PENGARUH PERKEMBANGAN TELEMATIKA TERHADAP TINDAK PIDANA PENCUCIAN UANG

Oleh : DR. Zulkarnaen Sitompul, SH, LL.M

A. Pendahuluan

Sepanjang sejarah, manusia dalam kehidupannya selalu berusaha memenuhi keperluannya dengan mengembangkan ilmu pengetahuan dan teknologi.[1] Apabila sebelumnya manusia menggunakan batu, kulit atau daun sebagai media untuk menulis atau menggambar, namun sekarang dapat dilakukan dengan menggunakan teknologi berbasis komputer. Kalau dahulu orang ingin menyampaikan pesan kepada orang lain harus berhadapan langsung dengan penerima pesan atau dengan menyuruh orang lain membawakan pesannya, maka sekarang dapat dilakukan dengan cukup menelpon atau memanfaatkan fasilitas jaringan komputer (e-mail). Memang sejak awal manusia selalu termotivasi memperbaharui teknologi yang ada. Dari semua kemajuan yang signifikan yang dibuat manusia sampai hari ini, mungkin hal terpenting adalah perkembangan dibidang teknologi informasi dan komunikasi.

Berbicara mengenai teknologi informasi dan komunikasi, pada masa sekarang tidak dapat dilepaskan dengan telematika (*cyberspace*)[2]. Perkembangan teknologi informasi dan komunikasi, telah mempengaruhi banyak aspek kehidupan di masyarakat, antara lain dalam bidang perdagangan (*e-commerce*), pemerintahan (*e-government*), dan bahkan terhadap perilaku masyarakat (*social behaviour*) yaitu semula berbasis media kertas (*paper based*) sekarang menjadi system elektronik (*electronic based*).[3]

Salah satu faktor pendorong yang utama berkembangnya teknologi informasi dan komunikasi di bidang perdagangan (*e-commerce*) ditandai dengan globalisasi

[1] Prof. DR. Hikmahanto Juwono, SH, LL.M, dalam makalah " Aspek Penting Pembentukan Hukum Teknologi Informasi di Indonesia, dmuat dalam Majalah Hukum Bisnis, Volume 16, November 2001, hal.48

[2] Perkembangan teknologi informasi terakhir, khususnya ledakan informasi didalam dunia maya (*cyberspace*), (seiring dengan meluasnya penggunaan komputer istilah cyberspace menunjuk kepada sebuah ruang elektronik *(electronic space)*, yakni sebuah masyarakat virtual yang terbentuk melalui komunikasi yang terjalin dalam sebuah jaringan komputer *(interconnected computer net-works)*

[3] Cahyana Ahmadjajadi, dalam makalah "RUU ITE Sebagai Infrastruktur Fundamental Untuk Pengembangan Sisfonas" disampaikan pada Diskusi Cyber Policy Seminar – GIPI-IMPLC, 23 September 2003, hal. 2.

perdagangan barang dan jasa. Perdagangan global telah diterima sebagai kesepakatan dunia, termasuk Indonesia yaitu dengan telah diratifikasinya perjanjian Marakesh dan pendirian *World Trade Organization* (WTO) dengan Undang-Undang Nomor 7 Tahun 1994 tentang Pengesaahan *Agreement Establishing the World Trade Organization.* Saat ini hampir semua negara telah bergabung dalam World Trade Organization (WTO). Sementara itu negara-negara yang belum tergabung ke dalamnya telah dan sedang berusaha dengan sungguh-sungguh untuk dapat diterima sebagai anggota.[4]

Maraknya *electronic transaction* (*e-transaction*), yang dikenal pula sebagai *eletronic commerce* (*e-commerce*)[5], menimbulkan tantangan baru. Kejahatan dengan *telemarketing*, yaitu menawarkan barang melalui telepon secara melawan hukum, sudah makin marak akhir-akhir ini di dunia maya (*virtual wold* atau *cyberspace*). Pengiriman e-mail melalui Internet atau pengiriman *short message system* (SMS) melalui telepon genggam (*hanphone* atau *mobile phone*) yang berisi informasi yang menyesatkan juga sering terjadi. Belum lagi upaya *hackers* untuk masuk ke *electronic files* badan-badan atau institusi pemerintah, perusahaan, atau perorangan dengan mencuri informasi, bahkan dengan melakukan perubahan data elektronik yang tersimpan, sungguh sangat merugikan negara dan masyarakat.[6]

Dalam dunia perbankan, pengiriman uang melalui *wire transfer* telah lazim dilakukan di Indonesia. Pada saat ini *Credit Card* dan *Debit Card* telah menjadi alat untuk melakukan pembayaran dalam kegiatan bisnis masyarakat perkotaan, antara lain untuk membayar belanja di mall, supermarket, restoran dan agen-agen penjualan yang menyediakan fasilitas tersebut.

Perkembangan yang cepat dalam bidang teknologi informasi dan globalisasi ekonomi memudahkan transfer dana (*wire transfer*) dilakukan secara cepat dan mudah dengan melewati batas-batas yurisdiksi suatu negara. Di samping itu, penggunaan *digital*

---

[4] Prof. DR. Sutan Remy Sjahdeni, SH, disampaikan dalam Kata Sambutan pada buku Pengantar Hukum Kejahatan Bisnis : Prof. DR. Romli Atmasasmita, SH, LL.M, Prenada Media, Jakarta, 2003.

[5] E-Commerce didefinisikan sebagai "by connecting to a standardized network we can find information, buy and sell quickly and easily, with lower process and administration costs" : Will Rowan, E-Commerce, Management Pocketbooks Ltd, U.K., 2000, p.5.

[6] Prof. DR. Sutan Remy Sjahdeni, SH, op.cit

cash (*e-cash*)[7] dalam transaksi melalui jaringan internet telah diperkenalkan karena adanya tuntutan transaksi yang efisien, namun pihak-pihak yang bertransaksi identitasnya tidak diketahui (*anonymous*). Tentu saja, kemudahan-kemudahan tersebut juga dimanfaatkan oleh para pencuci uang (*money launderer*) untuk menyembunyikan atau menyamarkan harta kekayaan yang dihasilkan dari tindak pidana, dengan cara harta kekayaan (uang) ilegal tersebut dimasukkan melalui *international banking system* atau melalui jaringan bisnis di internet sehingga akan sulit dilacak asal usulnya. Karena sifat kegiatan pencucian uang tersamarkan maka diperkirakan jumlah uang yang dicuci setiap tahunnya sebesar $500 miliar hingga $1 triliun.[8] Hal ini membuat tugas pemberantasan pencucian uang lebih sulit dan mendesak daripada sebelumnya.

B. Perkembangan dan Ruang Lingkup Telematika

Pengembangan teknologi informasi (telematika) terkait dengan jaringan yang terhubung diawali pada tahun 1962, ketika Departemen Pertahanan Amerika Serikat melakukan riset penggunaan teknologi komputer untuk kepentingan pertahanan udara Amerika Serikat. Melalui lembaga risetnya yaitu Advanced Research Project Agency (ARPA) menugasi the New Information Processing Techniques Office (IPTO), yaitu suatu lembaga yang diberi tugas untuk melanjutkan riset penggunaan teknologi komputer di bidang pertahanan udara.[9] Selanjutnya Pada tahun 1969 *Departement* Pertahanan Amerika Serikat menemukan sebuah teknologi yang esensinya memadukan teknologi telekomunikasi dengan komputer yang dikenal dengaan nama ARPANet (*Advanced Research Projects Agency Network)* yaitu system jaringan melalui hubungan antar

[7] "Digital Cash has been defined as a series of numbers that have an intrinsic value in some form of individually identified representations of bill and coins – similar to serial numbers on hard currency" : R. Mark Bortner, Cyberlaundering, 1996, sumber : http://www.miami.edu/%7Efroomkin/seminar/papers/bortner.htm

[8] ADB, Manual on Countering Money Laundering and the Financing of Terrorism, Asian Development Bank, March 2003, p.10

[9] http://www.livinginternet.com/i/ii_ipto.htm

komputer di daerah-daerah vital dalam rangka mengatasi masalah jika terjadi serangan nuklir.[10]

Keberhasilan dalam memadukan teknologi tersebut atau yang dikenal dengan istilah teknologi informasi (*information technology*) pada tahun 1970 mulai dimanfaatkan untuk keperluan non-militer oleh berbagai universitas.[11] Pada dekade inilah sebenarnya manusia telah memasuki era baru yaitu melalui perkembangan teknologi informasi telah dimanfaatkan manusia hampir di semua aspek kehidupan.

Berpadunya globalisasi dan kemajuan teknologi bidang informasi dan komunikasi, telah mendorong munculnya jenis-jenis transaksi bisnis yang baru dan secara berangsur cara-cara bisnis yang lama ditinggalkan. Bukan saja bisnis menjadi semakin maju, tetapi juga jenis-jenis transaksinya makin banyak, makin canggih dan makin cepat proses penyelesaiannya. Di pihak lain hal ini tentunya ekses negatif yang timbul tidak dapat dihindari, karena dapat memunculkan jenis-jenis kejahatan bisnis (*business crime*) baru, dan menimbulkan persoalan lain seperti pelanggaran *privacy*, *pornography*, *counterfeiting*, *defamation*, *hackers*, *drug cartel*, *cyberquatting*, *international money laundering*. Sedangkan dari sisi hukum, berkembangnya kegiatan teknologi informasi menimbulkan persfektif dalam cabang ilmu hukum antara lain, hukum perdata, pidana, tata negara, administrasi negara dan internasional, dan dari perspektif spesialisasi bidang hukum adalah hukum pasar modal, perbankan, hak atas kekayaan intelektual, dan pajak.[12]

Perkembangan teknologi informasi terakhir, khususnya ledakan informasi dalam dunia maya atau telematika (*cyberspace*) dan internet membawa perubahan ke segala aspek kehidupan manusia, pendidikan, hiburan, pemerintahan, dan komunikasi. Istilah telematika menunjuk kepada sebuah ruang elektronik (electronic space), yakni sebuah

---

[10] Dr. Hj. Hanny Kamarga, M.Pd., Belajar Sejarah Melalui E-Learning : Alternatif Mengakses Sumber Informasi Kesejarahan, PT Intimedia, Jakarta, 2002, hal 2.

[11] ibid

[12] Prof. DR. Hikmahanto Juwana, SH, LL.M, (Dalam makalah berjudul : Aspek Penting Pembentukan Hukum Teknologi Informasi di Indonesia) Jurnal Hukum Bisnis, Volume 16, November 200, hal.49-53

masyarakat virtual yang terbentuk melalui komunikasi yang terjalin dalam sebuah jaringan komputer (*interconnected computer networks*).[13]

Hampir setiap kali berbicara mengenai teknologi informasi, maka sulit dipisahkan dengan persoalan jaringan (net). Dewasa ini dikenal dengan istilah internet, intranet dan ekstranet. Internet didefinisikan sebagai "*a global network connecting millions of computers*"[14], intranet adalah "*a private network belonging to an organization, usually a corporation, accessible only by the organization's members, employes, or others with authorization*[15], dan ekstranet adalah "*a fancy way of saying that a corporation has opened up portions of its intranet to authorized users outside the corporation*.[16]

Peran penting internet secara umum adalah[17] :

a. Distribusi geografis mencakup seluruh dunia, pada saat masuk dalam jaringan maka dapat berkomunikasi dengan siapapun di seluruh dunia.
b. Memperlihatkan arsitektur yang kuat, karena merupakan jaringan kerja dan tidak terdapat pusat kontrolnya.
c. Kecepatan beroperasinya sesuai waktu yang sesungguhnya (*real time speed*).
d. Aksesnya bersifat universal, siapapun dapat menghubungkan diri dengan jaringan internet.
e. Memberikan kebebasan berbicara, tidak ada larangan untuk berpendapat dan berbicara.

Bagi Indonesia, permasalahan teknologi informasi masih dapat dikatakan sebagai hal yang relatif baru. Kalaupun dibeberapa kota terasa masyarakat sangat antusias dalam memanfaatkan teknologi ini, pada kenyataannya pemanfaatan itu hanya untuk hal-hal yang kurang produktif bagi kepentingan ekonomi dan pemerintahan.[18] Kondisi demikian tidak terlepas dari kepastian hukum penggunaan teknologi informasi ini. Banyak negara telah memiliki undang-undang yang mengatur teknologi informasi, seperti Singapura

[13] Ridwan Khairandy, SH, MH, Pembaharuan Hukum Kontrak Sebagai Antisipasi Transaksi Electronic Commerce, dimuat dalam Majalah Jurnal Hukum Bisnis, Vol.16 November 2001, hal,56
[14] http://webopaedia.internet.com
[15] http://netforbeginners.minings.com
[16] ibid
[17] http://www.livinginternet.com/i/ii_ipto.htm
[18] Editorial, Jurnal Hukum Bisnis, Volume 18 Maret 2002, hal.4

dengan The Electronic Transaction Act, Amerika Serikat dengan The Digital Signature Act pf 1999, dan Australia memiliki The Electronic Transaction Bill 1999, sedangkan Indonesia belum mengeluarkan regulasinya.

Dalam transaksi perdagangan eletronik (e-commerce), sangat terkait erat dengan masalah tanda tangan, pembuktian, perlindungan konsumen dan Hukum Perdata International.[19] Konsumen dalam transaksi elektronik sering tidak berpikir panjang dalam menyetujui berbagai kontrak yang dibuat ketika transaksi jual beli. Persoalan yang mungkin timbul, antara lain bagaimana jika salah dalam pengiriman barang yang telah dijual/dibeli, jika pembayaran dilakukan kepada orang yang tidak berhak, dan lain sebagainya. Oleh sebab itu, materi seperti liability, availability, Notice Disclaimers, compliance, dispute resolution, dan termination sebaiknya dituangkan dalam perjanjian antara Electronic Marketplace dengan anggotanya.[20]

Yang paling menarik dari perkembangan pasar dalam dunia maya adalah bisnis yang dikenal dengan *Business to Business (B2B) e-commerce marketplace*, yaitu suatu situs web dimana pembeli dan penjual bertemu untuk bertukar pikiran/ide, komunikasi, beriklan, mengadakan lelang, tender, penawaran dan melaksanakan perdagangan atau transaksi. Bisnis cara ini telah dilakukan di seluruh dunia, dan perkembangan B2B nilai transaksinya mencapai $25 billion pada tahun 2000 dan pada tahun 2005 diperkirakan mencapai $2,2 trillion,[21] sedangankan Betty Spence memperkirakan pada tahun 2000 pendapatan yang dihasilkan dari e-commerce sebesar $210 billion, dan pada tahun 2004 di United States sebesar $2.7trillion, di asia Pasifik $1.6 trillion dan di Eropa sebesar $1.5 trillion[22], suatu nilai yang sangat fantastis.

---

[19] DR. Ahmad M. Ramli, SH, MH, Perlindungan Hukum Terhadap Konsumen dalam Transaksi E-Commerce, dmuat dalam Jurnal Hukum Bisnis, Volume 18 Maret 2002, hal.14.

[20] Michael R. Geroe, dalam makalah "Agreements between an Electronic Marketplace and Its Member, The International Lawyer, Aquarterly Publication of The ABA/Section of International Law and Practice, Fall 2001, Volume 35, number 3

[21] Jupiter Communication, www.jup.com

[22] Betty Spence, E-Day, CEO E-Conference Report: Startegic B2B: Creating New Economy Growth and Profit, dikutip oleh Michael R. Geroe, op.cit.

Sejalan dengan perkembangan pasar perdagangan eletronik, cyberpayment system juga mengalami perkembangan dalam masyarakat. Saat ini terdapat 4 model[23] yang dikenal yaitu :

a. The Mercahant Issuer Model, yaitu Issuer Smart Card dan penjual barang adalah pihak yang sama, misalnya the creative star farecard used by riders in the Hongkong Transit System
b. The Bank Issuer Model, yaitu Merchant dan Issuer adalah pihak yang berbeda. Transaksi dikliringkan melalui sistem financial traditional, misalnya banksys'proton card di Belgium (licensed by Amex), dan the Danmont Card di Denmark.
c. Non bank Issuer Model, yaitu Pengguna beli e-cash dari issuer dengan menggunakan uang tradisional dan membelanjakan e-cash pada merchant yang berpartisipasi dalam skim tersebut. Issuer selanjutnya akan mengganti e-cash dari merchant, misalnya DigiCash dan CyberCash.
d. Peer to Peer Model, yaitu E-Cash yang dikeluarkan oleh bank atau non bank dapat dipindahtangankan diantara pengguna, misalnya Mondex Stored Value Smart Card.

C. Tindak Pidana Pencucian Uang (*Money Laundering*) dan Perkembangan Telematika

Pada kebanyakan negara, *money laundering* dan pembiayaan terorisme menjadi isu yang signifikan dalam rangka pencegahan, pemberantasan dan penuntutannya.[24] Isu *money laundering* dalam beberapa tahun terakhir selalu mengemuka dan menjadi perhatian publik khususnya di Indonesia atau tepatnya sejak bulan Juni 2001, yaitu pertama kalinya Indonesia dimasukkan dalam daftar negara yang tidak kooperatif dalam pemberantasan tindak pidana pencucian uang atau *Non Cooperatives Countries and Territories* (NCCTs) oleh FATF.[25]

---

[23] Iwan Setiawan, Cyberlaws & Kapasitasnya Dalam Memerangi Kejahatan Pencucian Uang, disampaikan pada diskusi Cyber Policy Seminar – GIPI-IMPLC, 23 September 2003

[24] Paul Allan Schott, Refence Guide to Anti-Money Laundering and Combating the Financing of Terrorism, The International Bank for Reconstuction/The World Bank, 2003

[25] Financial Action Task Force on Money Laundering (FATF) didirikan tahun 1989 dengan sponsor utama negara-negara industri besar (Group of Seven atau G 7 dan European Union. FATF beranggotakan

Sejak saat inilah kalangan akademis, pengamat, dan mayarakat dengan bantuan dari media masa, memberikan perhatian besar dalam pengkajian *money laundering* dan dampak-dampak yang ditimbulkannya. Sementara itu, regulator seperti Bank Indonesia, BAPEPAM dan Departemen Keuangan telah mempersiapkan diri dalam membuat regulasi demi pembangunan regime anti money laundering di Indonesia.

Membahas isu *money laundering*, tidaklah "*afdzol"* jika tidak memahami pengetiannya. Terdapat beberapa pengertian *money laundering* sebagai berikut :

Black's Law Dictionary mengartikan *money laundering* sebagai:

> *"Term used to describe investment or other transfer of money flowing from racketeering, drug transaction, and other illegal sources into legitimate channels so that is original source cannot be traced"*[26]

Konvensi PBB Tentang Pencegahan dan Pemberantasan Perdagangan Illegal Narkotika, Obat-obatan Berbahaya dan Psikotropika Tahun 1988 (the United Nations Convention Against Illicit Trafic in Narcotics, Drugs and Psychotropic Substances of 1988) mengartikan *money laundering* sebagai :

> "*The convention or transfer of property, knowing that such property is derived from any serious (indictable) offence or offences, or from act of participation in such offence or offences, for the purpose of concealing or disguising the illicit of the property or of assisting any person who is involved in the commission of such an offence or offences to evade the legal consequences of his action; or The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from a serious (indictable) offence or offences or from an act of participation in such an offence or offences."*

Konvensi tersebut merupakan konvensi yang pertama kali mendefinisikan *money laundering*. Dalam konteks pencucian uang, cakupan konvensi PBB tersebut belum memadai karena hanya mengatur pencucian uang yang berasal dari kejahatan perdagangan narkotika dan obat-obatan terlarang sedangkan tindak pidana yang dapat menjadi pemicu terjadinya pencucian uang sangat banyak antara lain mencakup korupsi, penyuapan, penyelundupan, kejahatan di bidang perbankan, narkotika, dan psikotropika.

---

29 negara dan dua organisiasi internasional, yaitu the European Commission dan the Gulf Cooperation Council

[26] Henry Campbell Black, Black's Law Dictionary (Sixth Edition), St. Paul Minn. West Publishing Co., 10990, hal. 884

Dalam RUU amandemen UU TPPU yang telah disetujui oleh DPR pada tanggal 16 September 2003, pencucian uang didefinisikan sebagai suatu perbuatan menempatkan, mentransfer, membayarkan, membelanjakan, menghibahkan, menyumbangkan, menitipkan, membawa ke luar negeri, menukarkan, atau perbuatan lainnya atas Harta Kekayaan yang diketahuinya atau patut diduga merupakan Hasil Tindak Pidana dengan maksud untuk menyembunyikan, atau menyamarkan asal usul Harta Kekayaan sehingga seolah-olah menjadi Harta Kekayaan yang sah.

Dengan demikian aktivitas pencucian uang secara umum merupakan suatu cara menyembunyikan atau mengaburkan atau menyamarkan asal-usul harta kekayaan dari hasil tindak pidana yang kerap dilakukan oleh *organized crime*, maupun individu yang melakukan tindak korupsi, perdagangan narkotika dan kejahatan lainnya. Melalui tindakan yang melanggar hukum ini, uang/pendapatan atau harta kekayaan yang didapat dari hasil kejahatan diubah menjadi dana yang seolah-olah berasal dari sumber yang sah atau legal. Modus tindak pidana seperti ini dari waktu ke waktu semakin kompleks dengan menggunakan teknologi dan rekayasa keuangan yang cukup *complicated*.

Dalam perkembangan selanjutnya, pengertian tindak pidana pencucian uang diperluas tidak hanya kepada para pelaku langsung, tetapi juga mencakup pihak-pihak yang membantu terjadinya kejahatan pencucian uang. Masuk dalam kategori ini misalnya seseorang yang membantu orang lain untuk menyembunyikan sebuah rumah yang diketahuinya atau patut diketahuinya dibeli dengan menggunakan uang hasil korupsi.[27] Undang-undang No. 15 Tahun 2002 di dalam Pasal 3 ayat (2) bahkan memasukkan unsur percobaan, pembantuan, atau permufakatan melakukan tindak pidana pencucian uang sebagai tindak pidana yang diancam pidana penjara dan pidana denda.

Adapun yang melatarbelakangi para pelaku pencucian uang melakukan aksinya adalah dengan maksud memindahkan atau menjauhkan para pelaku itu dari kejahatan yang menghasilkan *proceeds of crime*, memisahkan *proceeds of crime* dari kejahatan yang dilakukan, menikmati hasil kejahatan tanpa adanya kecurigaan kepada pelakunya,

[27] Sherman T, International Efforts to Combat Money Laundering: The Role of the Financial Task Force, yang dikutip oleh MacQueen L (ed.), Money Laundering, Edinburgh, 1993, hal. 12

serta melakukan reinvestasi hasil kejahatan untuk aksi kejahatan selanjutnya atau ke dalam bisnis yang sah.[28]

Melalui tindakan yang melanggar hukum tersebut, pendapatan atau kekayaan yang didapat kemudian dirubah menjadi dana yang seolah-olah berasal dari sumber yang sah/legal, dilakukan dengan modus tertentu. Modus kejahatan seperti ini dari waktu ke waktu semakin kompleks seiring dengan berkembangnya teknologi dan rekayasa keuangan yang cukup *complicated*. Secara sederhana, kegiatan ini pada dasarnya dapat dikelompokkan pada tiga kegiatan, yakni : *placement, layering* dan *integration.*[29]

Placement merupakan upaya menempatkan dana yang dihasilkan dari suatu aktifitas kejahatan misalnya dengan menggunakan sistem keuangan. Dalam hal ini terdapat pergerakan phisik dari uang tunai, baik melalui penyeludupan uang tunai dari suatu negara ke negara lain, menggabungkan antara uang tunai yang berasal dari kejahatan dengan uang yang diperoleh dari hasil kegiatan yang sah, ataupun dengan memecah uang tunai dalam jumlah besar menjadi jumlah kecil ataupun didepositokan di bank atau dibelikan surat berharga seperti misalnya saham-saham atau juga mengkonversikan ke dalam mata uang lainnya atau transfer uang kedalam valuta asing.

Layering, diartikan sebagai memisahkan hasil kejahatan dari sumbernya yaitu aktifitas kejahatan yang terkait melalui beberapa tahapan transaksi keuangan. Dalam hal ini terdapat proses pemindahan dana dari beberapa rekening atau lokasi tertentu sebagai hasil placement ketempat lainnya melalui serangkaian transaksi yang kompleks yang didesain untuk menyamarkan/mengelabui sumber dana “haram” tersebut. *Layering* dapat pula dilakukan melalui pembukaan sebanyak mungkin ke rekening-rekening perusahaan-perusahaan fiktif dengan memanfaatkan ketentuan rahasia bank, terutama di negara-negara yang tidak kooperatif dalam upaya memerangi kegiatan pencucian uang.

Integration, yaitu upaya untuk menetapkan suatu landasan sebagai suatu ’*legitimate explanation'* bagi hasil kejahatan. Disini uang yang di ‘cuci’ melalui *placement* maupun *layering* dialihkan ke dalam kegiatan-kegiatan resmi sehingga tampak

---

[28] Rick McDonnell, Regional Implementation, Regional Conference on Combating Money Laundering and Terrorist Financing, Denpasar, 17 Desember 2002.

[29] Money Laundering : a Banker;s Guide To Avoiding Problems, (occ.treas.gov/launder/org.htm), hal.2, lihat juga pengertian istilah tersebut pada Penjelasan Umum UU No. 15 Tahun 2002.

tidak berhubungan sama sekali dengan aktifitas kejahatan sebelumnya yang menjadi sumber dari uang yang di-*laundry*. Pada tahap ini uang yang telah dicuci dimasukkan kembali ke dalam sirkulasi dengan bentuk yang sejalan dengan aturan hukum.

Tingginya tingkat perkembangan teknologi dan arus globalisasi di sektor keuangan khususnya perbankan membuat industri ini menjadi lahan yang empuk bagi tindak kejahatan pencucian uang. Pelaku kejahatan dapat memanfaatkan sistem keuangan global untuk kegiatan pencucian uang karena jasa dan produk yang ditawarkan memungkinkan terjadinya lalu lintas atau perpindahan dana dari satu institusi keuangan satu ke institusi keuangan lainnya (pada tahap *layering*) sehingga asal usul uang tersebut sulit dilacak oleh penegak hukum. Bahkan melalui sistem keuangan global pelaku dalam waktu yang sangat cepat dapat memindahkan dana hasil kejahatan melampaui batas yurisdiksi negara, sehingga pelacakannya akan bertambah sulit apalagi kalau dana tersebut masuk ke dalam institusi keuangan yang negaranya menerapkan ketentuan kerahasiaan yang sangat ketat.

Untuk mengamankan sistem keuangan khususnya perbankan, *Financial Action Task Force on Money Laundering* (FATF) mengkategorikan beberapa risiko yang akan dihadapi oleh perbankan dan penyedia jasa keuangan lainnya yang terkait dengan penggunaan institusinya untuk keperluan pencucian uang.[30] Risiko-risiko tersebut antara lain sebagai berikut ：

***1) Politically Exposed Persons* (PEPs)**

Pengertian PEPs menurut *the Basle Committee on Banking Supervision* adalah :

"orang-orang terkemuka yang dipercaya untuk memegang fungsi publik termasuk pimpinan negara atau pemerintahan, politikus senior, pejabat tinggi, pejabat pengadilan atau militer, pejabat eksekutif dari badan usaha milik negara dan pimpinan partai". Orang-orang ini terutama jika datang dari negara dengan masalah korupsi yang cukup serius dapat menyalahgunakan fungsinya untuk keuntungan mereka sendiri melalui penggelapan, penerimaan suap dan kegiatan kriminal lainnya. Pada umumnya hasil kejahatan yang diterima oleh PEPs atau kerabatnya dipindahkan ke

[30] FATF Secretariat, *The Review of The Forty Recommendations FATF on Money Laundering*, 15 April 2002, hal.14-25

negara lain untuk dicuci, disembunyikan dan dilindungi. Hal tersebut dapat terlaksana dengan bantuan pelayanan jasa oleh *private banking* yang memungkinkan pembukaan rekening atas nama orang/pihak lain berupa individu, usaha komersial, *trust*, perusahaan intermediasi atau perusahaan investasi.

Dalam menerima dan menangani dana yang bersumber dari korupsi, bank dan penyedia jasa keuangan lainnya harus menyadari implikasi yang mungkin timbul, antara lain rusaknya reputasi lembaga tersebut, tuntutan pengembalian dari pemerintahnya atau dari individu, tindakan dari otoritas yang berwenang (misalnya kejaksaan) untuk melaksanakan peraturan perundang-undangan yang berlaku atau diajukannya tuduhan melakukan kejahatan pencucian uang. Kasus yang terkenal adalah kasus mantan Presiden Marcos dari Phillpina. [31]

2) Correspondent banking

Correspondent banking adalah hubungan penyediaan jasa perbankan antara satu bank (*correspondent bank*) dengan bank lain (*respondent bank*). Dengan membuat *multiple correspondent relationships world-wide*, bank-bank dapat menjalankan transaksi keuangan internasional untuk mereka sendiri dan nasabahnya dalam suatu yurisdiksi dimana mereka tidak mempunyai kantor cabang. *Correspondent banking* berada ditengah sistem pembayaran internasional yang memungkinkan bank di seluruh dunia melakukan pembayaran kepada dan melalui satu bank kepada bank lain. Efektifitas sistem pembayaran internasional tergantung pada tiga sifat utama yaitu kecepatan, akurasi dan keterjangkauan secara geografis, akan tetapi sifat tersebut justru memudahkan terjadinya pencucian uang. Kecepatan transaksi menyebabkan tidak dimungkinkannya untuk mengidentifikasi dan menahan pembayaran kecuali kedua-duanya baik pengirim maupun penerima dana telah diidentifikasi oleh *handling bank* dan diidentifikasi secara jelas pada *transmittal information*. Sekali kejahatan dana masuk ke dalam sistem pembayaran, sebenarnya hampir tidak mungkin untuk mengidentifikasi dana tersebut karena kecepatan perpindahan dana dari satu bank ke bank lain.

[31] Dalam kasus mantan Presiden Marcos, pada masa pemerintahan Corry Aquino yang bersangkutan telah diputus bersalah (korupsi) oleh Mahkamah Agung Filipina selanjutnya dana hasil korupsi tersebut dikembalikan oleh pemerintah Swiss kepada pemerintah Filipina

Dari sejumlah pedoman yang dikeluarkan oleh beberapa negara, beberapa persyaratan yang diperlukan untuk melawan risiko pencucian uang yang dilakukan melalui hubungan bank koresponden dan bank responden adalah :

1 Bank harus menolak untuk masuk kedalam atau melanjutkan hubungan bank koresponden dengan responden yang tidak berada di suatu yurisdiksi tertentu (*shell bank*) dan bukan merupakan afiliasi dari kelompok keuangan yang terdaftar pada suatu yurisdiksi. Bank juga harus menolak membuka hubungan dengan responden institusi asing yang mengijinkan rekening mereka digunakan oleh *shell banks.*

2 Bank harus menolak untuk membuka hubungan koresponden kecuali koresponden dan responden mempunyai dokumen perjanjian yang menyetujui diterapkannya ketentuan anti pencucian uang sesuai dengan ketentuan yang berlaku.

3 Bank harus menolak membuka hubungan hukum dengan setiap responden kecuali telah puas dengan semua informasi yang telah mereka terima, dan dapat melakukan pemeriksaan secukupnya. Minimal bank dapat mengumpulkan data kepemilikan, manajemen, kegiatan usaha utama serta keberadaan dan lokasi dari bank responden.

3) *Electronic and other Non Face-to-Face Financial services*

Jasa bank yang bersifat elektronis dan jasa keuangan *non face-to-face financial services* sangat rawan terhadap kejahatan pencucian uang. Walaupun Financial Services menetapkan customer wajib menyampaikan identitasnya untuk ditatausahakan, namun bukan tidak mungkin data identitas tersebut dipalsukan. Bagaimana mungkin petugas Financial Services mampu mengidentifikasi keakurasian data identitas yang dikirimkan oleh custemer jika tidak dapat mengecek kebenaran fisik dengan datanya.

4) *Deposits and withdrawals*

Pengambilan tunai, penyetoran/penyimpanan dan transfer dana melalui ATM dan *electronic of sale terminal* yang tidak memerlukan tatap muka antara nasabah dan bank juga sangat efektif untuk digunakan sebagai sarana pencucian uang.

5) ***Electronic money***

Pengertian *electronic money* (*e-money*) adalah sejumlah dana yang telah disimpan dalam medium elektronis dan diterima sebagai pembayaran oleh pihak ketiga. Risiko yang terjadi adalah kemungkinan pengiriman dana (*ciberpayment*)[32] dari pihak ketiga yang tidak dikenal dan ditransfernya dana dari satu kartu ke kartu lainnya. Transfer ini dapat terjadi melalui networks seperti internet, atau melalui penggunaan "*store Value Type Smart Cards*". Risiko terjadinya pencucian uang yang sama juga dapat terjadi pada dompet elektronis (*electronic wallet*) yang penggunaannya semakin berkembang.

Ciberpayment system adalah fenomena baru karena tidak semuanya menuntut kehadiran regulated third party (misalnya bank) dalam transfer financial value diantara kedua belah pihak atau lebih. Produk baru ini di *design* untuk menggantikan "cash" dalam kaitan dengan transaksi konsumen sehingga menurunkan biaya transaksi dan memungkinkan *network connectivity*, namun sekaligus menjadi sarana yang nyaman bagi pencuci uang.[33]

Oleh karena itu ketika *finacial services* termasuk bank hendak menyediakan jasa-jasa dimaksud diperlukan beberapa hal untuk meyakinkan identitas nasabah misalnya satu kali tatap muka dengan nasabah. Dalam *25 core Banking Supervision* yang ditetapkan oleh *Basel Committee,*[34] kepada perbankan agar menyediakan pedoman yang

---

[32] Cyberpayment adalah suatu instrumen baru dari instrumen sistem pembayaran yang mendukung terjadinya transfer nilai secara elektronik.

[33] Ibid

[34] Dalam Basel Committee Publication No.77 tentang Customer due diligence for banks disebutkan pula bahwa bank perlu melakukan penyesuaian-penyesuaian apabila terdapat perubahan dalam dokumen atau pencatatan transaksi nasabah, membentuk sistem informasi yang memudahkan manajemen bank dan compliance officer melakukan identifikasi, analisis dan monitor yang efektif terhadap rekening nasabah yang berisiko tinggi. Di sini termasuk pula sistem pelaporan mengenai dokumentasi yang hilang dan transaksi di luar kebiasaan yang dilakukan melalui rekening nasabah. Bank juga perlu memiliki sistem untuk deteksi setiap aktifitas rekening yang mencurigakan. Hal ini dapat dilakukan dengan menetapkan batasan jumlah untuk kelas atau kategori tertentu dari rekening-rekening yang ada. Selain itu bank perlu membuat suatu daftar mengenai aktifitas-aktivitas yang mencurigakan yang terkait dengan rekening nasabah

menetapkan prosedur yang digunakan oleh bank untuk memeriksa identitas nasabah dan pengawasan yang efektif terhadap pelaksanaan jasa bank dimaksud.

Di samping itu, cyberpayment system telah mendapat perhatian internasional, sebagaimana terlihat pada salah satu rekomendasi Financial Action Task Force on Money Laundering yang secara specifik menyoroti terjadinya money laundering dengan menggunakan cyberpayment (recommendation 8)[35] :

> "Financial Institution should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risk associated with non face to face business relationships or transactions"

Sejalan dengan tuntutan dan kebutuhan untuk melakukan penyesuaian terhadap standar internasional sebagaimana direkomendasikan oleh BIS (Bank for International Settlement), Basle Committee, Bank Indonesia menerbitkan ketentuan Know Your Customer Principle (Prinsip Mengenal Nasabah) dengan PBI No. 3/10/PBI/2001 tanggal 28 Juni 2001 jo. PBI No. 3/23/PBI/2001 tanggal 19 Desember 2001 dan Surat Edaran No. 3/29/DPNP tanggal 19 Desember 2001 mengenai Pedoman Standar Penerapan Prinsip Mengenal Nasabah. Rekomendasi Committee on Banking Regulation and Supervisory Practices mengenai prinsip-prinsip pedoman dalam menghadapi permasalahan money laundering adalah :

a. Semua bank sebaiknya menciptakan prosedur yang efektif dalam memperoleh identitas yang benar atas nasabah baru;
b. Manajemen bank sebaiknya menjamin bahwa kegiatan bisnis yang dilakukannya didasarkan pada standar etika yang tinggi, dan semua peraturan perundang-undangan yang mengatur transaksi keuangan benar-benar dijalankan;
c. Bank-bank bekerjasama secara penuh dengan pihak yang berwenang dalam bidang penegakan hukum, sampai batas-batas maksimal yang diijinkan oleh ketentuan-ketentuan kerahasiaan nasabah yang ada di masing-masing negara;

[35] FATF – GAFI, The Forty Recommendations, 20 Juni 2003

d. Bank-bank mempunyai kebijakan yang konsisten dalam hal pelaporan dan mengkomunikasikan kebijakan tersebut ke seluruh karyawannya yaitu dengan melakukan pelatihan staf, pengembangan prosedur spesifik dalam pengidentifikasian nasabah, penyimpangan internal, dan pengembangan prosedur audit internal.

Penerapan Prinsip Mengenal Nasabah (*Know Your Customer Principles*) dimaksudkan dapat mendorong terselenggaranya prinsip kehati-hatian dalam rangka mengurangi risiko usaha yang dihadapi bank dalam menjalankan kegiatan usaha yaitu *operational risk, legal risk, concentration risk,* dan *reputational risk.* Prinsip Mengenal Nasabah merupakan salah satu upaya untuk mencegah agar sistem perbankan tidak digunakan sebagai sarana kejahatan pencucian uang, baik yang dilakukan secara langsung maupun tidak langsung oleh pelaku kejahatan.

Sejalan dengan itu, terhadap Prinsip Mengenal Nasabah (KYC) bagi lembaga keuangan non bank, Departemen Keuangan melalui Keputusan Menteri Keuangan No. 45/KMK.06/2003 tanggal 30 Januari 2003 telah mengeluarkan KYC bagi lembaga non khusus industri perasuransian, dana pensiun dan lembaga pembiayaan. Sebelumnya pada tanggal 15 Januari 2003, Bapepam telah pula mengeluarkan Keputusan Ketua Bapepam No. KEP-02/PM/2003 Tentang KYC yang ditujukan bagi pelaku pasar modal.

Kedua ketentuan tersebut pada intinya bertujuan untuk menciptakan industri keuangan non bank yang sehat dan berstandar internasional serta terlindungi dari kemungkinan disalahgunakan untuk kejahatan keuangan dengan cara mengenal transaksi yang dilakukan nasabahnya.

Di samping hal di atas, guna memenuhi standard internasional dalam memperkuat rezim anti pencucian uang serta bukti nyata kepedulian Indonesia seperti halnya dengan negara-negara lain, adalah disahkannya Undang-Undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang pada tanggal 17 April 2002[36]. Produk hukum ini memberi landasan hukum yang kokoh dalam upaya pencegahan dan pemberantasan tindak pidana pencucian uang, sekaligus bukti nyata komitmen Indonesia untuk bersama-sama dengan masyarakat internasional bekerjasama menangkal setiap bentuk kejahatan

[36] RUU amandemen UU No. 15 Tahun 2002 telah disetujui oleh DPR dalam Rapat Paripurna tanggal 16 September 2003

money laundering dalam berbagai dimensi yang ada. Undang-undang ini bukan saja telah menyatakan, bahwa perbuatan pencucian uang merupakan suatu tindak pidana, tetapi juga telah melahirkan suatu lembaga baru yang bernama Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK). Dalam praktek internasional di bidang pencucian uang lembaga semacam dengan PPATK disebut dengan nama generik *Financial Intelligence Unit* (FIU).

Selanjutnya, berdasarkan Pasal 26 huruf (e) UU TPPU, PPATK mempunyai tugas antara lain mengeluarkan pedoman untuk membantu PJK dalam mendeteksi perilaku nasabah yang mencurigakan dalam melakukan hubungan usaha dengan PJK.

Terhadap Penyedia Jasa Keuangan, Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK)[37] telah mengeluarkan pedoman sebagaimana tertuang dalam Keputusan Kepala Pusat Pelaporan dan Analisis Transaksi Keuangan Nomor: 2/1/KEP.PPATK/2003 tanggal 9 Mei 2003 tentang Pedoman Umum Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang Bagi Penyedia Jasa Keuangan. Di samping itu PPATK juga mengeluarkan pedoman lain yaitu Keputusan Kepala Pusat Pelaporan dan Analisis Transaksi Keuangan Nomor: 2/4/KEP.PPATK/2003 tanggal …. 2003 tentang Pedoman Identifikasi Transaksi Keuangan Mencurigakan Bagi Penyedia Jasa Keuangan. Pedoman ini diberlakukan bagi bank umum, BPR, perusahaan efek, pengelola reksa dana, bank kustodian, perusahaan perasuransian, dana pensiun, dan lembaga pembiayaan. Selanjutnya, pedoman yang sama akan dikeluarkan terhadap Penyedia Jasa Keuangan berbentuk Jasa Pengiriman Uang dan Pedang Valuta Asing. Sementara itu, terhadap Penyedia Jasa Keuangan yang menyediakan jasa lainnya yang terkait dengan keuangan, seperti lembaga yang menerbitkan kartu telepon (satelindo dan telkomsel), konsultan keuangan, konsultan hukum, dealer mobil, dan lain-lain dapat menjadi *loophole* dalam pembangunan rezim anti pencucian uang karena lembaga-lembaga ini untuk sementara tidak menjadi pihak yang wajib melaporkan transaksi

[37] Berdasarkan Pasal 18 UUTPPU, untuk mencegah dan memberantas tindak pidana pencucian uang, dibentuk PPATK sebagai lembaga yang independen dalam melaksanakan tugas dan kewenangannya, bertanggung jawab kepada Presiden.

mencurigakan dan transaksi kas-nya[38], sehingga pencuci uang dapat dengan leluasa melakukan pencucian. Lebih dari itu, jika ternyata bisnis dengan menggunakan sarana elektronik atau teknologi informasi di Indonesia semakin berkembang, seperti munculnya lembaga non bank yang menerbitkan e-cash[39], maka lembaga ini akan dijadikan sarana pencucian uang yang marak. Lembaga-lembaga semacam ini bukanlah *reporting parties* (pihak-pihak yang diwajibkan oleh undang-undang menyampaikan laporan transaksi keuangan mencurigakan dan laporan transaksi cash) sehingga petugas akan kesulitan dalam menangkap pelaku pencuci uang.

Namun demikian, apabila dikemudian hari berdasarkan konvensi atau rekomendasi internasional, atau juga sesuai hasil pengkajian PPATK[40] memandang perlu suatu lembaga yang menyediakan jasa yang terkait dengan keuangan ternyata rawan terhadap praktik pencucian uang, maka lembaga-lembaga (*institution*) dimaksud diwajibkan menjadi pihak pelapor (*reporting parties*), baik melaporkan transaksi tunai (*Cash Transaction Report* - CTR) maupun traksaksi keuangan mencurigakan (*Suspicious transaction Report* - STR)

Pada dasarnya yang dimaksud dengan istilah "Transaksi Keuangan Mencurigakan" (STR) adalah transaksi yang menyimpang dari kebiasaan atau tidak wajar dan tidak selalu terkait dengan tindak pidana tertentu. Transaksi Keuangan Mencurigakan tidak memiliki ciri-ciri yang baku, karena hal tersebut dipengaruhi oleh variasi dan

[38] Berdasarkan Pasal 13 ayat 1 UU No. 15 tahun 2002 tentang Tindak Pidana Pencucian Uang ("UU TPPU"), Penyedia Jasa Keuangan ("PJK") seperti bank, lembaga pembiayaan, perusahaan efek, pengelola reksa dana, kustodian, wali amanat, lembaga penyimpanan dan penyelesaian, pedagang valuta asing, dana pensiun, dan asuransi, wajib menyampaikan laporan Transaksi Keuangan Mencurigakan dan laporan transaksi tunai kepada Pusat Pelaporan dan Analisis Transaksi Keuangan ("PPATK") sebagai upaya untuk mendeteksi kegiatan pencucian uang sejak dini. Selanjutnya Pasal 1 angka 5 RUU tentang Perubahan UUTPPU mendifinisikan pengertian Penyedia Jasa Keuangan yaitu setiap orang yang menyediakan jasa di bidang keuangan atau jasa lainnya yang terkait dengan keuangan termasuk tetapi tidak terbatas pada bank, lembaga pembiayaan, perusahaan efek, pengelola reksa dana, kustodian, wali amanat, lembaga penyimpanan dan penyelesaian, pedagang valuta asing, dana pensiun, perusahaan asuransi, dan kantor pos.

[39] Pengguna membeli E-cash pada dari issuer non bank dengan menggunakan cash money dan membelanjakan e-cash pada merchant yang berpartisipasi dalam skim tersebut. Issuer selanjutnya akan mengganti e-cash dari merchant dengan uang cash, misalnya produk DigiCash dan CyberCash

[40] Pasal 44B RUU RI tentang Perubahan atas UU TPPU (telah disetujui DPR RI) menyebutkan, dalam hal ada perkembangan konvensi internasional atau rekomendasi internasional di bidang pencegahan dan pemberantasan tindak pidana pencucian uang, PPATK dapat melaksanakan ketentuan tersebut menurut Undang-Undang ini sesuai dengan peraturan perundang-undangan.

perkembangan sistem keuangan yang ada. Meskipun demikian, terdapat ciri-ciri umum dari Transaksi Keuangan Mencurigakan yang dapat dijadikan acuan, sebagai berikut :

3. Tidak sesuai dengan tujuan komersial yang wajar
4. Menggunakan uang tunai dalam jumlah yang sangat besar dan/atau dilakukan secara berulang-ulang di luar kewajaran
5. Aktivitas nasabah diluar kebiasaan dan kewajaran.

Perlu digarisbawahi bahwa dalam memastikan/meyakini terjadinya Transaksi Keuangan Mencurigakan, PJK sedapat-dapatnya melakukan verifikasi terlebih dahulu terhadap transaksi tersebut. Apabila dari hasil verifikasi tersebut PJK meyakini bahwa transaksi tersebut diluar kewajaran atau tidak mendapat jawaban yang memuaskan maka kemudian PJK dapat melaporkan transaksi tersebut kepada PPATK sebagai Transaksi Keuangan Mencurigakan. PJK juga diperkenankan meminta dokumen pendukung transaksi yang dilakukan oleh nasabah apabila diperlukan. Dalam pelaporan Transaksi Keuangan Mencurigakan, yang menjadi objek kecurigaan adalah transaksi itu sendiri, bukan orang atau nasabah yang melakukan transaksi.

Berdasarkan UU TPPU, Transaksi Keuangan Mencurigakan pada prinsipnya terdiri dari 3 unsur, yaitu :

- Transaksi yang menyimpang dari profil dan karakteristik serta kebiasaan pola transaksi dari nasabah yang bersangkutan.
- Transaksi yang patut diduga dilakukan dengan tujuan untuk menghindari pelaporan yang wajib dilakukan oleh PJK.
- Transaksi keuangan yang dananya diduga berasal dari hasil kejahatan.

Beberapa indikator Transaksi Keuangan Mencurigakan adalah antara lain sebagai berikut :

1. Transaksi Transfer dana :
    - Transfer dana untuk dan dari offshore financial centre yang berisiko tinggi tanpa alasan usaha yang jelas.
    - Penerimaan/pengiriman dana dalam beberapa tahap dengan perbedaan jumlah yang signifikan antara penerimaan yang pertama dengan penerimaan berikutnya.

- Penerimaan/pembayaran dana dalam kegiatan ekspor impor yang tidak disertai dokumen yang lengkap.
- Transfer dana dari atau ke negara yang tergolong high risk.
- Transfer dana dari atau ke pihak yang tergolong high risk.
- Penerimaan/pembayaran dana dengan menggunakan lebih dari 1 (satu) rekening baik atas nama yang sama atau atas nama yang berbeda.

2. Nasabah membuka rekening hanya untuk jangka pendek saja.
   - Off-shore company yang terletak di negara bebas pajak atau negara yang ketat dalam penerapan rahasia bank.
   - Usaha yang berbasiskan uang tunai
   - Organisasi sosial
   - Cyber company
3. Negara/teritorial

   Dalam mengidentifikasikan suatu Transaksi Keuangan Mencurigakan, perlu diperhatikan negara pengirim dana, negara penerima dana, dan negara asal nasabah. Hal ini perlu dilakukan karena apabila dana tersebut berasal atau dikirimkan ke negara yang terkenal sebagai produsen narkoba maka dimungkinkan adanya keterkaitan dana tersebut dengan penjualan narkoba. Negara/teritorial yang perlu mendapat perhatian adalah negara/teritorial yang tergolong berisiko tinggi (*high risk country*) seperti :

   - Kawasan *offshore financial center*.
   - Tax heaven countries/teritories.
   - Negara-negara yang dikenal sebagai produsen narkoba.
   - Non-Cooperative Countries and Teritories sesuai dengan penetapan FATF.

Pengenalan terhadap transaksi keuangan mencurikan di atas, sangat erat dengan tahapan proses kegiatan money laundering. Dari tiga proses kegiatan pencucian uang (*placement, layering dan integration*), kegiatan pada tahapan *placement* merupakan titik terlemah dalam proses pencucian uang karena pada tahap *placement* inilah sebenarnya praktik money laundering paling mudah dideteksi. Setelah *placement*, tahapan money

laundering berikutnya secara umum adalah *layering*. Pada tahapan ini, pencuci uang dengan leluasa memindahkan dananya secara cepat dan mudah melalui *cyberpayment system*, termasuk menggunakan sarana offshore banking. Dengan telah masuknya uang pada tahapan ini maka akan sulit sekali dilacak oleh petugas. Apabila tahapan ini terlewati maka pencuci uang dapat dengan mudah melakukan integrasi atas uang hasil kejahatannya (*Proceed of crime*), sehingga akan sulit dibedakan antara uang tidak sah dengan legal lainnya.

Ketatnya pengaturan seperti kewajiban bagi PJK dalam penerapan Prinsip Mengenal Nasabah (*Know Your Customer Principles*), kewajiban menciptakan prosedur yang efektif dalam memperoleh identitas nasabah, dan ketersediaan pedoman bagi PJK dalam melakukan identifikasi transaksi nasabah yang mencurigakan, serta kewajiban PJK melaporkan setiap adanya transaksi mencurigakan, karena disadari bahwa tanpa pengaturan demikian maka rezim *anti money laundering* sulit dibangun.

Masih dalam konteks perkembangan telematika, ternyata masih membawa persoalan lain yaitu mengenai persfektif hukum pembuktian, yaitu apakah data eletronik termasuk *digital signature*[41] dapat dijadikan sebagai alat bukti yang sah dalam hukum pembuktian di Indonesia. Pasal 38 UU TPPU, disebutkan bahwa alat bukti pemeriksaan tindak pidana pencucian uang berupa :

a. alat bukti sebagaimana dimaksud dalam Hukum Acara Pidana, yaitu bukti tulisan, bukti dengan saksi, persangkaan-persangkaan, pengakuan, dan sumpah

b. alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu,

c. Pasal 1 angka 9 RUU TPPU, dokumen adalah data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa

[41] W. Diffie & M.E. Hellman dalam tulisannya "*New Directions in Crytography*" menyatakan "*Digital Signature is a specific term of art within the technical community that has been used consistently since the lancdmark publication describing public key cryptography*" : Dikutip oleh R.R. Jueneman dan R.J. Robertson, Jr. dalam tulisan berjudul " Biometrics and Digital Signatures in Electronic Commerce" dimuat dalam Jurimetrics ASU, Volume 38, Spring 1998, Number 3, hal. 437

bantuan suatu sarana, baik yang tertuang di atas kertas, atau yang terekam secara elektronik, termasuk tetapi tidak terbatas pada :

- tulisan, suara, atau gambar
- peta, rancangan, foto, atau sejenisnya
- huruf, tanda, angka, symbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.

Dengan demikian, sudah tidak menjadi persoalan lagi khusus dalam rangka penuntutan dan pemeriksaan di sidang pengadilan dalam kasus tindak pidana pencucian uang dengan menggunakan alat bukti dalam bentuk data elektronis.

Di samping itu, sesuai dengan sifat money laundering yang merupakan kejahatan transnasional, maka tindak pidana pencucian uang di samping berhadapan dengan individu dan organisasi juga terhadap bangsa dan negara. Sifat ini menjadi universal dan menembus batas-batas yurisdiksi negara, sehingga masalahnya bukan saja bersifat nasional, tetapi juga masalah regional dan internasional[42]. Seperti yang telah dikemuakan di atas bahwa praktik money laundering bisa dilakukan secara mudah dan cepat dengan memanfaatkan kemajuan teknologi informasi melalui sistem cyberspace (internet), dimana pembayaran melalui bank secara elektronik (cyberpayment) dapat dilakukan. Hal ini membawa tantangan baru terkait dengan pencegahan dan pemberantasan tindak pidana pencucian uang, dan kompetensi yurisdiksi dalam penanganan tindak pidana pencucian uang. Oleh karena itu, bentuk kerjasama internasional merupakan hal yang mutlak dan tidak dapat ditawar-tawar lagi.

Kebutuhan kerjasama tersebut telah disadari oleh FATF sesuai dengan The Forty Recommendations of the Financial Action Task Force on Money Laundering (FATF), antara lain dalam bentuk :

a. *Mutual Legal Assistance* (MLA) antar Pemerintah, sesuai rekomendasi ke 33 :

> "Countries should try to ensure, on bilateral or multilateral basis, that different knowledge standards in national definitions – i.e different standards concerning

[42] N.H.C. Siahaan, SH., MH, Pencucian Uang dan Kejahatan Perbankan, Pustaka Sinar Harapan, Jakarta, 2002, hal.3

the intentional element of the infraction – do not affect the ability or willingness of countries to provide each othe with mutual legal assistance".

Saat ini Indonesia telah melakukan MLA dengan Australia, China dan Korea Selatan, serta perjanjian ekstradisi dengan Australia, Hongkong, Filipina, Thailand, Korea Selata, dan Malaysia.

b. Pertukaran informasi (*information axchange)* antar FIU, sesuai dengan rekomendasi ke –32, yaitu :

"Every countries should make efforts to improve a spontaneous or "upon request" international information exchange relating to suspicious transactions, person and comparations involved inthose transactions between competent authorities. Strict safeguards should be established to ensure that this exchange of information is consistent with national and international provisions on privacy and data protection".

Indonesia telah menandatangani Agreement on Information Exchange and Communication Procedures dengan Malaysia dan Filipina, kemudia Kamboja dan Thailand ikut juga menandatangani. Di samping itu, PPATK sebagai FIU saat ini telah menandatangani perjanjian mengenai pertukaran informasi inteligen berkaitan dengan tindak pidana pencucian uang dan pembiayaan terorisme dengan Thailand dan Malaysia. Ke depan perjanjian semacam itu akan di tingkatkan FIU negara lain termasuk Korea FIU yang akan ditandatangani pada tanggal 20 Oktober 2003 di PPATK.

Jakarta, Oktober 2003