

## El lavado de dinero y las nuevas tecnologías

Dr. James A. Graham<sup>1</sup>

La Cábala establece en su segunda ley de la Trinidad, las tres madres: Aleph, Mem, y Schin, - el bien, el mal y la justicia para restablecer el equilibrio<sup>2</sup>. A su vez la justicia comporta una dualidad típicamente taoísta, tal como lo han enseñado los *cheng-jeng* hace miles de años<sup>3</sup>: el derecho y la criminología, uno que no tiene sentido sin el otro. El ultimo para prevenir; el primero para reprimir (lo que no se pudo prevenir). Y no hay mejor tema para ilustrar la interacción y la complementariedad de ambas disciplinas que el del lavado de dinero en relación con el uso de las nuevas tecnologías.

La primera clave en la lucha contra el lavado de dinero consiste en responsabilizar, bajo sanción, aquellos que participan de manera indirecta a su realización, sea los banqueros, los contadores o los abogados entre otros. Sin embargo, por su carácter transnacional, el Internet obliga hoy a los actores a conocer más que su simple marco legal local: por el efecto de la extraterritorialidad legislativa<sup>4</sup>, casi todas las leyes del mundo pueden aplicarse y así constituir un riesgo de condenación penal para el actor local. Y la prevención implica el entendimiento de varias nociones técnicas como la criptografía o el *Peer-to-Peer*<sup>5</sup>.

La prevención, especialmente en caso de duda, permite la violación de la libertad de comercio. En efecto, como lo subrayó la Corte constitucional colombiana, un banco tiene la obligación “constitucional” de rechazar un cliente si hay sospecha, porque el “valor” del combate al lavado de dinero es superior a el de la libertad de comercio:

---

<sup>1</sup> Profesor de posgrado de la Facultad de Derecho y Criminología de la UANL. Miembro nivel II del SNI.

<sup>2</sup> *Sepher Ietzirah*, II,1.

<sup>3</sup> Lie Tseu, *Tchoung niu-tchen king*, T'ien jouei, 2.

<sup>4</sup> Graham, *Lectures about the Legal System of the United States*, 3a ed., 2007, Lecture #26; The Harvard Research project on Codification of Jurisdiction Principles under International Law, 29 *Am.J.Int'L*. 435, 445 (1935).

<sup>5</sup> El autor se reserva para fines pedagógicos la facultad de utilizar ciertos términos ingleses en la medida que ellos son utilizados en el lenguaje común, al contrario de las traducciones españolas, así como el empleo de neologismos a fin de describir nuevas situaciones o técnicas.

*La Corte Constitucional, en esta sentencia de revisión de un fallo de tutela proferido por el Juzgado Sexto Penal del Circuito de Cali, sentó la siguiente doctrina en relación con el acceso a servicios financieros de personas que figuren en listas internacionales como vinculadas al lavado de activos, en este caso particular, en la llamada "Lista Clinton":*

- 1) La necesidad de velar por el interés general de los ahorradores y de preservar la estabilidad del sistema financiero, exige que la autonomía de voluntad privada de las entidades financieras se imponga como regla general, al momento de decidir acerca del acceso, contenido y prestación de los servicios bancarios (principio de confianza pública). Sin embargo la autonomía de la voluntad privada se encuentra limitada por el interés público que involucra la actividad bancaria y el respeto del núcleo esencial de los derechos fundamentales del cliente, los cuales se consideran transgredidos cuando ocurre un bloqueo financiero injustificado*
- 2) En el caso objeto de estudio por parte de la Corte, el bloqueo financiero injustificado no se presenta en la medida en que existe un medio administrativo de defensa para que las personas incluidas en la lista Clinton puedan proteger y amparar sus derechos fundamentales y se presenta una causal objetiva y razonable que justifica la negativa de negociación de las entidades bancarias demandadas.*
- 3) En efecto, para la Corte la inclusión de una persona en la lista Clinton, es una causal objetiva que justifica el que las entidades financieras se abstengan de iniciar o mantener relaciones comerciales con personas que figuren en la misma.*
- 4) Dicha causal se encuentra vinculada al riesgo de la operación en razón a las consecuencias de tipo económico que podrían derivarse para la banca colombiana v.g. por la confiscación de sumas*

*depositadas en sucursales o agencias del exterior o por la terminación de los contratos de corresponsalía con la banca extranjera. Igualmente por la pérdida de confianza pública derivada del riesgo reputacional y por las posibles sanciones o multas derivadas de falta de control al lavado de activos.*

- 5) *Para la Corte no resulta necesario que la persona incluida en la lista Clinton, haya sido condenada o esté siendo investigada por delitos relacionados con el narcotráfico en Colombia, para considerar legítima la conducta de las entidades bancarias, en razón a que el fundamento objetivo de dicha decisión reposa en el peligro inminente de una pérdida de solvencia y de liquidez que altere de manera irremediable al sistema financiero y, por ende, afecte al interés general de los ahorradores (principio de la confianza pública<sup>6</sup>.*

Consecuentemente, la búsqueda de soluciones tecnológicas para prevenir el lavado de dinero (Sección II) se hace en un marco técnico y legal (Sección I). Por una mejor comprensión del tema, sin embargo es conveniente, a título preliminar, ver cuáles pueden ser las hipótesis de lavado de dinero en el Internet.

### **Sección preliminar: El marco hipotético**

En su informe publicado en 2001, la *Financial Action Task Force on Money Laundering*<sup>7</sup> dio cuenta de algunos ejemplos reales de lavado de dinero a través del Internet. Un método consiste en crear una empresa proponiendo servicios pagados por Internet como por ejemplo un proveedor de música en línea. El “lavador” usa en seguida estos servicios y lo paga con tarjetas de crédito o de débito vinculadas con cuentas bancarias que él controla (cuentas probablemente situadas en una zona *offshore*) y sobre las cuales él

---

<sup>6</sup> Sala Quinta de Revisión, sentencia T-468, 2003 (inédita).

<sup>7</sup> LA FATF fue creada durante la junta del Grupo de los Siete (G-7) realizada en París en 1989. Sus informes de 2000 y 2001 ponen a la luz el papel del Internet en las operaciones de lavado de dinero y sus recomendaciones insisten sobre diversas soluciones, que son esencialmente de naturaleza técnica ([www.fatf-gafi.org](http://www.fatf-gafi.org)).

pone el producto de sus actividades criminales. En este ejemplo, el lavador controla solamente las cuentas cargadas y la sociedad de prestación de servicios en línea. El proveedor de Internet, el servicio de facturación en línea, la sociedad de tarjeta de crédito y el banco en donde se encuentran las cuentas no tienen ninguna razón para ser recelosos. En otros términos, el método consiste en descomponer el proceso fraudulento en pedazos individuales lícitos a fin de no parecer sospechoso.

Un en segundo ejemplo, estamos en presencia de una sociedad X en un país A que explota un casino virtual en el Internet a través de un servidor situado en el país B del Caribe y las apuestas se hacen vía tarjeta de crédito. Una sociedad Y, establecida en el país C del Caribe, compro el nombre de dominio <game.com>; después lo vendió a una empresa C, establecida en un país D en el Medio Oriente. El jugador apostó y en caso de ganar, recuperó el doble de la suma. El lavado consiste entonces en utilizar un servicio de juego considerado legal en un país offshore y pretender haber ganado el dinero lavado.

En el tercer ejemplo, se trata de la situación contraria en donde estamos en presencia de un lavado de dinero ganado a través de un casino virtual ilegal. Una organización criminal estableció una sociedad de apuestas y de prestación de servicios de Internet en el país A. El casino virtual se ubicó en un servidor en el Caribe en donde estas actividades fueron lícitas. Con el fin de lavar este dinero en el país E en donde la actividad es formalmente prohibida – se trato de un montó anual de 178 millones de dólares -, la organización criminal recurrió a un despacho de abogados que crearon diversas empresas que prestaron sus servicios exclusivamente a los miembros de la red criminal. Los beneficios de las empresas fueron depositados en cuentas bancarias offshore en el Caribe, en seguida transferidos a cuentas europeas.

El cuarto ejemplo tiene por objeto una persona en un país D quien crea una sociedad de juego *Gamblerz.com* en un país E sin obtener una licencia de juego. El nombre de la sociedad es muy similar al de una empresa de juego en el país F *Gamblers.com* que está operando legalmente con licencia. Después, un sitio Web es creado con un servidor en el país G con el nombre <gambler.com> y

una cuenta bancaria en línea es abierta en el país H. En un último movimiento Gambler.com apunta a los clientes del país J. Aprovechando la confusión de nombres, el dinero pasa a través las redes legales.

El último ejemplo se basa en el mecanismo conocido como el *hawala*<sup>8</sup>, que funciona más o menos como el método del *mercado negro del peso*. En el mundo material se trata de un narcotraficante que vende drogas en un país C contra dólares. Los beneficios se remiten a un intermediario – el *hawaladar* – en el mismo país donde normalmente tiene una empresa. Éste se busca un *hawaladar* correspondiente en el país D, país de origen del proveedor de las drogas, y le factura servicios o mercancías en dólares. El correspondiente paga en moneda local. Sin embargo se aplicará una tasa de cambio más alta de lo normal, permitiendo así al narcotraficante C de pagar a su proveedor D. La hipótesis “virtual” consistiría en que el criminal C explota un casino virtual ilegal y cobra los beneficios en moneda virtual – *cybercash* -, que es totalmente anónima e imposible de retrazar<sup>9</sup>. Sin embargo, por el momento el *cybercash* no está muy desarrollado y nuestra hipótesis es difícilmente realizable. Por lo tanto estamos seguros que en un futuro no muy lejano, las cosas cambiarán. Para entenderlo, se necesita no solamente conocer el marco legislativo, sino también el ambiente tecnológico.

## Sección I: El marco tecno-jurídico

Desde hace muchos años defendemos el concepto de la *tecnología & derecho*, significando que el derecho del comercio electrónico no es solamente “derecho”; se necesita una aprehensión muy profunda de la tecnología a fin de poder definir de manera inteligente el marco normativo<sup>10</sup>; en otras palabras, la criminología se pone al servicio del derecho. Consecuentemente presentamos en un

---

<sup>8</sup> La misma hipótesis podría realizarse a través otros métodos como el *Hundi*, el *sistema chino*, o la *IVA del carrusel* (sobre este último véase el informe del GAFI: *Laundering the proceeds of VAT Carousel Fraud*, 2007, [www.fatf-gafi.org](http://www.fatf-gafi.org))

<sup>9</sup> Graham, *La monnaie virtuelle: une nouvelle monnaie privée ?*, *CBLJ*, mayo 2002, [www.cyberbanking-law.de](http://www.cyberbanking-law.de).

<sup>10</sup> Graham, *New Paradigms in Cyberlaw: U-biz*, *RDI*, #3, 2002, [www.alfa-redi.org](http://www.alfa-redi.org).

primer movimiento el marco tecnológico (A), y, en un segundo movimiento el marco legal (B).

## **A - El marco tecnológico**

Presentáremos de manera breve una técnica de *hacking* muy utilizada que explica en que medida el delito financiero puede operarse de manera tan fácil (a) y una nueva concepción del Internet que tiene por objetivo realmente a-localizar una red ya de-localizada<sup>11</sup> (b).

### **1) El spoofing**

Un método para identificar los autores de actividades ilegales en un sitio Web, es buscar al dueño del nombre de dominio a través del registro del *WhoIS*. En nuestro ejemplo, a través de una búsqueda del nombre <games.com> es posible identificar aquel o aquella que registró el nombre de dominio así como su dirección. Así, a fin de evitar eso, la idea consiste en mascar el nombre de dominio a través de una “transformación”. El truco, conocido como el *DNS Spoof*, consiste en cambiar “games.com” en un valor hexadecimal o en una base *dbase* 4 o 8: el nombre de dominio visible será “http://%4344%3434%34564”<sup>12</sup> en lugar de “http://www.games.com”. Sin embargo, una dirección en hexadecimal parece inmediatamente rara y puede despertar sospechas. Desde luego, es suficiente con registrar varios nombres de dominio – con diferentes titulares a través del mundo – y utilizarles sobre servidores que funcionan como *proxy*. Por ejemplo, una segunda maquina se registra bajo <games2.com> ante un proveedor de Internet. Esté no verá nada sospechoso porque el servidor <games2.com> tendrá un contenido licito como por ejemplo la publicación de información sobre juegos electrónicos. Pero en realidad, este servidor funcionará también como proxi para el “http://%4344%3434%34564”, que en realidad es el <games.com>. Además, a través de varios *javascripts*, es posible que <games.com> tenga cada minuto otro valor numérico. La “invisibilidad” puede ser completa si se utiliza además un sistema peer-to-peer.

---

<sup>11</sup> Para el tema de la a-localización y la de-localización en material de arbitraje internacional, véase Graham, La delocalización del arbitraje virtual, *RLMA*, #1, 2001.23, [www.med-arb.net](http://www.med-arb.net).

<sup>12</sup> Valor ficticio.

## 2) El Peer-to-Peer

El peer-to-peer tiene su fama por el caso *Napster*<sup>13</sup>, aunque su origen es mucho más antiguo. En realidad, la técnica es anterior a esta del Internet. Se trata de conectar dos computadoras, ambas teniendo por función la de ser cliente y servidor. En otras palabras, es normalmente la configuración clásica de las redes que las personas tienen en sus casas o en pequeñas oficinas o tiendas. Las grandes redes, y *a fortiori* Internet, se basan al contrario sobre una configuración de cliente/servidor. El punto débil de esta infraestructura para las actividades criminales consiste entonces en el servidor; si el dueño de este último está descubierto, toda la organización calla – como lo vimos para Napster. De ahí, la idea de eliminar este punto débil y de utilizar a través del Internet la técnica del peer-to-peer, en donde todas las máquinas conectadas son a la vez cliente/servidor, como lo vemos en el marco del proyecto *Gnutella*<sup>14</sup>.

La ventaja del peer-to-peer consiste esencialmente en el hecho de que no se necesita una dirección IP fija como es el caso para el Internet. Y sin dirección fija, no es posible identificar al dueño de una computadora. En otros términos, si retomamos nuestro ejemplo de <games.com>, en un marco de peer-to-peer, no hay necesidad de tener un nombre de dominio, un servidor con una dirección IP, etc... Es suficiente entregar a los clientes una palabra clave y ya, ellos pueden conectarse y nadie, realmente nadie puede saber quien es quien y donde está.

El peer-to-peer puede tener muchas caras y su evolución consiste en crear varias “Internets” virtuales en el Internet como lo vemos con *Freenet*<sup>15</sup> o, en configuraciones más sofisticadas, con *Safe-X* que ofrece además de la técnica del peer-to-peer, una comunicación totalmente encriptada y más allá de la delocalización por la combinación con el GPRS<sup>16</sup> o el UMTS<sup>17</sup> a través de redes

---

<sup>13</sup> [www.napster.com](http://www.napster.com).

<sup>14</sup> [www.gnutelliums.com](http://www.gnutelliums.com).

<sup>15</sup> [www.freenet.org](http://www.freenet.org).

<sup>16</sup> *Global Package Radio System*.

móviles. Tecnología de punto, Safe-X pone al mal el marco legal actual.

## **B – El marco legal**

Según la jerarquía normativa<sup>18</sup> presentamos primero el derecho internacional (a). En segundo lugar, queremos también mencionar el derecho comunitario en la medida en que la Unión europea tiende más y más a dar efectos extraterritoriales a su normatividad (b). Por último, consideramos al derecho nacional, que en nuestra hipótesis es el derecho mexicano (c).

### **1) Derecho Internacional**

En ausencia de cualquier texto específicamente dirigido a los problemas de lavado de dinero en el Internet, el jurista tiene que referirse a las convenciones existentes. Sin analizar estos convenios, señalamos solamente que se aplican los acuerdos vigentes en materia de lucha contra el narcotráfico<sup>19</sup>, especialmente las convenciones de las Naciones Unidas, el Reglamento de la CICAD<sup>20</sup>, las resoluciones onusianas contra la lucha al terrorismo o la convención contra la corrupción de agentes públicos de la OCDE, entre otros. Desgraciadamente, se debe constar que se trata aquí de una normatividad disparada, al contrario del derecho en vigor en la Unión europea.

### **2) Derecho comunitario**

Uno de los sistemas más desarrollados en materia de lucha contra el lavado de dinero es el derecho comunitario, cuyo texto

---

<sup>17</sup> *Universal Mobile Telecommunication System*, más conocido como el GMS 3G (tercer generación).

<sup>18</sup> Recordemos que no obstante la posición monista nacionalista del Constituyente mexicano, el derecho internacional es imperativamente superior a cualquier orden nacional, como lo subrayó la Corte internacional en el asunto *Detroit de Corfou* (1949) y como lo especifica la Convención de Viena sobre el derecho de los tratados.... ¡ratificada también por México!

<sup>19</sup> 19/12/88.

<sup>20</sup> *Reglamento sobre el Lavado de Activos Relacionados con el Trafico Ilícito de Drogas* de la Comisión interamericana para el Control de Abuso de Drogas (OEA).

fundamental es la directiva del 10 de junio de 1991<sup>21</sup>, actualizada por los Principios emitidos por la Comisión europea en 1996. Estos últimos exigen la garantía de una identificación adecuada y prohíben las operaciones sospechosas. A fin de conferir un carácter jurídico a estos principios, la Comisión propuso en 1999 una nueva directiva que retoma el contenido de los Principios. Esta Tercera Directiva Europea sobre Blanqueo de Capitales fue finalmente aprobada en junio de 2005. Aunque la directiva no prevea una aplicación extraterritorial de sus disposiciones, el Tratado de Libre Comercio entre México y la Unión europea tendrá probablemente por efecto que las instituciones financieras mexicanas van a proyectar la apertura de filiales en Europa. Consecuentemente, el conocimiento de las reglas comunitarias son un requisito obligatorio, además del conocimiento del derecho nacional.

### 3) Derecho mexicano

En ausencia de disposiciones específicas para las hipótesis “virtuales”, se trata de aplicar las disposiciones actuales a los nuevos fenómenos. De lado de la incriminación general del artículo 400-bis del Código penal federal<sup>22,23</sup>, completado por el decreto del 10 de

---

<sup>21</sup> Zamora Sánchez, Marco jurídico del lavado de dinero, Oxford, 2001. 25.

<sup>22</sup> *Se impondrá de cinco a quince años de prisión y de mil a cinco mil días multa al que por sí o por interpósita persona realice cualquiera de las siguientes conductas: adquiera, enajene, administre, custodie, cambie, deposite, dé en garantía, invierta, transporte o transfiera, dentro del territorio nacional, de éste hacia el extranjero o a la inversa, recursos, derechos o bienes de cualquier naturaleza, con conocimiento de que proceden o representan el producto de una actividad ilícita, con alguno de los siguientes propósitos: ocultar o pretender ocultar, encubrir o impedir conocer el origen, localización, destino o propiedad de dichos recursos, derechos o bienes, o alentar alguna actividad ilícita.*

*La misma pena se aplicará a los empleados y funcionarios de las instituciones que integran el sistema financiero, que dolosamente presten ayuda o auxilien a otro para la comisión de las conductas previstas en el párrafo anterior, sin perjuicio de los procedimientos y sanciones que correspondan conforme a la legislación financiera vigente.*

*La pena prevista en el primer párrafo será aumentada en una mitad, cuando la conducta ilícita se cometa por servidores públicos encargados de prevenir, denunciar, investigar o juzgar la comisión de delitos. En este caso, se impondrá a dichos servidores públicos, además, inhabilitación para desempeñar empleo, cargo o comisión públicos hasta por un tiempo igual al de la pena de prisión impuesta.*

*En caso de conductas previstas en este artículo, en las que se utilicen servicios de instituciones que integran el sistema financiero, para proceder penalmente se requerirá la denuncia previa de la Secretaría de Hacienda y Crédito Público. Cuando dicha Secretaría, en ejercicio de sus facultades de fiscalización, encuentre elementos que permitan presumir la comisión de los delitos referidos en el párrafo anterior, deberá ejercer respecto de los mismos las*

marzo de 1997 reformando la Ley del Mercado de Valores, la Ley de Instituciones de Crédito y la Ley General de Organización y Actividades Auxiliares del Crédito, se deben también tomar en cuenta las directivas de la Comisión Nacional Bancaria y de Valores.

Al contrario de lo que se pretende muchas veces, no hay una necesidad de reformar todas las disposiciones penales para añadir la famosa frase “y por medios electrónicos”. A la luz del artículo 400bis CPF por ejemplo, se puede ver que la disposición también se aplica para el lavado de dinero a través del Internet. Si hay problemas, es más el presupuesto territorial de la incriminación. En efecto, en un ambiente cibernético en donde no hay fronteras, ¿cuál es el sentido de una “[.] transferencia dentro del territorio nacional, de éste hacia el extranjero y a la inversa [...]”? Es aquí que se necesitan difíciles reformas, que deberían ser reservadas a los expertos en derecho penal internacional y en derecho internacional público.

Sin embargo, la aplicación represiva no constituye un riesgo para las instituciones financieras, si ellas toman las medidas necesarias para evitar ser cómplice de transacciones ilícitas.

## **Sección II – El marco solucional**

A fin de impedir las operaciones ilícitas, se tiene que establecer filtros a dos niveles. Primero impedir la contratación de clientes sospechosos a través de procesos adecuados de identificación (a), después en la hipótesis que el criminal supo desjugar este filtro, analizar las operaciones para poner fin a las actividades prohibidas (b).

---

*facultades de comprobación que le confieren las leyes y, en su caso, denunciar hechos que probablemente puedan constituir dicho ilícito.*

*Para efectos de este artículo se entiende que son producto de una actividad ilícita, los recursos, derechos o bienes de cualquier naturaleza, cuando existan indicios fundados o certeza de que provienen directa o indirectamente, o representan las ganancias derivadas de la comisión de algún delito y no pueda acreditarse su legítima procedencia. Para los mismos efectos, el sistema financiero se encuentra integrado por las instituciones de crédito, de seguros y de fianzas, almacenes generales de depósito, arrendadoras financieras, sociedades de ahorro y préstamo, sociedades financieras de objeto limitado, uniones de crédito, empresas de factoraje financiero, casas de bolsa y otros intermediarios bursátiles, casas de cambio, administradoras de fondos de retiro y cualquier otro intermediario financiero o cambiario.*

<sup>23</sup> Para los antecedentes legislativos: Zamora, *op.cit.*, 65.

## A – Identificación

En el ámbito del Internet, la identificación se hace a través la certificación (a) que no obstante no puede constituir siempre una identificación sin riesgo. Por eso, una segunda verificación a través varios identificantes se impone (b).

### 1) Certificación

En la certificación el esquema es el siguiente. Una persona se rinde con su pasaporte ante una autoridad de registración (AR) y solicita un certificado electrónico. La AR verifica sus datos y después autoriza a la autoridad de certificación (AC) emitir un certificado retomando en forma digital los datos del pasaporte. La AR puede también añadir otros datos verificables como un título profesional o una razón social. En la mayoría de los casos el papel de la AR se confunde con el de la AC.

Sin embargo, a diferencia del pasaporte, la falla esencial del sistema consista en el nivel de confianza que uno puede tener en la AR. En efecto, el certificado como el pasaporte no tiene ningún valor intrínseco; el valor viene del “root” - de la autoridad que emite el documento. En el caso del Estado, la “seriedad” se presume de manera automática. Pero tal no puede ser el caso cuando la AR es una empresa privada. ¿Quién certifica la seriedad de la empresa? En la práctica la respuesta es muy simple: siendo el root, jella se autocertifica!

Una de las soluciones para luchar contra el lavado “virtual” consiste justamente en una identificación inambiguo. Sin embargo, como lo vimos, con ningún mecanismo estatal de certificación de los roots, la puerta esta abierta a todos los fraudes. Es por eso que el certificado no puede ser por si sólo una respuesta satisfactoria.

### 2) El cross-checking: Los Identificantes

En nuestra opinión, la verificación de los certificados electrónicos tiene que ser completada por un control de otros valores que pueden asegurar de la veracidad de las informaciones contenidas en el certificado. Si tomamos el ejemplo de una empresa que tiene un certificado comprobando su razón social por ejemplo, el

carácter ficticio de la empresa o no puede ser verificado a través la existencia de otros identificantes (ID) como los públicos como el RFC, el número de registro de comercio, etc... o como los privados: *Dun & Bradstreet*<sup>24</sup>, cámaras de comercio, etc...

A fin de facilitar esta investigación, una meta-identificante sería muy útil. Esto sería el punto de partida para encontrar los otros identificantes. Tal papel hubiera podido ser atribuido al *EBIC*<sup>25</sup>, promovido en su tiempo por la hoy difunta EDIRA<sup>26</sup> y emitido por el BSI<sup>27</sup>. Ilustramos nuestras palabras: una empresa quiere abrir una cuenta en línea y presenta un certificado electrónico emitido por una AC en el Caribe que atesta que tiene su domicilio en Zurich, Suiza. El banco, sospechoso del hecho de un certificado emitido en el Caribe para una empresa europea, decide efectuar verificaciones. Si la empresa tiene un EBIC, el banco puede a partir de él verificar en un primer lugar su ID del código postal: primera sorpresa, el código postal corresponde a Basilea y no a Zurich. Aparentemente, la dirección es falsa. Sin embargo, un error material siempre es posible, y el banco continúa con sus verificaciones. A través de su ID de la cámara de comercio, el banco puede *prima facie* constatar que la sociedad esta legalmente constituida y siempre en actividad. Sin embargo, no obstante la declaración de la empresa de ser un *leader* mundial en su sector, ella no tiene ningún ID *Dun & Bradstreet*, tampoco es miembro de ninguna organización representativa del sector y de ninguna organización profesional, etc... Este tipo de verificación cruzada, hecha por identificantes electrónicos en pocos minutos a través del mundo permite en un primer nivel eliminar clientes sospechosos.

Sin embargo, muchas asociaciones criminales están muy bien organizadas y pueden presentar todos los requisitos para ser un cliente “blanco”. Para identificar su carácter ilícito, es entonces necesario analizar sus movimientos financieros.

---

<sup>24</sup> [www.dunandbradstreet.com](http://www.dunandbradstreet.com).

<sup>25</sup> *Electronic Business Identifier Code* (ISO compliant).

<sup>26</sup> [www.edira.org](http://www.edira.org).

<sup>27</sup> *British Standard Institute*.

## B – Análisis

No obstante la virtualización de las transacciones, elementos localizadores pueden continuar jugando un papel importante para determinar el carácter sospechoso de una operación bancaria (a), aunque tal tipo de análisis no resiste a la ingeniosidad de los criminales y consecuentemente otros métodos tienen que completar el dispositivo (b).

### a) Trace y Remailing

Aunque *prima facie* el Internet es por esencia una red de-localizada, es también un hecho que por el momento los servidores, indispensables para el servicio del Web, tienen una localización física. Esto permite por varias técnicas y por el sistema del GPS<sup>28</sup> localizar muchas veces un servidor geográficamente. Por ejemplo, la empresa *Gamez.com* declara al banco que tiene un sitio de casino virtual lícito en Brasil sobre un servidor en el mismo país; la empresa hace varias operaciones por correo electrónico con el banco a partir de su cuenta de correo electrónico <gamez.com>; por medio de programas especiales como el *traceroute*, es posible de trazar el “viaje” del correo electrónico; y se consta que el correo electrónico no paso por ningún servidor en Brasil: se puede concluir que al menos con respecto a la localización del servidor el cliente mintió.

Sin embargo, una técnica como esta tiene sus límites. En efecto, es muy posible cancelar sobre el servidor de origen la función de localización por GPS, impidiendo así cualquiera posibilidad de utilizar el *traceroute*. De la misma manera, el cliente puede utilizar varias técnicas para ocultar el origen de la partida del correo electrónico, ya sea la utilización del *Telnet* sobre el puerto 25, la utilización de anonimadores o técnicas de *mixmaster*. De manera muy esquemática, porque en realidad las cosas son mucho más complicadas, el *Mixmaster*<sup>29</sup> funciona de la manera siguiente. El remitente encripta su correo electrónico con la clave pública del destinatario. Sin embargo, el remitente también encripta este

---

<sup>28</sup> *Global Positioning System.*

<sup>29</sup> Cotrell, *Mixmaster and Remailer Attacks*, [www.jjtc.com/ihws98/jjgmu.html](http://www.jjtc.com/ihws98/jjgmu.html).

mensaje ya encriptado con la clave pública del remitente [ $n^{+1}$ ]. Este último recibe el correo encriptado y lo encripta a su vez con la llave pública del remitente [ $n^{+2}$ ] y lo manda a este último, etc... hasta el remitente [ $n^{x-1}$ ] quien lo manda al destinatario que describiera el correo original. Mixmaster funcionando en red, los remitentes son elegidos de manera aleatoria y en ningún momento uno de los “intermediarios” sabe de donde viene el correo y a donde él va. La técnica combinada con un *spoof* sobre el servidor original rinde una localización totalmente imposible. Es por eso que necesitamos otros métodos de análisis para corroborar actividades de lavado de dinero.

## **b) Scoring systems**

El *scoring system* se basa sobre la técnica del *data mining*: muchos datos separados, con existencias individuales, no tienen ningún valor; pero si se les colecta todos y que hay la posibilidad de construir relaciones entre ellos, el resultado es impagable. Con respecto a las actividades financieras se trata de analizar por diversos métodos de estadísticas datos constantes para descubrir “comportamientos” que permitan conclusiones.

En pocas palabras, se trata de definir parámetros y niveles de alerta. El ejemplo tipo es una línea de crédito de un cliente. Se calcula su promedio de utilización de crédito los últimos doce meses. Este promedio, el parámetro, va a funcionar como nivel de alerta. Todas las operaciones del cliente son monitoreadas y si ocurre que una transacción supera el parámetro, una alerta atrae la atención del gestor de la cuenta, que tiene consecuentemente la oportunidad de investigar mas allá el caso y de poner el cliente sobre una *watch-list*, si tal fuera la necesidad. Es así que muchos parámetros pueden ser definidos e, integrados en un sistema computacional eficaz, el método se revelara muy rápidamente como un instrumento indispensable en el nuevo ámbito en cual las relaciones bancarias han definitivamente cambiado.

Hasta ahora, ellas fueron el ejemplo clásico del contrato *intuitu personae*, en donde la apariencia y la “buena impresión” fueron valores claves para iniciar un negocio. En el mundo virtual, esta forma de empirismo no puede seguir existiendo. El impresionismo cede su lugar al realismo: datos sobre sentimientos – datos y

solamente datos. A través del ejemplo del lavado de dinero, intentamos demostrar que la llave en la lucha contra los delitos financieros en general en el Internet consiste justamente en “jugar” con los datos. En otras palabras, el “maestro” de los datos es el maestro del juego. Dos niveles de control tienen que ser establecidos en el espacio virtual: una identificación electrónica unívoca y un análisis riguroso y en tiempo real de lo que se ocurre de manera desmaterializada para detectar las señales de alerta<sup>30</sup>.

## **Conclusión**

En caso de fracaso, la sanción tiene que intervenir. La primera reforma del derecho penal mexicano no tiene que ser tanto a nivel del derecho substancial, sino con respecto al campo de aplicación *rationae loci*, previendo nuevas reataduras en el derecho penal internacional. Una vez clarificado este punto, la adaptación de las incriminaciones substanciales puede seguir. Sin embargo, el verdadero campo de batalla no es tanto la represión (el derecho) sino la prevención (la criminología). Y solo así, el Schin cabalístico podrá continuar a ser el equilibrio entre el Yin e Yang taoista ...

## **ANEXO**

### **Summary of the fatf mutual evaluation**

*Extract from FATF-XI Annual Report (1999-2000), 22 June 2000, pp. 11-13.*

Mexico has a large population, an extensive financial sector, and due to its geographical position occupies a very important geographical position with respect to drug production, trafficking and consumption. Other criminal activities such as smuggling, financial crime, organised crime and trafficking in firearms and human beings also result in significant amounts of illegal proceeds. A wide variety of money laundering methods and techniques appear to be used, both

---

<sup>30</sup> Ver por ejemplo la lista de las señales de alerta de la Federación Latinoamericana de Bancos: [http://www.felaban.com/lavado/cap5\\_senales.php](http://www.felaban.com/lavado/cap5_senales.php).

within and outside the financial sector. Mexico has had a money laundering offence since 1990. However, in 1997 the Government decided to significantly reinforce its anti-money laundering regime through the adoption of several measures in the financial sector. Since that time Mexico has taken a number of further important steps to improve its anti-money laundering system. Almost all of the basic measures are now in place, and efforts now need to be concentrated on removing remaining loopholes, refining existing requirements, and working to make the system more effective.

The money laundering offence - Article 400 bis, Penal Code – is potentially very broad. It applies to all predicate criminal activity, it covers a wide range of physical acts which could amount to money laundering, and applies to laundering the proceeds of any foreign offence in Mexico. Unusually for a criminal offence, it also contains a provision that gives the court the discretion to reverse the burden of proof regarding the proof of the origin of the property alleged to have been laundered, once the prosecution provides sufficient evidence that the property has an illegal source. Few convictions have been obtained for the offence, and there are many cases before the courts and under investigation. Some of the difficulties, as in many other countries, include the need to prove: (a) that the property was proceeds of crime, (b) that the laundering took place for a specific purpose, or (c) that the defendant knew it was illegal proceeds. Another difficulty is associated with the use of the reverse onus provision. Some of these problems are likely to be overcome through further cases, combined with legal training. However consideration could be given to the introduction of a lesser offence based on negligence, with lesser penalties, and the need to prove that the defendant committed the money laundering for the specific purpose of concealing or disguising the ownership of the assets should be removed.

Basic provisions exist in the Penal and Penal Procedure Codes dealing with confiscation, and the powers to take provisional measures, including action against third parties that hold illicit property, are quite significant. More recently, Article 29 of the Organised Crime law extended these powers by allowing the onus of proof to be reversed in certain circumstances. However, there is no power to make an order for an equivalent value to the proceeds if

they have been dissipated and this situation should be reviewed. Consideration should also be given to creating specialised law enforcement and prosecutorial units dedicated exclusively to investigating proceeds of crime cases.

Mexico has signed and ratified the Vienna Convention, and has entered into a wide range of international agreements, which provide the legislative basis for it to provide assistance. It can provide assistance without a treaty on the basis of reciprocity, and does not require dual criminality for requests made pursuant to treaties. The DGAIO has also entered into several financial information exchange agreements with other FIU and can exchange STR information with them, though these possibilities need to be broadened.

The key operational bodies in the Mexican anti-money laundering system are the Attached General Directorate for Transaction Investigations (DGAIO) of the Secretariat of Finance and Public Credit and the anti-money laundering unit of the General Attorney's Office (PGR). They are well resourced units, with a strong commitment to integrity. They have been very active in introducing and promoting the anti-money laundering laws and regulations, and occupy a central co-ordination and co-operation function. The DGAIO, in its role as the Mexican financial intelligence unit, receives all the different types of reports, including STR, and has access to a wide range of intelligence and commercial data, though this role could be made more efficient if it had on-line access to some of these databases. The system could also be made more efficient by creating a gateway through the bank secrecy laws so as to allow the STR to be sent directly to the DGAIO, and for criminal investigation requests to be sent directly to the financial institutions, rather than routing these through the Commissions which supervise the financial sectors. The fight against money laundering could be enhanced by a creation of a more co-ordinated strategic plan or strategy with objectives, combined with consideration as to how policy level co-operation and co-ordination can be further developed, both across government and with the financial sector.

The preventive measures in the financial sector are generally sound and comprehensive, covering most of the requirements in the FATF Recommendations, and the financial regulatory Commissions

and the banking sector have actively implemented the laws and regulations. In certain respects, such as the introduction of "Know your customer" principles, Mexico has gone well beyond the minimum requirements. However, the scope of the anti-money laundering measures in the financial sector need to be extended to cover money remittance businesses and action needs to be taken in relation to the more than 5,000 unregulated money exchange establishments. The laws or regulations also need to be amended to require all financial institutions to identify beneficial owners of accounts.

Mexico has introduced a comprehensive system of reporting, with obligations to report suspicious and unusual transactions, large value and cross-border transactions. The results from the STR system, which commenced in 1997, started at a very low level, and have substantially increased each year, though the number of reports from the NBFIs sector is still low. Although the mechanics of the reporting systems are working reasonably well, it takes too much time for an STR to reach the DGAIO from the time that they are initially found to be suspicious. This time period could be reduced by eliminating some of the intermediary steps, and requiring reports to be passed on more quickly. Increased specific and general feedback needs to be provided to assist reporting institutions in identifying transactions that are truly suspicious. Mexico receives a large number of cross-border reports for amounts greater than US\$ 20,000 each year, and this number has steadily increased over the last few years. These reports can be a source of valuable information, and consideration could be given to reducing the reporting limit for imported currency to US\$ 10,000, which will be the same as in a number of other FATF members, and in line with the proposed reporting obligation for currency exiting Mexico.

The financial regulatory Commissions and the DGAIO has been very active in preparing the regulations and the handbooks that are the basis for the internal controls and guidelines for financial institutions. A comprehensive programme of training has also been put in place by the Mexican Bankers Association, and the DGAIO has also participated actively. Similarly, the National Banking and Securities Commission (*CNBV – Comisión Nacional Bancaria y de Valores*) has created examiners manuals which extend to cover

money laundering, and its on-site supervision, which occurs at least once a year, is already checking the anti-money laundering controls and policies that institutions have put in place. Measures are generally solid, though some additional refinements could be made.

Mexico fully meets FATF Recommendation 4, since it has a money laundering offence that extends to all predicate crimes. As regards Recommendations 10, 11 and 15, it is almost fully compliant with these Recommendations, since the obligations to identify customers and report suspicious transactions do not extend to money remittance businesses or to the unregulated money exchange establishments. Accordingly, the FATF recognises Mexico as a full member.