1 angka 8 tersebut dibatasi dengan Pasal 13 ay. 1 yaitu adanya kewajiban melaporkan transaksi keuangan mencurigakan kepada PPATK dan menyampaikan laporan kepada PPATK tentang transaksi keuangan yang dilakukan secara tunai dalam jumlah kumulatif sebesar limaratus juta rupiah atau lebih atau yang nilainya setara, baik dilakukan dalam satu kali transaksi maupun beberapa kali transaksi dalam satu hari kerja atau transaksi dilakukan dengan valuta asing yang nilainya setara (Pasal 13 ay. 1, huruf b). Pasal 13 ini ternyata kurang lengkap karena tidak mengantisipasi: (1). Perkembangan setoran menggunakan emas (*bullion bank*); (2). Praktik *structuring* atau *smurfing* dengan memecah transaksi keuangan secara tunai yang bertujuan untuk melakukan penyelundupan hukum; (3). Transaksi menggunakan *e-money* yang dapat dilakukan dimanapun dan dikirim kemanapun di dunia sepanjang sarana untuk itu tersedia (*online*). Disamping itu, *e-money* dapat diterbitkan oleh lembaga keuangan yang bukan bank sentral, baik lembaga tersebut berbentuk perbankan atau lembaga bukan

bank.[34] Sekarang terdapat dua mata uang resmi berkenaan dengan berkembangnya *e-money* yaitu mata uang *government currency* dan *private currency*. *E-money* adalah merupakan uang tunai demikian pula *digital money* maka istilah itu disebut juga sebagai *e-cash*. Dikatakan oleh Geoffrey Turk sbb:[35]

> "competition between currencies, whether government or private, is beneficial to everyone in digital economy. The currencies of substance that maintain their value over time and are implemented under a trustworthy and secure computer and communications system will be the one that will circulate and be accepted globally"

E-money telah mengubah citra uang tunai yang dikeluarkan lembaga resmi pemerintah suatu negara yaitu bank sentral. Pengakuan atas suatu uang tunai akhirnya menjadi titik sentral yaitu dalam arti uang tunai tersebut dapat dipercaya dan aman sehingga nilai intrinsiknya dapat terjaga. Sebagai konsekuensi dari *private currency*, negara akhirnya akan mengalami kesulitan menjaga nilai uang karena uang yang secara konvensional diterbitkan oleh bank sentral masing-masing negara telah tercampur dengan berbagai uang tunai hasil dari *e-money* yang masuk melalui transaksi-transaksi perdagangan maupun transaksi-transaksi keuangan lain yang berasal dari *private currency*. Dalam *e-money*, untuk membuktikan uang palsu menjadi sulit. Perkembangan terakhir nampaknya *e-money* sebagai *e-cash* akan selalu menggunakan teknologi informasi yang berkembang pesat tersebut sebagai alat untuk sarana transaksi-transaksi serta alat tukarnya. Goffrey secara tepat memberikan gambaran hal ini karena kecenderungan bisnis memang selalu melekat pada teknologi dan tidak hanya dimasa yang akan datang tetapi sekarang telah terjadi. Ia menguraikannya sbb:[36]

---

[34]Ibid., p.17.

[35]Goffrey Turk, *Money and Currency in the 21st*, dalam http://www.info.goldmoney.com, akses tanggal 22 February 2008.

[36]Ibid.

> The 21st century will not be "cashless", as many now predict. However, it does seem clear that the currency of the 21st century will be "paperless"...The wallet of the future will hold less paper cash, coins, and magnetic stripe cards. It will hold instead smart cards containing digital cash and other financial information, updated - perhaps automatically-by a PDA with a satellite communication link. The question is no longer if this evolution will happen, but when.

Kecenderungan untuk menggunakan *e-money* yang besar itu, memberikan kerawanan yang serius karena teknologi informasi sangat rentan untuk penyalah gunaan dan menjadi alat perlindungan yang aman suatu kejahatan pencucian uang. Pesan-pesan elektronik, *records* ataupun bentuk lainnya sulit dilakukan pelacakan karena hal sbb:

> "...in an electronic environment, the original of a message is undistinguishable from a copy, bears no hand-written signature and is not on paper. The potential for fraud is considerable, due to the ease of intercepting and altering information in electronic form without detection."[37]

Alert Global Media, Inc. mengingatkan bahwa untuk meminimalkan tindak pelanggaran pencucian uang, beberapa pedoman telah dikeluarkan yang intinya bahwa pengenalan terhadap nasabah, standarisasi perbankan, penyempurnaan teknologi untuk melakukan identifikasi dan deteksi aktivitas *online* dan kerjasama global untuk menanggulangi penyelundupan hukum melalui keterbatasan-keterbatasan yurisdiksi masing-masing negara. Alert Global Media mengusulkan hal-hal sbb:[38]

1) Globally consistent Internet banking standards;
2) Technology to assist in customer identification and detection of suspicious online activity;
3) Know Your Customer procedures that include continual monitoring of account activity;

---

[37]UNCITRAL, Working Group on Electronic Commerce Thirty-First session, **Planning of Future Work on Electronic Commerce: Digital Signatures, Certification Authorities and Related Legal Issues**, New York, 18-28 February 1997, p.6.

[38]Alert Global Media, Inc., FATF Experts espouse strict laundering controls for cyberbanking, An article form the April 2000 issue of Money Laundering Alert, **http://www.moneylaundering.com**

4) Laws that restrict internet banking operations to jurisdictions where the bank is licensed.

Berbagai cara teknologi bisa dilakukan untuk meminimalisir *cyberlaundering*. Untuk mengatasi masalah kurangnya atau sulitnya pendeteksian pencatatan atau *recording* dari *wire transfer*, adalah dengan menggunakan *digital signature* atau tanda tangan digital. *Digital signature* adalah:

> "...an electronic substitute for a manual signature that serves the same functions as a manual signatures and more...In more technical terms, a digital signature is the sequence of bits that results from using a one-way hash function to create a message digest of an electronic communication. The resulting message digest is then encrypted using a public-key algorithm and the sender's private key. A recipient who has the sender's public key can accurately determine (1) whether the sequence of bits was created using the private key that corresponds to the signer's public key, and (2) whether the communication has been altered since the sequence of bits was generated."[39]

Di Malaysia dan di Singapura, tanda tangan elektronik mempunyai pengertian yang agak berbeda yang dapat dilihat pada uraian di bawah:[40]

> Menurut *Malaysia Digital Signature Act 1977* [Part I, 2.(1)]:
>
> "digital signature" means a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine -
>
> (a) wether the transformation was created using the private key that corresponds to the signer's public key; and
> (b) wether the message has been altered since the transformation was made.
>
> Menurut *Philipine E-Commerce Act No. 8792, Tahun 2000, Part II, Chapter 1, Sec.5.(e):*
>
> "Electronic signature" refers to any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a

[39]Lorijean G. Oei, dalam Thomas Smedinghoff, J, (ed), **Online Law, The SPA's Legal Guide to Doing Business on the Internet**, Addison-Wesley Publishing Company, Inc., Canada, 1999, p.43.

[40]Sumarsono Raharjo, Ign, Informasi Elektronik Pada *Electronic Commerce* Dalam Hukum Pembuktian Perdata, Disertasi, UNAIR, Surabaya, 2005, h.127.

person and attached to or logically associated with the electronic data message or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic document.

Menurut UU Informasi dan Transaksi Elektronik (UU No. 11 Tahun 2008), tanda tangan digital adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi. Maka informasi elektronik yang dilekatkan, memiliki hubungan langsung atau terasosiasi pada suatu informasi elektronik lain yang dibuat oleh penandatangan itu dan digunakan untuk menunjukkan identitas dan statusnya sebagai subyek hukum, termasuk dan tidak terbatas pada penggunaan infrastruktur kunci publik (tanda tangan digital), tetapi juga berbasis pada biometrik, kriptografi simetrik. Dengan penerapan *digital signature* pada setiap bank atau lembaga keuangan lainnya yang menyediakan pelayanan *wire transfer* maka diharapkan setiap transaksi melalui *wire transfer* dapat di lacak atau dideteksi.

Dasawarsa ini, *digital signatures* menggunakan *cryptography* yang dimaksudkan untuk komunikasi yang tersembunyi dari intersepsi pihak-pihak yang tidak berkepentingan sehingga terjamin keamanannya. Hal ini tidak saja digunakan untuk komunikasi-komunikasi yang terbuka saja (misal: internet) tetapi juga digunakan untuk telex, fax, EFT, and EDI, seperti dijelaskan oleh Boumer & Poindexter sbb:

"Cryptography has been applied to the various means of electronic communications including telex, fax, electronic funds transfers, and EDI. Each of the foregoing are generally closed systems, not accessible by the general public, but are subject to interception by a saboteur or spy who has detailed knowledge of the underlying technology. During World War II, US intelligence spent considerable resources trying, ultimately successfully, to crack codes used by the

Japanese to encrypt the transmission of orders that directed their military operations."[41]

Lebih jauh apabila dilihat dari sisi kesejarahan yaitu sejak jaman Julius Caesar, teknik *cryptosystem* juga telah digunakan, yang lebih dikenal dengan nama Sandi Caesar yaitu dengan cara mengubah suatu huruf dengan huruf lain. Misalnya suatu huruf tertentu menggantikan huruf pada urutan ketiga di dalam alfabet itu. Huruf A menjadi D, C menjadi F, dan T menjadi W. Dengan demikian CAT menjadi FDW.[42] Pola sandi seperti ini juga sering digunakan oleh kalangan Kepanduan/Pramuka dan militer. *Test key* sebagai bentuk kunci rahasia juga dilakukan di kalangan perbankan yang lebih dikenal dengan sebutan *Patterson code* serta asuransi. Aplikasi-aplikasi tersebut di atas merupakan pola-pola sederhana yang dikembangkan dari *cryptography*.

Pada dasarnya *cryptography* adalah seni dan ilmu untuk keamanan menyimpan komunikasi.[43] Menurut *Oxford Advanced Learner's Dictionary*: *"cryptography is the art writing or solving code."* Sedang *Cryptanalysis is the art and science of defeating such security.*[44] Di dalamnya terdapat dua macam yaitu *symmetric cryptosystem*, atau *conventional cryptography* atau *secret key cryptosystem*, suatu sistem kriptografi yang konvensional dan *Asymmetric cryptosystem* atau dikenal juga sebagai *Public Key Cryptosystems* yang menjadi salah satu bentuk teknologi yang paling mutakhir *cryptography*, diciptakan pada tahun 1976 oleh Diffie dan Hellman.[45] Pendapat lain menyatakan bahwa *cryptography* adalah seni dan ilmu yang mempelajari bagaimana suatu *message* atau

---

[41]David Baumer & Poindexter, J.C., Op.cit., p.79.

[42]Ian J. Lloyd, Information Technology Law, 2ed, London, Butterworths, 1997, p.482.

[43]Bruce Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C-1, (2d ed., 1996).

[44]Ibid.

[45]Ian J. Lloyd, Op.cit., p.482.

data yang dikirim *originator*[46] dapat disampaikan kepada *addressee*[47] dengan aman.[48] Pendapat antara Bruce Schneir dan Lorijean G. Oei di atas pada intinya sama hanya Bruce Schneir lebih menunjuk dengan tegas bahwa keamanan komunikasi melalui *cryptography* adalah hubungan antara *originator* dan *addressee*. Dari sisi teknis, RSA Laboratories berpendapat bahwa *cryptography* adalah suatu bidang ilmu pengetahuan yang mempelajari teknik-teknik aplikasi yang keberadaannya tergantung pada keberadaan suatu masalah yang sulit atau sukar.[49] Pandangan yang menekankan segi teknis lain juga disampaikan oleh Ono W. Purbo dan Aang Arif Wahyudi,[50] bahwa *cryptography* adalah suatu bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi (*encrypt*) dan deskripsi (*decrypt*) suatu data. Teknik ini digunakan untuk mengkonversi data/*message* ke dalam bentuk kode-kode elektronis tertentu yang dimaksudkan agar informasi elektronik yang disimpan dan atau ditransmisikan melalui jaringan yang rentan keamanannya (misal: internet) tidak dapat digunakan oleh pihak-pihak yang tidak berkepentingan kecuali mereka yang mempunyai otoritas atas informasi elektronik tersebut. Menurut Lorijean G. Oei, contoh komunikasi sederhana tentang hal itu dapat dijelaskan sbb:

> "Communications are encrypted according to some predetermined code or chiper. For example, a simple, albeit easily breakable, cipher is A = 1, B = 2, and so on, so that "1-21-25 6-15-18-20-25 19-8-1-18-5-

---

[46]Pengertian Originator dapat ditemukan di dalam UNCITRAL Model Law on Electronic Commerce 1998, Art.2.c., karena di dalam UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, justru tidak ada. Artinya: "...a person by whom, or on whose behalf , the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message."

[47]Dalam **UNCITRAL Model Law on Electronic Commerce 1998, Art.2.d.**, addressee adalah **"...a person who is intended by the originator to receive the data message but does not include a person acting as an intermediary with respect to that data message."**

[48]**Bruce Schneir, Applied Crypthography,** Second Edition, New York, Willey and Son Inc., 1996, p.1.

[49]**RSA Laboratories, Frequently Asked Question About Today's Cryptography 4.0,** RSA Data Security Inc., 1988, p.2.

[50]**Ono W. Purbo dan Aang Arif Wahyudi, Mengenal E-Commerce,** Jakarta, Alex Media Computindo, 2001, h.27.

19 15-6 1-12-21-5 3-8-9-16 9-14-3" is the ciphertext of "Buy forty shares of Blue Chip, Inc."

Cryptography terdiri dari dua unsur yaitu *encryption* dan *decryption. Encryption* adalah proses yang tersamar, karena di dalam *encryption, "...a readable communication into an unintelligible scramble of characters according to some code or cipher."*[51] Komunikasi yang terbaca tersebut biasa dinamakan *plaintext,* dengan berbagai kemungkinan bentuk yaitu bisa terdiri dari *text, file, bitmap, digitized voice, digital video image,* dan lain sebagainya.[52] Sedang untuk komunikasi yang terinkripsi biasa dinamakan *ciphertext.* Selanjutnya, *Commweb*[53] memberikan penjelasan sbb:

> "The conversion of data into a secret code for transmission over a public network. The original text, or plaintext, is converted into a coded equivalent called ciphertext via an encryption algorithm. The ciphertext is decoded (decrypted) at the receiving end and turned back into plaintext.
>
> The encryption algorithm uses a key, which is a binary number that is typically from 40 to 128 bits in length. The greater the number of bits in the key (cipher strength), the more possible key combinations and the longer it would take to break the code. The data is encrypted, or 'locked,' by combining the bits in the key mathematically with the data bits. At the receiving end, the key is used to 'unlock' the code and restore the original data."

Encryption dengan demikian digunakan untuk meyakinkan kepada pihak lawan bahwa informasi elektronik tertentu tersembunyi dan tidak dapat dimengerti oleh orang lain yang tidak berhak, meskipun orang lain masih dapat melihat data yang telah terenkripsi tersebut. Rumus sederhana yang populer dikenal sbb:

---

[51]Lorijean G. Oei, 'Digital Signatures' dalam Thomas J. Smedinghoff (ed), Op.cit., p.497.

[52]Muhammad Aulia Adnan, "Aspek Hukum Protokol Pembayaran Visa/Mastercard Secure Electronic Transaction (SET)", Skripsi Strata 1, Fakultas Hukum Universitas Indonesia, Depok, Jawa Barat, 2001,p.24.

[53]http: www.commweb.com, Commweb adalah sebuah website yang menyuplai definisi kata-kata dan konsep-konsep yang sering digunakan dalam internet.

$$C = E(M)$$

Keterangan:

M : pesan asli

E : proses *encryption*

C : pesan dalam bahasa sandi

Proses lain dikenal sebagai *Decryption* yaitu *"...the process of converting the ciphertext back to its original, readable form."*[54] Jadi *Decryption* merupakan proses kebalikan dari *encryption* yang berfungsi untuk mengubah *message* dalam suatu bahasa sandi menjadi *message* asli yaitu bentuk yang dapat terbaca berupa teks biasa (*plaintext*) atau dalam rumus sederhana dikenal sbb:

$$M = D(C)$$

Keterangan:

D : proses *decryption*

M : pesan asli

C : pesan dalam sandi

Dalam perkembangannya, *Modern Encryption* menggunakan *algorithma* dan tidak hanya *chipers* yang sederhana, seperti dikemukakan oleh Lorijean G. Oei:

> "modern encryption does not rely upon such simple chipers, but instead relies on algorithms. These algorithms are complex mathematical functions for converting plaintext to ciphertext and vice versa."[55]

Seseorang yang menginginkan, mengirim dan menerima enkripsi komunikasi membutuhkan parameter yang dikenal dengan istilah "kunci". *Cryptography*

[54]Ibid.
[55]Ibid.

konvensional menggunakan kunci untuk *encryption* informasi. Kunci yang sama dipergunakan juga penerima untuk mendekripsikan informasi. Kunci rahasia ini adalah merupakan nilai yang sangat spesifik dan bekerja dalam algoritma *cryptography* untuk menghasilkan yang terenkripsi secara spesifik pula. Keamanan suatu dokumen tergantung pada ukuran "bit"[56]. Semakin besar kapasitas bit, nilai kunci dan sistem prosesor komputer akan juga berpengaruh terhadap keamanan teks/dokumen yang terenkripsi karena periode penjaminan keamanannya dalam tenggat waktu yang cukup lama. Keselamatan *message* yang dikirim sangat tergantung pada bagaimana kunci tersebut dilindungi.[57] Kondisi ini mulai dapat diminimalisasi untuk keselamatan data/*message* dengan sistem sandi asimetrik atau kunci publik. Sistem ini didasarkan pada dua kunci yaitu kunci privat dan kunci publik yang secara matematis berkaitan. Dengan menggunakan kunci privatnya, message dapat dikirimkan dan hanya dapat dienkripsi oleh kunci publik yang bersangkutan sehingga dapat dipastikan integritas dan keaslian pesannya.[58]

Selain itu, sebenarnya berdasarkan UU no 8 tahun 1997 tentang Dokumen Perusahaan, maka setiap perusahaan memiliki kewajiban untuk membuat catatan dan menyimpan dokumen perusahaan. Berdasarkan UU ini maka yang dimaksud dengan dokumen adalah dokumen perusahaan yang terdiri dari dokumen keuangan dan dokumen lainnya. Yang dimaksud dengan catatan disinipun termasuk pula dengan segala bentuk catatan hal-hal lain yang berkaitan dengan kegiatan usaha suatu perusahaan. Layanan jasa *wire transfer* dilakuka oleh bank dana atau lembaga keuangan bukan bank yang merupakan pengelola jasa keuangan dan

---

[56]bit adalah a binary digit, or a number, often encoded in a computer readable form, which has a value of either 0 or 1.

[57]Chris Reed and John Angel (ed), **Computer Law**, 4ed, London, Blackstone Press Limited, 2000, p.239.

[58]Ibid.

berbentuk sebuah perusahaan. Maka pengelola *wire transfer* tersebut harus mematuhi ketentuan dalam UU tentang Dokumen Perusahaan ini dan melakukan pencatatan dan penyimpanan catatan transaksi *wire transfer* dan digunakan sebagai bukti hukum serta untuk digunakan identifikasi personal, sehingga dapat meminimalisir potensi *moneylaundering*.

B. Kebijakan Hukum Berkenaan Dengan Berkembangnya Tindak Pencucian Uang Melalui Sarana *Electronic Money*

Perkembangan *cyberlaundering* sebagai konsekuensi pengembangan sistem *e-money* membutuhkan kebijakan hukum tepat yang terintegrasi secara global. Permasalahan muncul karena setiap negara mempunyai sistem hukumnya sendiri, sedang perkembangan teknologi informasi dengan cepat dapat terintegrasi dan holistik karena standar-standar teknologinya jelas dan terukur. Dalam konteks hubungan internasional, adanya berbagai aturan-aturan hukum nasional yang terbentuk menjadi sistem hukum sendiri itu, akan sangat mempengaruhi kelancaran transaksi-transaksi *online* yang dapat dilakukan di manapun juga dan dikirim ke manapun juga di dunia. Dalam sidang Majelis Umum PBB No. 2102 (XX), khususnya dalam dunia perdagangan yang terkait dengan transaksi-transaksi online, PBB menyadari hal itu dan menyatakan bahwa: *"conflict and divergencies arising from the laws of different states in matter relating to international trade constitute an obstacle to the development of the world trade."*[59] Kenyataan-kenyataan inilah yang perlu disikapi melalui kebijakan hukum yang memadai dan terintegrasi.

[59]United Nation, **Progressive Development of the Law of International Trade: Report of the Secretary-General of the United Nations**, New York; United Nations, 1966, par. 14.

Kebijakan adalah keputusan tetap yang dicirikan oleh konsistensi dan pengulangan tingkah laku dari mereka yang membuat dan dari mereka yang mematuhi keputusan tersebut.[60] Definisi ini dapat diterapkan dalam kebijakan hukum. Menurut Eulau dan Prewitt, suatu kebijakan dapat dikatakan sebagai kebijakan publik atau tidak, harus memenuhi beberapa komponen yang terintegrasi sebagai komponen kebijakan publiknya yang mencakup hal-hal sbb:[61]

a. *Intentions*, yaitu niat/tujuan sebenarnya dari sebuah tindakan (sic: hukum);
b. *Goals*, yaitu tujuan/keadaan akhir yang hendak dicapai;
c. *Plans or proposals*, yaitu rencana atau usulan untuk mencapai tujuan;
d. *Program*, yaitu program yang disahkan untuk mencapai tujuan kebijakan;
e. *Decissions or choices* yaitu keputusan atau pilihan atas tindakan-tindakan yang diambil untuk mencapai tujuan, mengembangkan rencana, melaksanakan dan mengevaluasi program;
f. *Effect*, yaitu dampak atau pengaruh yang dapat diukur.

Kebijakan hukum pada dasarnya adalah kebijakan publik karena hukum adalah untuk kepentingan publik. Sehubungan dengan perkembangan *e-money* maka kebijakan hukum yang harus dilakukan ada dua cara. Pertama, hukum nasional perlu menyusun dan mengundangkan hukum yang mengatur tentang *e-money* dan pencegahan *cyberlaundering* yang disesuaikan dengan standar internasional dan fungsional; Kedua, perlu dilakukan unifikasi dan harmonisasi aturan-aturan hukum substantif *e-money* dan pencegahan *cyberlaundering*. Dua pendekatan tersebut perlu integratif dan diharapkan berjalan cukup efisien yang berpedoman pada pola kerja sibernetis. Lembaga internasional seperti FATF yang sudah membuat kriteria negara yang dinyatakan *"on the right track"* terhadap pencegahan pencucian uang yang terdiri dari 40 kriterium perlu dijalankan

[60]Hessel Nogi Tangkilisan, **Kebijakan dan Manajemen Otonomi Daerah**, Lukman Offset, Yogyakarta, 2003, h.3.
[61]**Ibid**, h.4.

secara tegas dan selalu *up date*. Pemerintah yang masuk kriteria FATF dalam konteks *e-money* harus selalu memperbaharui pengaturan hukumnya karena terdapat kesadaran bahwa kejahatan jenis ini akan selalu selangkah di depan hukum karena mereka (para pelaku) juga selalu mengembangkan diri di bidang teknologi informasinya, yang bisa digambarkan sbb:[62]

> As e-money systems develop, governments may need to identify the additional legislative and regulatory measures that may be needed to combat money laundering and other financial crimes involving these systems. Police may have to develop new techniques to deal with on-line crime. Even so, it is likely that laws and regulations will always lag behind technological advances, and criminals will continue to exploit technology and try to stay one step ahead of the law.

Potensi untuk penyalahgunaan sistem *e-money* oleh kejahatan terorganisasi, pencuci uang dan penjahat keuangan lain bisa menjadi penting. Sebab *e-money* bisa mendorong kearah transaksi yang tidak bisa terlacak dan penawaran mobilitas transaksi dan penukaran uang yang belum pernah terjadi dalam kaitan dengan kecepatan dan perpindahan uang lintas batas dan ini bisa menciptakan tantangan baru bagi pemerintah seperti dapat dijelaskan sbb:[63]

> The potential for abuse of e-money systems by organized crime, money launderers and other financial criminals could be significant. Because e-money could lead to untraceable transactions and offer unprecedented mobility both in terms of speed of transfer and absence of borders, it could create new enforcement challenges:

Namun, FATF juga telah memberikan standar-standar untuk memerangi *cyberlaundering* yaitu dengan saran-saran sbb:

---

[62]Department of Justice Canada Solicitor General Canada, Op.cit.,p.11.

[63]Ibid.

1) Internet service providers establish log files with traffic data providing internet-protocol numbers of subscreibers and telephone number used for server connection;
2) Information collected through the servers be shared with enforcement agencies;
3) Information collected be maintained for up to a year;
4) Internet service provider keep records, including identification information, on those who transit through their servers.

Negara yang sudah menerapkan standar pengaturan hukum seperti yang diinginkan oleh FATF, contoh yang cukup baik adalah Negara Swiss. Sejak awal delapan puluhan, negeri Swiss yaitu dunia perbankan dan Otoritas hukum sudah bereaksi kepada bahaya bahwa penyalahgunaan pasar uang oleh organisasi kriminal sebagai tempat untuk pencucian uang. Hukum nasional dan instrumen internasional telah dikembangkan dari tahun ke tahun dan dimodernisasi untuk ukuran-ukuran yang bersifat represif dari hukum pidana konvensional dan sudah menciptakan suatu hubungan baru antara pemerintah dan dimasukkan dalam sektor keuangan. Pemerintah dan aparat penegak hukum lain sekarang ini merasa terikat dengan dengan aktip menggabungkan diri dalam perlawanan terhadap tindak pencucian uang. Aparat pemerintah dan semua aparat penegak hukum yang dapat bergabung secara bersama-sama adalah mutlak diperlukan dalam memerangi *moneylaundering* terlebih khususnya *cyberlaundering* karena kompleksitasnya. Penjelasan dibawah menunjukkan konsistensi pemerintah Swiss terhadap pelanggaran *moneylaundering*, sbb:[64]

> Since the early eighties, Swiss authorities and banks have reacted to the danger that abuse of the financial market by criminal organizations embodies. The ***national*** and ***international instruments*** that have been developed over the years have thus modernized the repressive measures derived from ordinary criminal law and have created a new relationship between the authorities and those involved in the

[64]The Royal Canadian Mounted Police, Proceeds of Crime Branch, Op.cit., p.2.

financial sector. They are currently committed to actively joining forces in the fight against money laundering.

Konsistensi kebijakan hukum pemerintah dalam menyikapi pelanggaran yang bersifat global, menyangkut banyak aspek dan serta melekat pada teknologi informasi sangat dibutuhksan. Maka, apabila semua Negara di dunia mempunyai kesamaan persepsi terhadap hal ini, setidaknya akan mempersempit gerak para pencuci uang melalui *cyber* dan penanganan yang cepat sesuai karakter informatika serta dapat membentuk *"court"* yang memadai seperti halnya penyelesaian sengketa domain yang sekarang semakin baik melalui *Online Dispute Resolution (ODR)*. Karakter sibernetis harus selalu melekat dalam pembentukan hukum, penegakan hukum, proses peradilan serta penyelesaian perkara.

PENUTUP

KESIMPULAN

1. Undang-Undang No. 25 Tahun 2003 dan peraturan pelaksanaannya termasuk peraturan yang dibuat oleh PPATK, PBI, Undang-Undang ITE tidak cukup untuk mencegah pelanggaran tindak pencucian uang di *cyber* karena disamping pola *smurfing* atau *structuring* masih tetap dilegalkan tetapi juga yang paling penting bahwa *e-money* dapat dilakukan tidak hanya oleh lembaga perbankan pemerintah tetapi juga dilakukan oleh lembaga keuangan lainnya. *E-money* mempunyai 'karakter' dapat dilakukan dimanapun di dunia sebagai konsekuensi globalisasi serta kapanpun juga baik untuk mengirim transaksi maupun menerima transaksi, sifat anonimitas, sehingga relatif sulit dilakukan pelacakan, biarpun pengaturan prinsip mengenal nasabah sudah ditegakkan.
2. Berkembangnya tindak pencucian uang melalui sarana *electronic money* adalah suatu keniscayaan. Maka, hukum juga harus berkarakter sibernetis yaitu *variety, circularity, process* dan *observation*. Hukum sibernetis adalah hukum yang fungsional, dalam arti, hukum berfungsi melindungi dan sebagai tempat menuntut keadilan dengan relasi ketergantungannya dengan suatu sistem dan faktor lingkungan dari sistem hukum di dunia maya yang menciptakan *lex informatica* sehingga menjadi hukum bagi para pihak di dalam aktivitasnya di dunia maya. Pencegahan *cyberlaundering* hanya dapat dilakukan melalui kebijakan hukum yang berkarakter sibernetis yaitu harus cepat berubah, fungsional dan disesuaikan kebutuhan.

SARAN

1. Perbaikan teknologi yang terus menerus untuk pelacakan pencucian uang serta kerjasama internasional yang intensif dan perbaikan terus-menerus standarisasi

keamanan serta prosedur hukum untuk pemberantasan pencucian uang secara global adalah merupakan cara yang bisa dilakukan untuk menanggulangi *cyberlaundering* karena sifat yang *boderless, paperless, timeless* serta sifat anonimitas subyek. Disamping itu, system audit lembaga keuangan bukan bank yang mengeluarkan e-money perlu dilakukan secara ketat sebagai bentuk pencegahan untuk penyalahgunaan lembaga keuangan bukan bank tersebut untuk cyberlaundering

2. Kebijakan hukum yang sekarang sudah dilaksanakan melalui pengaturan, pengawasan secara internasional dan adanya kewajiban Negara-negara di dunia untuk ikut dalam memerangi *cyberlaundering* melalui pembentukan hokum adalah sudah masuk dalam jalur yang benar. Hanya, perlu didorong terus untuk selalu mencari peluang paling pas dan efisien serta efektif penggunaan teknologi untuk mengidentifikasi dan melakukan kegiatan indikatif terhadap penyalahgunaan e-money untuk kegiatan *cyberlaundering*. Penggunaan teknologi informasi di Indonesia, apabila ditinjau dari pendekatan internal, perlu selalu dilakukan up-date dan pengawasan.