

**Fredrick Vega**  
Decano de la Facultad de Derecho  
de la Universidad Interamericana de  
Puerto Rico, docente de la cátedra de  
Derecho Cibernético.

**Sasha M. García, Johel Ocasio,  
Michelle Matos, Irelis Rodríguez.**  
Estudiantes de la Facultad de Derecho  
de la Universidad de Puerto Rico.

## **Derecho cibernético**

# **El uso de sistemas cibernéticos de pago en el lavado de dinero**

### **Palabras clave:**

Derecho Cibernético,  
Cibercriminalidad, Internet.

### **Keywords:**

Cybernetic law, Cybercrime,  
the Internet.

### **Resumen**

Este artículo es el resultado de las revisiones de investigaciones realizadas durante la etapa de conformación y preparación del programa académico del “Derecho Cibernético”; durante el estudio del tema de la cibercriminalidad como delito se plasma la importancia de crear un marco legal en los países industrializados, que regule el control del manejo de los dineros a través del Internet.

Este análisis compila algunos casos presentados o sucedidos en países como Puerto Rico, Estados Unidos, Argentina, Brasil, entre otros.

### **Abstract**

This article is the result of a research checking work. That research took place during the conformation and preparation of the “Cybernetic Law” academic program. During the studying process of the cybercrime as an offense, it embodies the importance of creating a legal framework in the industrialized countries to regulate the control of money management through the Internet.

This analysis compiles some cases that took place in countries like Puerto Rico, United States, Argentina, Brazil, among other.

Recibido: Marzo 10 de 2009 / Aceptado: Mayo 8 de 2009

Artículo de Revisión/Review Article

Revisión del Derecho Cibernético

### **Lavado de dinero - en general**

El crecimiento y desarrollo de los mercados financieros globales hacen más fácil la comunicación y el comercio entre países, que hace 80 años atrás, no se imaginaban que pudieran estar llevando a cabo transacciones monetarias tan fácil como oprimir un botón en una computadora. Esto ha ayudado a mejorar la relación y el mercado entre diferentes naciones. Pero así como se ha logrado con la tecnología mejorar actividades tan legítimas como el comercio, también han facilitado lo que se conoce como lavado de dinero. Países con leyes que protegen la privacidad bancaria están directamente conectados a países con leyes para reportar las transacciones bancarias. Estos dos intereses económicos, el de proteger la privacidad de una persona *vis a vis* el reportar a las agencias gubernamentales las transacciones sospechosas, hacen posible el depósito de dinero sucio en un país poco reglamentado y la transferencia del mismo a cualquier otro con mayores restricciones. Se crea una red económica subterránea, la cual sustenta y alimenta tanto las actividades delictivas como los actos terroristas.

El lavado de dinero ocurre en casi todos los países del mundo. Un solo esquema de lavado de dinero puede envolver la transferencia a través de varios países para obscurecer sus orígenes. Mientras más difícil es rastrear en dónde surge la raíz de una transacción, más difícil es poder obtener la convicción de una empresa criminal organizada.

La Organización de las Naciones Unidas (ONU), en una sesión especial del 10 de junio

de 1998 estudió el problema y determinó cómo afecta mundialmente esta actividad. Nos dicen que: “The infiltration and sometimes saturation of dirty money into legitimate financial sectors and national accounts can threaten economic and political stability... money laundering impacts financial behavior and macroeconomic performance in a variety of ways including policy mistakes due to measurement errors in national account statistics; volatility in exchange and interest rates due to unanticipated cross border transfers of funds; the threat of monetary instability due to unsound asset structures; effects on tax collection and public expenditure allocation due to misreporting of income; misallocation of resources due to distortions in asset and commodity prices; and contamination effects on legal transactions due to the perceived possibility of being associated with crime”.

Son empresas subterráneas las cuales trabajan con cantidades de dinero, a veces inimaginables. “Depending on which international agency you ask, criminals launder (UN General Assembly Special Session on the World Drug Problem (8-10 June 1998). Descargado el 26 de abril de 2009 de la página web de las Naciones Unidas: <http://www.un.org/ga/20special/featur/laundry.htm>) anywhere between \$500 billion and \$1 trillion worldwide every year. The global effect is staggering in social, economic and security terms”.

Entonces, al día de hoy, el lavado de dinero es cómplice y participe directo del problema número uno el cual sufre el mundo entero, el económico. Entre otras cosas, afecta los recaudos

de impuestos de los gobiernos, pues al existir ingresos los cuales se utilizan para hacer riquezas, pero no se reflejan para aportar económicamente al funcionamiento de los estados, merman los recaudos fiscales. Por lo que el Estado se ve obligado a recortar gastos, los empleados se ven afectados al perder empleos y los comercios decaen por el pobre consumo de las personas.

Pero, ¿qué es el lavado de dinero? ¿cómo funciona esta actividad? ¿quiénes la llevan a cabo? Al día de hoy, ¿está la tecnología aportando a estas actividades ilegales? ¿cuán cerca estamos nosotros de sistemas que ayuden a llevar a cabo estos delitos? ¿cuán activa está la comunidad global para trabajar con este problema? ¿qué es el lavado de dinero? “Money laundering, at its simplest, is the act of making money that comes from Source A look like it comes from Source B. In practice, criminals are trying to disguise the origins of money obtained through illegal activities so it looks like it was obtained from legal sources.” Es el acto de disfrazar, o hacer parecer que dinero que viene de una fuente (ilegal) en realidad proviene de otra (legal). El fin de hacer esto es poder utilizar el dinero, ya que utilizándolo sin llevar a cabo esta operación lo vincularían directamente a actos delictivos, promoviendo la investigación de las autoridades.

Quiénes son los que llevan a cabo estas operaciones. El tipo de criminal que lleva a cabo por lo general estas transacciones son los traficantes de drogas, políticos corruptos, mafiosos y terroristas. Los traficantes de drogas son los que más necesitan llevar a cabo estas operaciones de lavado de dinero, ya que casi en su totali-

dad, las transacciones que estos efectúan son en dinero en efectivo. El movimiento de dinero en efectivo es el que llama la atención a las autoridades. Nos dice el Departamento de Justicia de los Estados Unidos, que los traficantes de drogas continuarán utilizando estos métodos de pagos electrónicos porque “it enables standardized international financial transactions and operates largely outside the regulatory requirements of the traditional banking system. The ability of individuals and businesses to conduct complex, immediate, and irreversible (Layton, J. *How Money Laundering Works*. Descargado el 25 de abril de 2009 de How Stuff Works:<http://money.howstuffworks.com/money-laundering3.htm>) international transactions with very little financial transparency greatly benefits drug traffickers and other criminals.” Procedimiento del lavado de dinero. En la percepción más básica de estas operaciones, hay tres etapas necesarias para poder llevar a cabo la operación de lavado de dinero. Estas son llamadas colocación, “Layering” e integración.

En la etapa llamada colocación, se deposita o “coloca” el dinero sucio en una institución financiera legítima. Mayormente se hace en depósitos bancarios. Es la etapa más riesgosa porque los depósitos de grandes cantidades de dinero son sospechosos y los bancos están obligados a reportar transacciones grandes o de mucho dinero.

La etapa de “Layering” (encubrimiento, estructuración de transacciones) es el envío del dinero a través de varias transacciones financieras para cambiar su apariencia y hacer más difícil su rastreo. Puede consistir en transferencias de

banco a banco, transferencias electrónicas entre cuentas diferentes con diferentes nombres o a diferentes países, cambiar la moneda, compra de artículos de mucho valor (yates, casas, autos, diamantes) para cambiar la forma del dinero. Esta es la etapa más compleja. Todo es para hacer más difícil seguir el dinero sucio original.

Por último, la integración, que es cuando el dinero entra nuevamente al flujo económico de manera aparentemente legítima. Puede involucrar una transacción bancaria final en la cuenta de un negocio local en el cual se “invierte” en intercambio mediando un corte de las ganancias. (Ejemplo, vendiendo el yate comprado en la etapa de “Layering”). En este punto, el criminal puede utilizar el dinero sin ser atrapado. Es muy difícil atrapar a un criminal en esta etapa si no hay documentación en las etapas anteriores. Es el lavado de dinero a través del ciberespacio.

El Internet ha crecido grandemente en los últimos años, y con esto, el comercio a través del ciberespacio. El desarrollo de nuevas prácticas comerciales ha dado paso a la evolución de delitos existentes como el lavado de dinero. Aunque en esencia el lavado de dinero a través del Internet mantiene la misma técnica, los métodos de distribución han sido alterados de modo que estos se utilizan para reintegrar al comercio legal o “limpiar” el dinero obtenido ilegalmente. (Money Laundering in Digital Currencies (2008). Descargado el 25 de abril de 2009 de National Drug Intelligence Center Website: <http://www.usdoj.gov/ndic/pubs28/28675/intro.htm> 5 Layton, J. *How Money Laundering Works*. Descargado el 25 de abril de 2009 de How

Stuff Works: <http://money.howstuffworks.com/money-laundering3.htm>).

El Internet goza de varias características que facilitan las transacciones de dinero ilegal. Algunas de estas son:

- **Anonimato**

Gracias a los millones de usuarios que tiene el Internet, resulta muy atractivo el poder “escondese” dentro de una gran multitud a la hora de cometer un delito. Aunque se han desarrollado distintos métodos para lograr seguir a las personas a través del Internet y así prevenir el uso ilegal de los servicios, existen tecnologías como la codificación o “encryption” que proveen el anonimato necesario para continuar con la actividad ilegal.

- **No hay contacto cara a cara**

Las operaciones comerciales realizadas por Internet son hechas por una persona frente a una computadora, evitando que como parte del proceso se requiera ver a la persona físicamente para efectuar una transacción. Al eliminar el contacto humano como intermediario, se elimina también el riesgo de que el acceso a alguna cuenta o alguna transacción le resulte sospechosa a algún empleado de la institución bancaria. Gracias a esta falta de contacto cara a cara, es posible que se pretenda ser una persona diferente cada vez que se entra a una cuenta bancaria a través del ciberespacio, es tan simple como tener el nombre de usuario y la contraseña para poder acceder.

- **Rapidez de las transacciones**

El uso de las transacciones por Internet abarata los costos que conllevan los métodos tradicionales del lavado de dinero y permite el movimiento rápido del dinero ilegal. Este aspecto le deja a los delincuentes transferir fondos de forma rápida entre varias localizaciones, ya sea dentro del mismo país o entre distintos países, lo que dificulta a las autoridades el poder seguir la cadena de transacciones del dinero ilegal.

- **Globalización**

La globalización de la economía ha motivado a personas (comerciantes y consumidores) a invertir y gastar dinero donde quieran. Para poder facilitar dichas transacciones, la tecnología ha desarrollado nuevas técnicas de pago que permiten hacer negocios a larga distancia, sin la preocupación de tener que viajar con grandes cantidades de dinero. Esto ha recibido el término de “movilidad de la inversión”. Dado que el acceso a estos servicios cibernéticos es fácil y común, este canal de distribución se ha convertido en uno sumamente importante para productos financieros. Actualmente, existe una tendencia para reducir los obstáculos legales entre países o buscar nuevas formas eficientes de invertir, y así maximizar las ventajas que los sistemas cibernéticos de pago ofrecen.

- **Actividad internacional**

Usualmente, el domicilio del proveedor de servicio en-línea difiere del lugar donde los servidores están verdaderamente localizados, del lugar de donde estos están administrados o de

donde el cliente tiene acceso al Internet (“Cyber Laundering”, 2002).

Estas nuevas tecnologías de pago permiten llevar a cabo transacciones de negocios entre distintos países y sistemas legales (Chepesiuk, 2000). Sin embargo, esto significa que son varias las jurisdicciones que pueden estar envueltas en el caso de alguna ofensa o infracción aún cuando hay un sinnúmero de tratados legales y acuerdos entre naciones, la coordinación conjunta de agencias policíacas, de rentas internas y de justicia suele ser una tarea difícil a la hora de tratar crímenes internacionales. Por estos obstáculos, resulta relativamente fácil salirse con la suya en este tipo de actividad ilícita. Foros del Lavado de dinero por Internet.

- **Subastas En-Línea**

Otro modelo de negocios muy utilizado por los blanqueadores de dinero es la subasta en-línea. Actualmente, este goza de un auge en la industria del Internet pues le permite a un usuario registrado vender o comprar una inmensa gama de productos. Muchas de estas páginas de subasta ofrecen servicios financieros básicos para ofrecer seguridad a las personas que están adquiriendo o vendiendo productos. El comprador envía dinero a la cuenta bancaria de la compañía y el vendedor entonces vende el artículo al comprador. Si todo marcha bien, y el artículo cumple con las especificaciones anunciadas, la compañía le envía el dinero al vendedor. Esto da una apariencia de legalidad a la transacción de negocio pues envuelve la cuenta bancaria de una compañía reconocida. Dado a que el precio

de apuesta no tiene límite, cualquiera puede continuar apostando más y más hasta que el precio llega a ser extraordinariamente alto, y mientras más alto el precio, más dinero el blanqueador puede dar la apariencia de legalidad.

#### • **Foros de juegos y apuestas por Internet**

Los foros cibernéticos de juegos y apuestas han sido identificados como el servicio en-línea ideal para lavar dinero. Esto no debe ser un concepto difícil de aplicar, si consideramos que actualmente los casinos son utilizados para manejar y distribuir dinero lavado. El blanqueador o “launderer” utiliza el dinero para comprar fichas de apuestas, y aún cuando pierde un porcentaje de los fondos, es el precio que paga para poder “limpiar” el dinero. Al final del día, el blanqueador cobra las fichas restantes y pide que se le pague en un cheque a ser depositado a su cuenta. El pago se reflejará proveniente de una fuente de ingresos legítima: el casino.

Mientras que los casinos están altamente regulados, requiriendo una identificación válida para poder hacer transacciones como la anteriormente mencionada, los foros cibernéticos de juegos y apuestas no, permitiendo así que los blanqueadores puedan mover dinero de una cuenta de tarjeta de crédito a una cuenta bancaria a través del foro.

#### • **Servicios Bancarios En-Línea**

Los Servicios Bancarios En-Línea son el blanco principal de los blanqueadores de dinero debido a la variedad de servicios financieros que proveen. Dado que las leyes y regulaciones

varían de jurisdicción en jurisdicción, aquellas que son más laxas son las más utilizadas por los blanqueadores porque no otorgan información personal a las agencias policíacas.

El servicio en línea puede ser falso, es decir, que en realidad no se ofrece ningún servicio, pero el ofrecerlo provee la oportunidad de mezclar consumidores legítimos (mezclar tanto la actividad lícita e ilícita) para que sea más difícil a las agencias gubernamentales reconocer las transacciones como sospechosas.

#### • **Sistemas intermediarios de pago**

Son sistemas que proveen el servicio de pagos y transferencias de dinero a través del Internet que se utilizan como una alternativa de procesamiento de pago para vendedores, subastas y servicios ofrecidos en-línea. Los sistemas de pago pueden utilizar fondos de cuentas de banco o tarjetas de crédito. La persona que reciba un pago a través de estos sistemas puede solicitar un cheque emitido por uno de estos servicios o en su alternativa puede exigir que el dinero sea transferido a su cuenta bancaria.

Lavado de dinero a través de los sistemas intermediarios de pago para motivos del trabajo investigativo, nos concentraremos en el sistema intermediario de pago antes mencionado, puesto que sirve como un buen punto de partida para la entera comprensión del lavado de dinero a través del Internet. Estos sistemas de pago, al igual que otros métodos del lavado de dinero por Internet, comparten las características de la rapidez y la falta de contacto cara a cara que le hacen atractivos para transacciones ilícitas. La internaciona-



lidad de estos sistemas de pago son también un agravante a la dificultad de prevención de este tipo de lavado de dinero.

Debido a que estos intermediarios de pago son utilizados para una variedad de servicios, se presta para diferentes tipos de procesos de lavado de dinero como lo son:

- **Venta de artículos o servicios inexistentes**

Mediante este método, una persona ofrece en venta algún artículo o servicio inexistente a través de una página cibernética de ventas y subastas. Este artículo o servicio es comprado por el mismo vendedor o una persona confabulada con este, con una cuenta bancaria que contiene el dinero ilegal. El dinero ilegal de la cuenta bancaria es entonces transferido a través del sistema intermediario de pago, a la cuenta bancaria del supuesto vendedor. Este mismo método se repite una y otra vez en varias transacciones con diferentes cuentas bancarias hasta que el dinero ilegal se re-integra a la economía, dando la apariencia de ser transacciones legales.

- **Disolución de cuenta a cuenta**

La rapidez de la transmisión de dinero a través de los sistemas intermediarios de pago toma un papel importante en la transferencia de dinero ilegal a varias cuentas. En este método, el dinero ilegal se deposita en cuentas bancarias y se transfieren fracciones de los fondos a otras cuentas hasta que queda disuelta en pequeñas cantidades que pasan por desapercibidas. La característica de la internacionalidad de los servicios

intermediarios de pago es también importante en este método de lavado de dinero, puesto que el dinero puede ser transferido a varias cuentas bancarias a través del mundo.

Este sistema se ha vuelto tan elaborado que en el pasado se han creado programaciones de computadoras con el propósito de abrir cientos de cuentas fraudulentas a la vez. Compañías como PayPal han creado sistemas para distinguir entre cuentas creadas por personas y cuentas creadas por computadoras, para así entonces poder reducir el número de cuentas fraudulentas a las cuales se pueda transferir dinero utilizando sus servicios.

Políticas de las compañías que ofrecen Sistemas Intermediarios de Pago las compañías de métodos de pagos electrónicos han implementado una serie de políticas en sus reglamentos para poder manejar, evitar y detectar posibles actos ilícitos en la utilización de sus recursos. En el caso de la empresa PayPal, Inc., han establecido una política de recolección de información específica para identificar debidamente a los usuarios del sistema. Entre otras cosas, su política indica:

“How we collect information about you  
When you visit the PayPal website, we collect your IP address and standard web log information, such as your browser type and the pages you accessed on our website.

If you open an account, we collect the following types of information from you:

- Contact information - your name, address, phone, email, Skype ID and other similar information.

- Financial information - the bank account numbers and credit card numbers that you link to your PayPal account. Before permitting you to use our Service, we may require you to provide additional information we can use to verify your identity or address or manage risk, such as your date of birth, social security number or other information. We may also obtain information about you from third parties such as credit bureaus and identity verification services.

When you are using our Service, we collect information about your account transactions and we may collect information about your computer or other access device for fraud prevention purposes. “También establece cómo va a utilizar la información y con quién la va a compartir. Dicen que compartirán la información tanto entre sus empresas conglomeradas, como con las agencias gubernamentales cuando les sea solicitado. Como verán, su propósito es, además de proveer servicios integrados y de calidad, detectar violaciones a sus políticas de la compañía y a las leyes financieras y cualesquiera otras. “How we share personal information with other parties We may share your personal information with:

- Members of the eBay Inc. corporate family - like eBay, Shopping.com or Skype - to provide joint content and services (like registration, transactions and customer support), to help detect and prevent potentially illegal acts and violations of our policies, and to guide decisions about their products, services and communications. Members of our corporate family will use this information to send you

marketing communications only if you have requested their services.

- Service providers under contract who help with parts of our business operations; (fraud prevention, bill collection, marketing, technology services). Our contracts dictate that these service providers only use your information in connection with the services they perform for us and not for their own benefit.
- Law enforcement, government officials, or other third parties when o we are compelled to do so by a subpoena, court order or similar legal procedure o we need to do so to comply with law o we believe in good faith that the disclosure of personal information is necessary to prevent physical harm or financial loss, to report suspected illegal activity, or to investigate violations of our User Agreement.
- Other third parties with your consent or direction to do so.”

Otra de las empresas utilizadas como métodos electrónicos de pago es la de la empresa Google, Inc., y su herramienta se llama Google Checkout©. Como práctica. (Privacy Policies for Paypal Services. Descargado el 29 de abril de 2009 de PayPal: [https://www.paypal.com/us/cgi-bin/webscr?cmd=p/gen/ua/policy\\_privacy-outside](https://www.paypal.com/us/cgi-bin/webscr?cmd=p/gen/ua/policy_privacy-outside) imilar a Paypal, Inc.), esta herramienta guarda información sobre quienes utilizan el sistema. Cualquier información o actividad que encuentren sospechosa de ser ilegal, ellos establecen en su política que será verificada.

“Payment Transaction Processing the Service facilitates the processing of Payment Tran-



sactions to complete a payment for a purchase between a Buyer and a Seller. The Service will store information from Buyers, such as their Payment Instruments and shipping information, and will process Payment Transactions on behalf of Sellers through the appropriate credit card or debit card network. GPC may delay payment processing of suspicious transactions or transactions which may involve fraud, misconduct, or violate applicable law, this Terms of Service for Buyers, or other applicable GPC or Service policies, as determined in GPC's sole and absolute discretion. Buyer authorizes the charge or debit to Buyer's Payment Instrument as necessary to complete processing of a Payment Transaction. Buyer also authorizes the crediting to Buyer's Payment Instrument in connection with reversals, refunds, or adjustments through the Service..."

Además, recopilan información sobre las transacciones hechas mediante el sistema. Esto para detectar posibles fraudes o usos ilegítimos del sistema. Así tienen información suficiente la cual pueden utilizar en caso de detectar algún uso ilegal de su sistema de pago. "...Información sobre las transacciones - Google recopila información sobre todas las transacciones realizadas mediante Google Checkout, incluido el importe, la descripción del vendedor de los bienes o servicios adquiridos, los nombres del vendedor y del comprador, y el tipo de pago utilizado.

Información sobre el uso del servicio con el fin de evitar fraudes, suplantaciones de identidad y otras acciones malintencionadas, Google puede recopilar información sobre su interac-

ción con el servicio para ayudarle a validar su identidad o a detectar alguna conducta potencialmente fraudulenta..." También definen para qué se utilizará la información recopilada en el caso que tenga que ser compartida con otras empresas o agencias. En este caso, podemos ver ocho Condiciones del Servicio de Google Checkout. (Descargado: 29 de abril de 2009 de Google Checkout: <https://checkout.google.com/termsOfService?type=Buyer> 9 Política de privacidad de Google Checkout. Descargado el 29 de abril de 2009 de Google Checkout: <https://checkout.google.com/files/privacy.html>) que cualquiera que utilice el sistema de Google, está consintiendo a la utilización de la información de la manera descrita. Por lo que si se llevan a cabo actividades ilegales, los usuarios están conscientes que de ser detectados, sus transacciones no quedarán en el anonimato:

"Uso compartido de la información Google no venderá ni alquilará los datos personales de los usuarios a empresas o individuos externos. [...] Además, solo se compartirán estos datos con otras empresas o individuos externos a Google en los siguientes casos:

- Para detectar, evitar o abordar casos de fraude, problemas técnicos o seguridad.
- Google tiene su consentimiento. Su consentimiento resulta necesario para compartir cualquier dato confidencial.
- Google considera de buena fe que el acceso, el uso, la preservación o la divulgación de esta información son razonablemente necesarios para (a) cumplir con las leyes correspondientes, las regulaciones, los procesos le-

gales o las solicitudes gubernamentales, (b) aplicar estas condiciones del servicio, incluida la investigación de posibles infracciones, (c) detectar, impedir o, de cualquier modo, abordar casos o problemas de fraude, seguridad o asuntos técnicos o (d) proteger contra daños inminentes los derechos, la propiedad o la seguridad de Google, sus usuarios o el público en la forma exigida o permitida por la ley”.

Aún cuando estas políticas estén siendo implementadas día a día, sigue siendo muy complicado para estas compañías mantener una investigación frecuente de todos sus usuarios y así evitar completamente el uso de sus servicios para fines ilícitos. Es peor aun la situación cuando el dinero ilícito a ser transferido se divide en sumas pequeñas que pasan desapercibidas a través de múltiples cuentas. En fin, aun cuando existen políticas para aminorar el impacto del uso de medios cibernéticos para fines ilícitos sigue siendo imposible una supervisión y cuestionamiento de cada transacción ya sea por parte de la compañía que ofrece el servicio o por alguna entidad gubernamental. (Política de privacidad de Google Checkout. Descargado el 29 de abril de 2009 de Google Checkout: <https://checkout.google.com/files/privacy.html>).

Legislación y jurisprudencia relacionada al lavado de dinero a través del Internet. El Congreso de los Estados Unidos de América ha legislado para controlar e identificar el lavado de dinero con tres actas principales; Bank Secrecy Act de 1970, Money Laundering Act de 1986 y el controversial US Patriot Act.

El Bank Secrecy Act de 1970, mejor conocida como *Currency and Foreign Transactions Reporting Act* le requiere a las instituciones bancarias de Estados Unidos que ayuden al gobierno para detectar y prevenir el lavado de dinero. Se enfocan específicamente en guardar expedientes de las compras de instrumentos negociables (mayores de \$3,000.00) para poder detectar actividades ilegales. Luego de la creación de estas regulaciones muchos bancos implementaron como política institucional no vender instrumentos negociables cuando se paga con dinero en efectivo. Se requiere la transferencia de los fondos de alguna institución en Estados Unidos. El acta se firmó en 1970 y se le llama comúnmente la ley “Anti-Money Laundering” law (AML). La realidad es que esta acta no tuvo ningún efecto significativo hasta que el “US Treasure” no la implementó. *Cal. Bankers Ass’n v. Shultz*, 416 U.S. 21, 26, 94 S.Ct. 1494, 39 L.Ed.2d 812 (1974).

El Money Laundering Control Act de 1986 es el acta donde el Congreso de los Estados Unidos hizo del lavado de dinero un crimen federal. Fortaleció el Bank Secrecy Act porque codificó como un crimen el estructurar maneras alternas de transacciones de dinero para evitar seguir los procedimientos estructurados que requiere el acta. El US Patriot Act es un estatuto que el gobierno de los Estados Unidos de América creó luego de los ataques terroristas del 11 de septiembre de 2001. Las siglas corresponden a “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept

and Obstruct Terrorism Act of 2001” (Public Law Pub. L. 107-56).

En su artículo III el US Patriot Act indica las regulaciones para combatir el lavado de dinero en aras de acabar el terrorismo y se le conoce como International Money Laundering Abatement and Financial Anti-Terrorism Act de 2001. Se creó para facilitar, prevenir, detectar y castigar el lavado de dinero internacional y el financiamiento del terrorismo. Básicamente enmienda porciones de Money Laundering Control Act of 1986 (MLCA) y Bank Secrecy Act of 1970 (BSA). Se divide en tres subtítulos; regulaciones bancarias; comunicación efectiva entre las instituciones financieras y las agencias investigadoras; y por último cubre la falsificación de dinero.

Se mantienen expedientes para identificar posibles cuentas fraudulentas, se utilizan programas para detectar estas transacciones y se tienen bases de datos compartidas en la industria para atacar el problema agresivamente. Se le delegó al Departamento (Bank Secrecy Act 31 U.S.C. §§ 5311-5330 and 12 U.S.C. §§ 1818(s), 1829(b) and 1951-1959 (1970), 12 Money Laundering Act, 18 U.S.C. §1956(f) and 1957(d) (1986)). USA PATRIOT Act 26 de octubre de 2001, 115 Stat. 272, Title III, Subtitle A, Sec. 312, 313, 319 & 325). USA PATRIOT Act, 26 de octubre de 2001, 115 Stat. 272 Title III, Subtitle A, Sec. 314.) de Tesorería de los Estados Unidos formular nuevas regulaciones y requerir mayor monitoreo de las transacciones monetarias para controlar el problema de lavado de dinero. Además el Acta creó delitos y multas

para los que no cooperen con las autoridades correspondientes.

La definición de lavado de dinero se expandió con el “US Patriot Act”. Las regulaciones concernientes al lavado de dinero, anteriores al controvertible acta, no se implementaban eficazmente. El atentado terrorista del 11 de septiembre de 2001, en contra de las Torres Gemelas de Nueva York, provocó que el gobierno norteamericano incursionara en medidas radicales para combatir el terrorismo. La controversial acta enmendó las leyes existentes haciéndolas menos restrictivas para encausar criminalmente a las personas naturales o jurídicas que realizan transacciones de dinero sin seguir las regulaciones requeridas. U.S. vs E-Gold, 8 de mayo de 2008 550 F.Supp.2d 82.

En US vs. E-Gold se le formularon cargos federales por conspirar y operar un negocio de transferencia de dinero sin la licencia requerida. La empresa se defendió argumentando que no utilizaban dinero en efectivo sino que era virtual por lo que no tenían que licenciarse o seguir las regulaciones porque no les aplicaban. El Tribunal ha entendido que las regulaciones en estas áreas desconocidas no pueden ser restrictivas y sí liberales para poder defender los intereses de la seguridad nacional de los Estados Unidos. Las personas naturales o jurídicas que se dediquen a hacer transacciones de dinero, sea el dinero que sea, tienen que ser registradas, obtener una licencia, hacer reportes de movimientos de dinero mayores de 10 mil dólares y otros requerimientos para que se pueda combatir eficazmente el lavado de dinero.

Lavado de dinero a través del Internet en el contexto internacional. Por años los países han tratado de implementar legislación para minimizar la incidencia de lavado de dinero en sus territorios. Lo realmente preocupante de todo esto es que esta práctica sobrepasa las fronteras poniendo retos a los países, creando conflictos jurisdiccionales y convirtiéndose en una problemática de índole global.

Resulta difícil determinar cuánto ha lacerado esta práctica las economías en los distintos países, a sus instituciones económicas y a sus gobiernos. Lo cierto es que por más esfuerzos que realicen los países y la comunidad internacional esto solo ayudará a mitigar el daño. Lamentablemente, los adelantos tecnológicos de esta nueva generación y la globalización, entre otros factores harán cada vez más ardua la tarea de eliminar totalmente este esquema. (USA PATRIOT Act 26 de octubre de 2001, 115 Stat. 272, Title III, Subtitle A, Sec. 312, 313, 319 & 325. 16 U.S. v. E-Gold, 550 F.Supp.2d 82, D.D.C., May 08, 2008).

### **Problemática internacional**

El Salvador

- Hace menos de un año se publicó en un periódico de ese país un reportaje sobre el crecimiento del lavado de dinero por Internet, utilizando “mulas cibernéticas” para realizar las transacciones. Veamos en qué consiste el esquema: Una persona recibe un correo electrónico para ofrecerle empleo desde su casa. El trabajo consiste en ayudar a empresas a pagar a clientes en terceros países. Esta per-

sona deberá abrir una cuenta de banco a su nombre y aceptar depósitos anónimos. Luego que recibe el dinero, deberá transferirlo electrónicamente a otro país que normalmente es en Europa. A la “mula” se le paga una parte del dinero enviado.

- Según el reportaje los expertos en seguridad de la red aseguran que a medida que crece el desempleo en el país, más gente está dispuesta a asumir el riesgo y participar de este tipo de fraudes.
- Se han detectado 873 portales de Internet para contactar mulas en Gran Bretaña en la primera mitad de 2008, un 33% más que en el 2007.

Argentina

- El 26 de noviembre de 2007 muchos ciudadanos argentinos quedaron atónitos ante la noticia de que el Banco Central de la República Argentina (BCRA) indicó que los usuarios de las tarjetas de crédito Visa, Master Card y American Express no podrían emitir pagos mediante PayPal, Moneybookers y otros. Según la noticia publicada el BCRA ha tomado estas medidas para evitar la fuga de capital. El descontento de la gente se hizo sentir de inmediato manifestando los daños que esta acción causaba a las personas que con más frecuencia realizan sus compras a través de estos sistemas. Afortunadamente el problema fue solucionado posteriormente.

Estos son solo ejemplos de la infinidad de incidentes de lavado de dinero que ocurren en el mundo diariamente. El blanqueo de dinero

como se le conoce en América Latina y Europa a este fenómeno ya no se da solo por depósitos misteriosos a los bancos, está en la red, haciendo más fácil su proliferación y más difícil identificar a las personas que están detrás de todo el esquema. No son solo las mulas, ahora puedes lavar dinero por medio de los chats y los casinos virtuales, entre muchos otros sitios de Internet. Precisamente las Naciones Unidas realizan actualmente investigaciones sobre estos asuntos y cada vez más países están creando legislación para mitigar el daño económico y político que esta conducta pueda causar. (El Salvador (14 de diciembre de 2008). Descargado el 2 de mayo de 2009 del periódico *El diario de hoy*, www.elsalvador.com).

(El Banco Central vs. PayPal Money Brokers (26 de noviembre de 2006). Descargado 2 de mayo de 2009 de Invisionarg: <http://php.invisionarg.com/2007/11/26/el-banco-central-vs-paypal-moneybookers-yotros/>).

### Legislación internacional

#### Paraguay

Ley Número 1015 (1996) “Que previene y reprime los actos ilícitos destinados a la legitimación de dinero o bienes” Disposiciones Generales:

#### Artículo 1. Ámbito de aplicación.

“La presente ley: regula las obligaciones, las actuaciones y los procedimientos para prevenir e impedir la utilización del sistema financiero y de otros sectores de la actividad económica para la realización de los actos destinados a la legitimación del dinero o bienes que procedan, directa

o indirectamente, de las actividades delictivas contempladas en esta ley. Actos caracterizados en adelante como delitos de lavado de dinero o de bienes; tipifica y sanciona el delito lavado de dinero o bienes; y, le aplicará sin perjuicio de otras acciones y omisiones tipificadas y sancionadas en la ley penal.”

### Argentina

Ley Número 26.023 del 30 de marzo de 2008 – (Art. 4 inciso C) Artículo 4 - Medidas para prevenir, combatir y erradicar la financiación del terrorismo 1. Cada Estado Parte, en la medida en que no lo haya hecho, deberá establecer un régimen jurídico y administrativo para prevenir, combatir y erradicar la financiación del terrorismo y para lograr una cooperación internacional efectiva al respecto, la cual deberá incluir: (Alertan sobre el tráfico de drogas y el lavado de dinero por Internet (jueves 7 de marzo de 2002). Descargado el 2 de mayo de 2009 en periódico Clarin En-Línea: <http://www.clarin.com/diario/2002/03/07/s-354996.htm>, Legislation Paraguay. Descargado el 2 de mayo de 2000: <http://www.lexadin.nl/wlg/legis/nofr/oeur/lxwepar.htm>: Gil Lavedra y D' Alessio presentan proyecto para constituir al terrorismo internacional como crimen de lesa humanidad (19 de octubre de 2009). Descargado el 2 de mayo de 2009 en el periódico UCRCapital En-Línea: [http://www.ucrcapital.org.ar/noticias\\_detalle.php?id=106](http://www.ucrcapital.org.ar/noticias_detalle.php?id=106)). Medidas que aseguren que las autoridades competentes dedicadas a combatir los delitos establecidos en los instrumentos internacionales enumerados en el artículo 2 tengan

la capacidad de cooperar e intercambiar información en los niveles nacional e internacional, de conformidad con las condiciones prescritas en el derecho interno. Con ese fin, cada Estado Parte deberá establecer y mantener una unidad de inteligencia financiera que sirva como centro nacional para la recopilación, el análisis y la difusión de información relevante sobre lavado de dinero y financiación del terrorismo.

Cada Estado Parte deberá informar al Secretario General de la Organización de los Estados Americanos sobre la autoridad designada como su unidad de inteligencia financiera.

Artículo 6. Delitos determinantes del lavado de dinero 1. Cada Estado Parte tomará las medidas necesarias para asegurar que su legislación penal referida al delito del lavado de dinero incluya como delitos determinantes del lavado de dinero los delitos establecidos en los instrumentos internacionales enumerados en el artículo 2 de esta Convención. Los delitos determinantes de lavado de dinero a que se refiere el párrafo 1 incluirán aquellos cometidos tanto dentro como fuera de la jurisdicción del Estado Parte.

### **Marruecos**

Reglamento de la Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de prevención del blanqueo de capitales, aprobado por Real Decreto 925/1995, de 9 de junio, en relación con el informe de experto externo sobre los procedimientos y órganos de control interno y comunicación establecidos para prevenir el blanqueo de capitales.

### **Conclusión**

Si Darwin, en su teoría de la evolución de las especies, hubiera intentado explicarla basándose en la rápida adaptación y transformación de los criminales, cómo “evolucionan”, a los cambios que surgen en la sociedad, más personas le hubieran entendido y no hubiera terminado en tal controversia milenaria con la Iglesia.

Entendemos que, el lavado de dinero es una actividad ilícita, la cual ha estado presente por muchos años en el mundo. A medida que surgen cambios sociales y avances tecnológicos, la actividad criminal se adapta a los nuevos patrones de comportamiento social y logra evadir eficazmente las leyes promulgadas en contra de la criminalidad.

Además, el criminal se beneficia de todos aquellos adelantos tecnológicos que puedan ayudar a que sus operaciones ilícitas sean “exitosas”. Operaciones desde las más sencillas como hacer un pago de un artículo por Internet, hasta las más complejas, como llevar a cabo transferencias de un banco a otro que se encuentra en otro país. Todos estos adelantos tecnológicos y financieros, a la misma vez que proveen un manto de protección al consumidor y al mercader, a la misma vez abren una puerta para dejar pasar a los que necesitan llevar a cabo transacciones ilícitas, para que parezcan totalmente legítimas.

Es una tarea ardua el lograr detener estas prácticas, pues muchas veces poner en vigor las mismas, puede traer como consecuencia una carga económica a las empresas bancarias, comercios, etc. O también pueden implicar violaciones a los derechos civiles si hay intervenciones



generalizadas contra algún ciudadano que sea sospechoso de delito. El intento legítimo de las empresas procesadoras de pagos electrónicos a veces no es suficiente, puesto que muchas veces ya los criminales conocen a cabalidad las políticas internas sobre el manejo de los fondos y la información y logran evadir las técnicas impuestas para prevención o detención del problema.

Como polémica mundial, tiene un efecto económico directo en los mercados globales. Los recaudos tanto de negocios *bona fide* y de los gobiernos centrales de los países se ven afectados, puesto que hay una merma en cuanto a ventas y/o recolección de impuestos para poder sustentar a la población nacional en cuanto proveer los servicios gubernamentales. Los países crean sus propias políticas en contra del lavado de dinero y en conjunto con tratados entre las naciones intentan controlar las actividades criminales. Son esfuerzos positivos y afirmativos, aunque hay que reconocer que el mundo subterráneo de las empresas delictivas logra muchas veces burlar todas estas trabas que imponen las naciones.

### Referencias

- BUMETER, B. H. (2001). *Cyberlaundering: Low Tech meets High Tech*. Descargado el 2 de mayo de 2009 de Maven Mapper's Information Web site: <http://www.softduit.com/mavenmappersinformation/2001/06/01/cyberlaunderinglow-tech-meets-high-tech/>
- Condiciones del Servicio de Google Checkout. Descargado: 29 de abril de 2009 de Google Checkout: <https://checkout.google.com/termsOfService?type=Buyer>
- Cyber Laundering: The Risks to On-line Banking and E-Commerce Companies. Descargado el 1 de mayo de 2009 de Stop money laundering! International conference (Londres, febrero, 2002): <http://www.antimoneylaundering.ukf.net/papers/solicitor.htm>
- FILIPKOWSKI, W. (1 January - June 2008). *Cyber Laundering: An Analysis of Typology and Techniques*. Descargado el 23 de 12 de abril de 2009 de International Journal of Criminal Science: <http://cjsjournal.brinkster.net/wojciech.html>
- Lavedra, Gil y D'Alessio presentan proyecto para constituir al terrorismo internacional como crimen de lesa humanidad (19 de octubre de 2009). Descargado el 2 de mayo de 2009 en el periódico *UCRCapital* En-Línea: [http://www.ucrcapital.org.ar/noticias\\_detalle.php?id=106](http://www.ucrcapital.org.ar/noticias_detalle.php?id=106)
- GROW, B. (2006). *Gold Rush*, [Versión Electrónica] Business Week, January 9, 2006. Descargado 12 de abril de 2009 de Business Week Online: [http://www.businessweek.com/magazine/content/06\\_02/b3966094.htm](http://www.businessweek.com/magazine/content/06_02/b3966094.htm)
- LAYTON, J. *How Money Laundering Works*. Descargado el 25 de abril de 2009 de How Stuff Works: <http://money.howstuffworks.com/money-laundering3.htm>
- Legislation Paraguay. Descargado el 2 de mayo de 2000: <http://www.lexadin.nl/wlg/legis/nofr/oeur/lxwepar.htm>
- LILLEY P. (2006). *The Untold Truth About Glo-*

- bal Money Laundering, International Crime and Terrorism*. Descargado 3 de mayo de 2009 de Proximal Consulting: [http://www.proximalconsulting.com/Pages/dirtydealing/dirty%20dealing\\_PP.pdf](http://www.proximalconsulting.com/Pages/dirtydealing/dirty%20dealing_PP.pdf)
- Money Laundering in Digital Currencies* (2008). Descargado el 25 de abril de 2009 de National Drug Intelligence Center Website: <http://www.usdoj.gov/ndic/pubs28/28675/intro.htm>
- Política de privacidad de Google Checkout*. Descargado el 29 de abril de 2009 de Google Checkout: <https://checkout.google.com/files/privacy.html>
- Privacy Policies for Paypal Services*. Descargado el 29 de abril de 2009 de PayPal: [https://www.paypal.com/us/cgi-bin/webscr?cmd=p/gen/ua/policy\\_privacy-outside](https://www.paypal.com/us/cgi-bin/webscr?cmd=p/gen/ua/policy_privacy-outside)
- RIJOCK, K. (2007). *Virtual money laundering now available on the world wide web*. Descargado el 12 de abril de 2009 de World Check: <http://www.worldcheck.com/articles/2007/01/02/virtual-money-laundering-now-available-worldwide/>
- The Global Response to Money Laundering*. Descargado 2 de mayo de 2009, de la página web del Australian Institute of Criminology: <http://www.aic.gov.au/conferences/2002-ml/part1.pdf>
- UN General Assembly Special Session on the World Drug Problem* (8-10 June 1998). Descargado el 26 de abril de 2009 de la página web de las Naciones Unidas: <http://www.un.org/ga/20special/featur/laundry.htm>
- USA PATRIOT Act: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 26 de octubre de 2001, 115 Stat. 272
- U.S. v. E-Gold, 550 F.Supp.2d 82 (2008)