

**CENTRO DE EDUCAÇÃO SUPERIOR REINALDO RAMOS - CESREI**  
**FACULDADE REINALDO RAMOS - FARR**  
**CURSO DE BACHARELADO EM DIREITO**

**MAÉCIO MAGENI DAMASCENO DE SANTANA FILHO**

**OS CRIMES VIRTUAIS E AS NOVAS MODALIDADES DE LAVAGEM DE  
DINHEIRO**

Campina Grande – PB

2018

**MAÉCIO MAGENI DAMASCENO DE SANTANA FILHO**

**OS CRIMES VIRTUAIS E AS NOVAS MODALIDADES DE LAVAGEM DE  
DINHEIRO**

Trabalho de Conclusão de Curso – TCC,  
apresentado à Coordenação do Curso de  
graduação em Direito do Centro de Ensino Superior  
Reinaldo Ramos - CESREI, em cumprimento aos  
requisitos parciais para obtenção do grau de  
Bacharel em Direito.

Orientador: Prof.º MS. Rodrigo Araújo Reül.

CAMPINA GRANDE

2018

S232c Santana Filho, Maécio Mageni Damasceno de.  
Os crimes virtuais e as novas modalidades de lavagem de dinheiro /  
Maécio Mageni Damasceno de Santana Filho. – Campina Grande, 2018.  
55 f.

Monografia (Graduação em Direito) – Faculdade Reinaldo Ramos-  
FAAR, Centro de Educação Superior Reinaldo Ramos-CESREI, 2018.  
"Orientação: Prof. Me. Rodrigo Araújo Reül".

1. Crimes Virtuais – Lavagem de Dinheiro. 2. Crimes na Internet.  
3. Internet – Lavagem de Dinheiro – Bitcoins. I. Reül, Rodrigo Araújo. II.  
Título.

CDU 343.359.3:004.738.5(043)

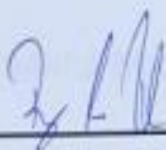
---

MAÉCIO MAGENI DAMASCENO DE SANTANA FILHO

OS CRIMES E AS NOVAS MODALIDADES DE LAVAGEM DE DINHEIRO

Aprovada em: 11 de JUNHO de 2016.

**BANCA EXAMINADORA**

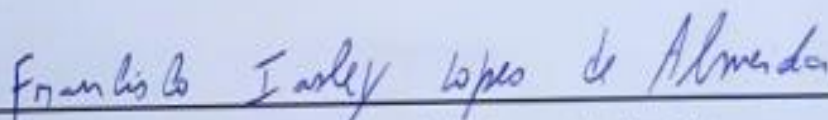


---

Prof. Ms. Rodrigo Araújo Reul

Faculdade Reinaldo Ramos FARR/ CESREI

(Orientador)

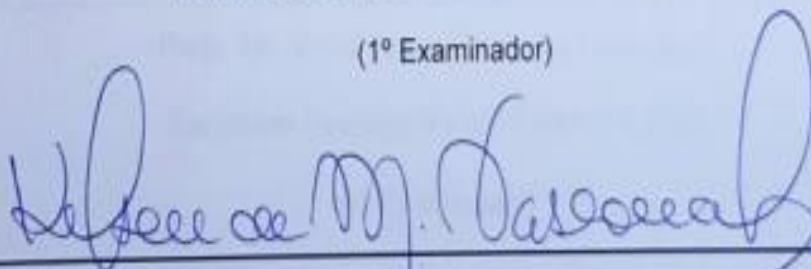


---

Prof. Esp. Francisco lasley Lopes de Almeida

Faculdade Reinaldo Ramos FARR/ CESREI

(1º Examinador)



---

Prof. Ms. Kelsen de Mendonça Vasconcelos

Faculdade Reinaldo Ramos FARR/ CESREI

(2º Examinador)

## **AGRADECIMENTOS**

A Deus, por ter me mantido de pé nesta caminhada. Ter me dado força e coragem para perseverar, mesmo diante das dificuldades surgidas no caminho.

Aos meus pais, Maécio M. D. De Santana, Marcelina Oliveira Santana, por sempre acreditarem em mim e, jamais me deixar desistir dos meus objetivos.

Minha namorada, Jéssica Mylena Justino e, minha sogra Maria José de Souza por jamais me deixar desistir e ser conforto nas horas mais difíceis.

Ao meu Grande Amigo Severino Felix, que me deu muita força, coragem e que me acompanha a bastante tempo. Sem esquecer de sua avó Dona Rita, e sua tia Marines, que nos acompanham.

Aos meus amigos, Arnon Hiluey, Glauber Costa, Jéssica Renale, Muriene Lima, Marikya Rocha, Gamaliel Gonzaga, primeiramente pela amizade, que jamais deixemos esse laço se desfazer. Mas também por todo apoio nas horas fáceis e difíceis nestes cinco anos de convivência diária.

A meus avos João de Deus e Maria Alaíde, com seus conselhos e confortos.

O meu grande orientador e professor, Rodrigo Araújo Reul, por todo altruísmo e prontidão para me ajudar a construir esta pesquisa.

A liberdade, que é uma conquista, e não uma doação, exige permanente busca. Busca permanente que só existe no ato responsável de quem a faz. Ninguém tem liberdade para ser livre: pelo contrário, luta por ela precisamente porque não a tem. Ninguém liberta ninguém, ninguém se liberta sozinho, as pessoas se libertam em comunhão.

*Paulo Freire*

## RESUMO

A lavagem de dinheiro é um fenômeno de proporções mundiais que não respeita mais nenhuma fronteira. As melhores ofertas de condições econômicas e de investimentos fazem com que elevadas quantias de dinheiro sejam movimentadas para outros países em frações de segundos. Aliado as tecnologias e ao uso da internet, bem como ao uso de moedas virtuais e diante da possibilidade de total anonimato, a lavagem de dinheiro vem se tornando também uma das principais modalidades de crimes virtuais em todo o mundo. O presente estudo teve como objetivo geral compreender a dinâmica do crime de lavagem de dinheiro no meio virtual. De maneira específica, buscou-se contextualizar os conceitos de crime virtual e de lavagem de dinheiro, assim como analisar como e quando ocorrem estes tipos de crime. Buscou-se ainda analisar a legislação e os mecanismos prevenção e repressão dessa nova modalidade criminosa. Para tanto, foi realizada uma pesquisa exploratória de abordagem qualitativa. No caso dos crimes virtuais, a pesquisa mostrou que a lavagem de dinheiro no meio virtual ocorre atualmente de duas formas principais: através do uso das criptomoedas ou *bitcoins* e do tráfico de drogas e armas por meio da *deep web*. As dificuldades de detecção das atividades suspeitas envolvendo as criptomoedas se devem ao fato de que as transações não ocorrem no sistema bancário oficial. Além disso, os *bitcoins* podem facilmente ser convertidos em qualquer outra moeda corrente sem grandes dificuldades. Na *Deep Web*, o tráfico de armas e drogas é até mais diversificado que no “mercado” presencial facilita o crime de lavagem de dinheiro por que impossibilita a identificação dos vendedores e compradores, a identificação da origem dos produtos e a investigação policial. Verificou-se que a legislação brasileira é escassa e precisa urgentemente se adequar as inovações advindas da tecnologia, como a lavagem de dinheiro por meio virtual. A inexistência de um sistema normativo eficaz que regule a utilização de moedas ou mercados negros virtuais pode resultar em operações policiais frustradas, aumento da impunidade, não identificação dos agentes da lavagem de dinheiro e trazer prejuízos até mesmo para a estabilidade da moeda brasileira dentro e fora do país.

Palavras-Chave: Crimes virtuais. Lavagem de dinheiro. *Bitcoins*. *Deep web*.

## ABSTRACT

Money laundering is a phenomenon of global proportions that no longer respects any frontier. The best offers of economic conditions and investments make large amounts of money move to other countries in fractions of seconds. Combined with technologies and the use of the internet, as well as the use of virtual currencies and the possibility of total anonymity, money laundering has also become one of the main forms of virtual crimes worldwide. The objective of this study was to understand the dynamics of the crime of money laundering in the virtual environment. Specifically, we tried to contextualize the concepts of virtual crime and money laundering, as well as analyze how and when these types of crime occur. It was also sought to analyze the legislation and mechanisms for prevention and repression of this new criminal modality. For that, an exploratory qualitative approach was carried out. In the case of cybercrime, research has shown that money laundering in the virtual environment currently occurs in two main ways: through the use of crypto-coins or bitcoins and the trafficking of drugs and weapons through the deep web. The difficulties in detecting suspicious activities involving crypto-coins are due to the fact that transactions do not occur in the official banking system. In addition, bitcoins can easily be converted into any other currency without major difficulties. In the Deep Web, the trafficking of arms and drugs is even more diversified than in the "market" in person facilitates the crime of money laundering because it makes it impossible to identify the sellers and buyers, the identification of the origin of the products and the police investigation. It was verified that Brazilian legislation is scarce and urgently needs to adapt the innovations coming from technology, such as money laundering by virtual means. The lack of an effective regulatory system that regulates the use of virtual black currencies or markets may result in frustrated police operations, increased impunity, non-identification of money laundering agents, and even damage to the stability of Brazilian currency inside and outside from the country.

Keywords: Virtual Crimes. Laundering of monetary instruments. Bitcoin. Deep weeb.



## SUMÁRIO

<b>INTRODUÇÃO</b> .....	<b>0</b>
<b>CAPÍTULO I</b> .....	<b>3</b>
1. A INTERNET E OS CRIMES VIRTUAIS .....	3
1.1 - BREVE HISTÓRICO DO SURGIMENTO DA INTERNET .....	3
1.2 - A INTERNET NO BRASIL .....	5
1.3 - OS CRIMES VIRTUAIS .....	7
<b>1.3.1 - Os crimes virtuais próprios</b> .....	<b>10</b>
<b>1.3.2 - Os crimes virtuais impróprios</b> .....	<b>11</b>
1.4 - A LEGISLAÇÃO BRASILEIRA E OS CYBERCRIMES .....	13
<b>CAPÍTULO II</b> .....	<b>15</b>
<b>2. O CRIME DE LAVAGEM DE DINHEIRO</b> .....	<b>15</b>
2.1 - CONCEITOS E ASPECTOS HISTÓRICOS .....	15
2.2 - AS FASES DA LAVAGEM DE DINHEIRO .....	18
2.3 - PRINCIPAIS TIPOLOGIAS .....	21
2.4 - A LEGISLAÇÃO BRASILEIRA .....	24
<b>CAPÍTULO III</b> .....	<b>27</b>
<b>3. OS CRIMES VIRTUAIS E AS NOVAS MODALIDADES DE LAVAGEM DE DINHEIRO</b> .....	<b>27</b>
3.1 - AS CRIPTOMOEDAS COMO INSTRUMENTO DE LAVAGEM DE DINHEIRO .....	28
3.2 - A LAVAGEM DE DINHEIRO ORIUNDA DO TRÁFICO DE DROGAS E ARMAS NA <i>DEEP WEB</i> .....	31
3.3 - A ESCASSEZ DE LEGISLAÇÃO ESPECÍFICA NO BRASIL .....	34
3.4 - PROPOSTAS DE AÇÕES PREVENTIVAS E REPRESSIVAS .....	37
<b>CONCLUSÃO</b> .....	<b>40</b>
<b>REFERÊNCIAS</b> .....	<b>43</b>

## INTRODUÇÃO

Com a sociedade cada vez mais globalizada e a crescente evolução tecnológica, as distâncias entre as pessoas e as organizações encurtaram. As relações passaram se construir por meio de equipamentos eletrônicos, redes sociais, *smartphones* e outros dispositivos conectados à internet. É o que se chama de era digital, onde culturas diferentes começaram a se encontrar através da rede mundial de computadores. Por sua vez o Direito deve se adaptar à nova realidade, caminhar em conjunto com essas transformações e com a segurança da informação para que o Estado mantenha sua função jurisdicional (CAETANO; MENEZES, 2015).

Na verdade o Direito se faz presente em praticamente todos os momentos da vida dos indivíduos que compõem os Estados Democráticos de Direito, como no caso do Brasil. Ao longo dos anos, o Direito tem sido a ferramenta para dar solução aos conflitos interpessoais e institucionais que surgem dia a dia na sociedade moderna e que avançam em ritmo acelerado, devido às inúmeras descobertas e melhorias tecnológicas que visam facilitar a vida de todos. Pelo seu caráter regulador e reorganizador, cabe ao direito acompanhar todas as mudanças tecnológicas pelas quais a sociedade passa.

Nesse sentido, a evolução tecnológica permitiu o surgimento da rede mundial de computadores, mais conhecida como internet, capaz de interligar pessoas e países do mundo inteiro. Entretanto, o que a princípio surgiu como uma tecnologia comunicação se transformou em um dos maiores instrumentos de utilizados para a prática de condutas delituosas, cada vez mais perigosas. A internet se tornou um ambiente propício para o cometimento de novos delitos, alguns ainda desconhecidos e outros não, como no caso da lavagem de dinheiro (ANDRADE, 2017).

A lavagem de dinheiro pode ser conceituada como um processo pelo qual um ou mais agentes objetivam ocultar ou dissimular a origem de determinados bens, direitos ou valores relacionados a atividades ilícitas, mediante a utilização de operações comerciais ou financeiras, redirecionando esses ativos sem atrair a atenção do Estado. Em outras palavras, a lavagem de dinheiro é uma atividade que busca demonstrar uma origem aparentemente lícita aos ativos provenientes de atividades delituosas (BARROS, 2013).

No Brasil, a atividade de lavagem de recursos de origem ilícita ou duvidosa passou a ser considerado crime a partir do advento da Lei nº. 9.613 de 1998. Na redação da lei, o legislador optou por utilizar o termo “lavagem” para designar a conduta penal típica. A origem dessa expressão está ligada a tradição anglo-saxônica que consagrou o uso da expressão “*Money laundering*”, muito embora em outros países a nomenclatura adotada tenha sido outra. O citado dispositivo legal foi substituído, em 2012, pela Lei nº. 12.683.

De acordo com Andrade (2017), o crime de lavagem de dinheiro atualmente possui várias modalidades, dentre as quais se destacam o envio não declarado do dinheiro sujo para paraísos fiscais, a compra de bens ou a criação de empresas em nomes de terceiros (laranjas) e a compra de joias, imóveis e automóveis. Entretanto, uma nova modalidade de lavagem de dinheiro vem chamando a atenção da sociedade das autoridades, qual seja a lavagem de dinheiro pelo meio digital, usando criptomoedas, câmbio ilegal e atividades desenvolvidas no mercado negro da internet, conhecido como *deep web*.

Diante dessa realidade, o presente estudo se norteou pelos seguintes questionamentos: Quais são as particularidades do crime de lavagem de dinheiro utilizando o meio virtual? Nessa perspectiva, a falta de regulamentação específica para esta modalidade delituosa possui relação com sua expansão?

Para responder a estes questionamentos, o estudo tem como objetivo geral compreender a dinâmica do crime de lavagem de dinheiro no meio virtual. De maneira específica, busca-se contextualizar os conceitos de rede mundial de computadores, de crime virtual e de lavagem de dinheiro, assim como analisar como ocorre o crime, quando ocorre e quais as suas principais modalidades, características e fins. Pretende-se ainda analisar a legislação e os mecanismos de prevenção e repressão dessa nova modalidade criminosa, que cresce sem o controle do Estado.

## **METODOLOGIA**

Em termos metodológicos, realizou-se uma pesquisa exploratória de abordagem qualitativa. A pesquisa qualitativa busca captar não apenas a aparência do fenômeno, mas também as suas essências, explicando as suas origens, relações e mudanças e tentando determinar suas consequências. Ou seja, a utilização desse

tipo de abordagem propicia o aprofundamento da investigação das questões relativas ao fenômeno abordado, mediante a valorização do contato direto com as situações já que na pesquisa qualitativa a preocupação é muito maior com o processo do que com o produto (GIL, 2008).

Em relação aos procedimentos técnicos adotados, foi utilizada a pesquisa bibliográfica, caracterizada como um apanhado geral sobre os principais trabalhos já realizados, revestidos de importância, por serem capazes de fornecer dados atuais e relevantes sobre o tema (MARCONI; LAKATOS, 2017). Nesse sentido, foram utilizados livros, revistas e artigos científicos, respeitando um critério de antiguidade razoável. Para Gil (2008), quando se necessita de qualquer tipo de informação acerca de determinado assunto, deve-se recorrer justamente ao auxílio da bibliografia existente, a fim de se obter respostas, como ocorre no caso do presente estudo.

Visando facilitar a compreensão do tema e alcançar os objetivos da pesquisa, o estudo foi dividido em três momentos. No primeiro capítulo, buscou apresentar os conceitos de internet e de crimes virtuais, mostrando suas modalidades na forma própria e imprópria e fazendo uma ponte com os crimes virtuais praticados com o objetivo de fraude. No segundo capítulo, foram abordados os conceitos, características e modalidades do crime de lavagem de dinheiro e as suas relações com o crime organizado. Por fim, o terceiro capítulo da nova modalidade de crime virtual, qual seja a lavagem de dinheiro, explicitando seus métodos e construindo uma proposta de prevenção e repressão.

## CAPÍTULO I

### 1. A INTERNET E OS CRIMES VIRTUAIS

Atualmente a internet é o meio de comunicação em massa mais difundido em todo o mundo, tendo em vista a sua capacidade infindável de facilitar e modernizar a vida das pessoas que vivem em sociedade. De acordo com Pinheiro (2013), em virtude da sua capacidade tecnológica, existe uma grande quantidade de pessoas que utilizam as suas informações, quer seja para entretenimento, como ferramenta de trabalho, ferramenta de pesquisa e até mesmo para a prática de ilícitos. Nesse capítulo, busca-se justamente descrever como surgiu a rede mundial de computadores, bem como realizar uma abordagem histórica e jurídica acerca dos crimes virtuais, suas características e modalidades.

#### 1.1 - BREVE HISTÓRICO DO SURGIMENTO DA INTERNET

A internet foi criada inicialmente para fins militares e servia como base de apoio para as comunicações entre os militares norte-americanos em caso de eventuais investidas de inimigos que pudessem colocar em risco as informações repassadas através dos meios comuns de comunicação. A internet surgiu na década 1960, logo após o fim da segunda guerra mundial e o início da guerra fria, período em que EUA e União Soviética disputavam o poder econômico, político e militar de todo o mundo (LEMOS, 2010).

Wertheim (2001), explica que no ano de 1957 a União Soviética lançou ao espaço o Sputnik, primeiro satélite artificial existente no mundo, com a finalidade de realizar estudos envolvendo radiação e capacidade de lançamento de cargas para o espaço, o que compeliu os EUA a criar uma agência específica para conseguir realizar os mesmo tipos de pesquisa ou desenvolver tecnologias iguais ou melhores aos dos soviéticos. Surgiu então a *Advanced Research Projects Agency* – ARPA, com a missão de pesquisar e desenvolver tecnologias para as forças armadas.

Depois de criar a ARPA o governo americano verificou a necessidade de criar na agência, um mecanismo para tratar exclusivamente de assuntos secretos e informações sigilosas, quer recebeu o nome de ARPAnet. Tal mecanismo funcionava através de várias redes locais e privadas de baixo alcance, batizadas posteriormente de *Local Area Network* ou LAN e que tinham como objetivo agrupar

as informações das pesquisas americanas e enviava-las para as partes interessadas, quando necessário (CALAZANS; LIMA, 2013).

De acordo com Abreu :

O apoio financeiro do governo norteamericano através da pesquisa promovida pelo Departamento de Defesa dos Estados Unidos por meio da ARPA - Administração dos Projetos de Pesquisa Avançada, já em 1968, foi o impulso para a implantação do sistema de informação em rede. Iniciada com objetivos militares, propondo uma sobrevivência aos elementos partícipes por não estarem conectados de modo hierárquico, característica marcante daquele setor, a disposição em rede permitia a não ameaça ao cabeça do programa, caso fosse atacada. Era crucial que a arquitetura do sistema fosse diferente daquela apresentada pela rede de telefonia norte-americana. (ABREU, 2008, p. 2)

A ARPAnet utilizava-se ainda de um *backbone*, link de alta velocidade e que é usado geralmente como a espinhal dorsal das redes. A internet, no formato conhecido atualmente é formada justamente por esses *backbones* que interligam redes, pessoas, instituições e provedores de acesso, dentre outros. A ARPAnet conectava os militares e investigadores sem que eles estivessem em um local fixo, podendo ser encontrados em qualquer lugar onde houvesse cobertura da tecnologia. Esse avanço foi capaz de evitar perda de informações e resguardar aquelas que já estavam no banco de dados (WERTHEIM, 2001).

De acordo com Abreu (2008), a internet foi disponibilizada para uso acadêmico e científico no início da década de 1970, funcionando como sistema de comunicação entre alunos e professores ou professores e pesquisadores. Essa disponibilização para o meio acadêmico foi o primeiro passo para expansão da rede e a sua evolução para os moldes conhecidos hoje em dia.

Entretanto, uma das dificuldades do ARPAnet era conectar computadores de fabricantes diferentes e que falavam idiomas diferentes. Foi então que surgiram os primeiros protocolos de comunicação, uma espécie de linguagem comum a todos os computadores e que tratavam desde o nível físico até a aplicação da informação transmitida.

O TCP/IP é o protocolo atualmente usado na internet. Os primeiros testes realizados naquela época conseguiram transmitir cerca de 1.800 conversações de voz de uma só vez por meio de um único cabo. Vinte anos depois, na década de 1990 a maior capacidade registrada era de condução de 230 mil conversações

simultâneas. Atualmente um cabo de fibra ótica, da espessura de um fio de cabelo, conduz quase 10 milhões de conversações simultâneas (CARVALHO, 2006).

Em 1990 o ARPAnet foi desativado, sendo colocado em seu lugar o *Defense Research Internet* – DRI e em 1992 a ANSNET, que passou a ser o principal *backbone* da internet. Nessa mesma época iniciou-se o desenvolvimento de um *backbone* europeu, interligando alguns países da Europa à internet (CALAZANS; LIMA, 2013). A partir de 1993 a internet deixou de ser uma instituição voltada apenas para o meio acadêmico e de pesquisas e passou a ser explorada comercialmente, tanto para construção de novos *backbones* por empresas privadas, como para fornecimento de serviços diversos e com cobertura mundial.

## 1.2 - A INTERNET NO BRASIL

Segundo Recuero (2011), o processo de inserção da internet no Brasil ocorreu de forma lenta e progressiva, através de uma série de programas e ações do Governo Federal, voltadas para o desenvolvimento do setor de telecomunicações nacional. Esse processo para a criação de um sistema de telecomunicações nacional começou pouca antes do primeiro governo militar tomar o poder no país.

Até a década de 1960 o setor de telecomunicações no Brasil era dominado por empresas privadas, com prestação de serviços de baixa qualidade e deixando regiões mais pobres sem o serviço. O governo militar de 1964 com sua agenda voltada para a integração nacional promoveu a implantação do CBT e a estruturação do CONTEL, que depois foi substituído pelo Ministério das comunicações e a construção da Empresa Brasileira de Telecomunicações (EMBRATEL), (LEMOS, 2010).

Nas palavras de Carvalho :

Em 1964, os militares tomaram o poder e se empenharam para que o Brasil dispusesse de uma infra-estrutura moderna de telecomunicações, necessária à segurança e ao desenvolvimento da integração nacional. Até então o setor de telecomunicações era dominado por empresas privadas, sendo extremamente fragmentado e de baixa qualidade. Este modelo não interessava ao governo brasileiro, pois deixava regiões pobres totalmente desatendidas e implicava na operação das comunicações estratégicas por empresas estrangeiras. (CARVALHO, 2006, p. 51)

De acordo com Abreu (2008), no início da década de setenta, em virtude do aumento do uso de equipamentos eletrônicos no país, o Ministério das Comunicações passou a se preocupar com a questão da transferência eletrônica de dados. Para isso foi criada no ano de 1979 a Secretaria Especial de Informática – SEI, subordinada ao Conselho Nacional do Presidente General João Figueiredo. Após assumir o controle da informática no país, a SEI passou a cuidar também do fluxo internacional dos dados e decidir sobre que tipo de informação estaria acessível aos usuários.

Entretanto, essa subordinação dificultava o desenvolvimento do País nessa área. Por isso, muitos países sedes de grandes agências de notícias defendiam o livre fluxo de informações, apontando questões de ordem política, econômica e tecnológica.

Segundo Carvalho:

O modelo brasileiro estava afinado com o panorama internacional da época, que tratava as telecomunicações como um monopólio. Nos países europeus, o sistema de telecomunicações era baseado em monopólios estatais, assim como no Japão. Nos Estados Unidos havia um monopólio privado para as comunicações de longa distância, estabelecido ainda no início do século, em torno da AT&T.(CARVALHO. 2006, p. 52)

Apenas no final do regime militar, em 1984, a política de informática deixou de ser de competência exclusiva do Poder Executivo, levando o debate também para as instituições acadêmicas, que enxergavam na tecnologia uma importante ferramenta para a capacitação e comunicação de seus membros, assim como ocorria nos EUA. Assim, após um intenso debate o Congresso Nacional aprovou a Lei n. 7.732 de 1984, também conhecida como Lei da Informática que democratizou os processos decisórios e criou o CONIN – Conselho Nacional de Informática e Automação (RECUERO, 2011).

De acordo com Lemos (2010), o processo de implantação da internet no país teve início com uma série de desafios. Após o fim do regime militar começou a disseminação de computadores nas organizações, nas instituições acadêmicas, mas principalmente nas residências, como o objetivo de se comunicar através dos computadores, com a utilização do modem em conjunto com a telefonia convencional. Entretanto, o serviço ainda era muito precário, o que desencadeou a



realização de novos projetos e pesquisas para que se chegasse ao modelo utilizado atualmente.

Calazans e Lima (2013), explicam ainda que a primeira rede no Brasil ocorreu por meio da criação da Rede Nacional de Pesquisa – RNP, em setembro de 1989, com o objetivo de construir um ambiente acadêmico virtual para estudo e pesquisas. O RNP foi criado pelo Ministério de Ciência e Tecnologia e se dedicava a várias tarefas como disseminar o uso da rede em todo território nacional e divulgar e conscientizar a população sobre o uso correto da internet por meio de seminários, feiras e treinamentos, se tornando referências em aplicações.

Mas foi a partir do ano de 1994, depois do lançamento da *World Wide Web* que as empresas que ofereciam o serviço de rede isolada passaram a atuar como provedores de acesso a internet, viabilizando o conteúdo da rede para seus assinantes. Foi quando também surgiram as grandes lojas de comércio eletrônico como *Amazon* e *ebay*, dentre outros que passaram a buscar seu espaço nesse novo mercado em expansão (ABREU, 2008).

De acordo com Recuero (2011), porém, a internet comercial só chegou ao Brasil no ano de 1996 com um serviço totalmente obsoleto e com uma estrutura insuficiente para atender os provedores de acesso e os usuários. Entretanto, seu uso cresceu rapidamente, não apenas entre pessoas, mas entre as empresas para realização de negócios e comércio eletrônico. Começaram a surgir as lojas virtuais, portais de conteúdo e redes sociais.

Dessa forma, a internet progrediria para se tornar o sinal mais material e visível da globalização mundial. O computador deixou de representar uma tecnologia isolada, como uma calculadora ou manipulador de imagem, e passou a ser uma espécie de filtro para todas as formas culturais, mediando os tipos de produção. Por outro lado, a internet que antes era usada apenas para fins militares e acadêmicos, também passou a ser usada para fins comerciais, de comunicação interpessoal e até para a prática de delitos, conforme destacado no tópico adiante.

### 1.3 - OS CRIMES VIRTUAIS

A definição de crime é analisada pelos doutrinadores sobre diversos prismas. Em termos materiais, o crime é definido como sendo a violação de um bem juridicamente protegido. Essa definição segue o critério de que quando um bem tutelado é atingido, o direito penal deve punir. Já sob a ótica formal, o crime pode ser definido como uma conduta vedada por lei em decorrência da política criminal adotada pelo Estado. Trata-se da visão do legislador sobre os bens que devem ser juridicamente tutelados. Por fim, o conceito analítico do crime que é dividido em duas vertentes a bipartição e a tripartição. (CRESPO, 2011).

Para a teoria bipartida, o crime é considerado um fato típico e antijurídico, e a culpabilidade é apenas o fator responsável pela dosagem da pena. Por outro lado, a teoria tripartida defende que o crime é um fato típico, antijurídico e culpável. Ambos os conceitos sofrem influência da teoria das ações, mas o conceito advindo da teoria tripartida é mais amplo e abrangente. É exatamente a definição adotada por Nucci, ao afirmar que o crime:

Trata-se de uma conduta típica, antijurídica e culpável, vale dizer, uma ação ou omissão ajustada ao modelo legal de conduta proibida (tipicidade), contrária ao direito (antijuricidade) e sujeita a um juízo de reprovação social incidente sobre o fato e seu autor, desde que existam imputabilidade, consciência potencial de ilicitude e exigibilidade e possibilidade de agir conforme o direito. (NUCCI 2011, p. 173)

A partir desses conceitos de crime é necessário também conceituar os crimes virtuais, objetos desse estudo. Os crimes virtuais são resultantes da evolução tecnológica pela qual passa a sociedade contemporânea. Os avanços tecnológicos e as novas descobertas da ciência trouxeram uma nova realidade política, econômica, social e cultural para a humanidade, de modo que o espaço e a presença física não são fundamentais para a realização de uma conduta delituosa. (CAETANO; MENEZES, 2015).

De acordo com Almeida e colaboradores (2015) é importante destacar que os crimes virtuais também são chamados de crimes digitais, crimes eletrônicos, *cybercrimes*, crimes cibernéticos, crimes de informática, dentre outros, que tratam da mesma modalidade delituosa. Para Colli (2010), a utilização da nomenclatura de *cybercrimes* seria mais adequada por se tratar de um termo genérico. Entretanto, em

se tratando de suas especificidades também é possível chama-los de crimes digitais ou crimes de informática.

Em que pese o não consenso entre os doutrinadores que abordam a temática e expõem a diversidade de nomenclaturas sobre essa modalidade criminosa, a que será utilizada nesse estudo será a nomenclatura de crimes virtuais, por entender que essas condutas são praticadas em ambientes virtuais ou com o uso destes.

Em relação ao seu conceito, Oliveira e colaboradores (2017) destacam que os crimes virtuais são aqueles delitos praticados por intermédio de um computador. Em uma abordagem mais ampla, podem ser conceituados também como ilícitos praticados por intermédio da internet ou com o auxílio desta, de modo que cause algum dano à vítima ou ainda práticas ilícitas penais contra o computador ou contra as informações contidas no mesmo.

De acordo com Caetano e Menezes (2015, p. 5):

Também chamados de crimes digitais, crimes eletrônicos, cyber crimes, crimes cibernéticos, entre outras nomenclaturas. São os nomes dados à atividade onde um computador ou rede destes é utilizada como base para cometimento de crimes ou facilitação para estes. Podendo se categorizar esses crimes de acordo com a sua forma de cometimento: os crimes que são cometidos utilizando o computador como instrumento para que se cometa a infração e aqueles que o crime é cometido contra o aparelho em si, o objeto é danificado ou violado de alguma forma. (CAETANO. MENEZES, 2015, p. 5)

Apesar de sua nomenclatura, os crimes associados a estes são de amplo conhecimento da sociedade e muito comuns como roubos, apropriação indébita, estelionato, chantagens, lavagem de dinheiro, dentre outros menos comuns, como acesso ilegal a base de dados, interceptação ilegal, obstrução de dados, deterioração ou supressão de arquivos de computador, interferência nos sistemas, uso indevido de equipamentos, falsificação de moeda, etc. (CRESPO, 2011).

Almeida e colaboradores (2015) citam ainda o exemplo do conceito de crime virtual utilizado pela Organização para Cooperação Econômica Desenvolvimento da ONU, no sentido de que o crime virtual, ou crime de informática, é qualquer conduta ilegal ou não autorizada que envolva processamento ou transmissão de dados. É toda ação antijurídica e culpável, que se utiliza do computador conectado a internet, servindo a esta como instrumento ou objeto do delito.

Em relação ao sujeito ativo do crime virtual, Oliveira e colaboradores (2017) explicam que estes podem ser os próprios usuários, que podem praticar alguma conduta ilícita sem a intenção de agir criminosamente, como divulgando fotos de terceiros sem autorização ou criando perfis falsos nas redes sociais; os *hackers*, que são pessoas com alto conhecimento e habilidade em informática; os *crackers*, que além dos conhecimentos de informática possuem habilidades para lidar com o mundo virtual e os *carders*, que atuam em pequenos grupos ou sozinhos, praticando pequenos delitos como roubos de senhas de cartão de crédito, fotos íntimas ou informações privilegiadas.

Em relação ao sujeito passivo nesse tipo de infração penal, segundo Crespo (2011), pode ser qualquer indivíduo normal, pessoa física ou jurídica, que podem ter seus bens desviados, seu patrimônio deteriorado ou informações violadas. Observe-se que muitos crimes virtuais praticados ainda não são divulgados, seja pela falta de amparo às eventuais vítimas, seja pela ausência de denúncias, como por exemplo, quando grandes empresas evitam divulgar ataques virtuais e invasões que demonstram a fragilidade da segurança.

Quanto a classificação doutrinária dos crimes virtuais, além dos sujeitos ativos e passivos, estes também são classificados em crimes virtuais próprios e crimes virtuais impróprios, conforme destaca a seguir.

### **1.3.1 - Os crimes virtuais próprios**

Segundo Pinheiro (2013), os crimes virtuais próprios são aqueles que só podem ser cometidos por meio da internet, ou seja, aquelas condutas que só podem realizadas tendo como ferramenta a rede mundial de computadores. Em outras palavras, são aqueles em que o bem jurídico ofendido é a tecnologia da informação propriamente dita. Até dez anos atrás a legislação penal era lacunosa em relação a esse tipo de crime, tendo em vista que diante do princípio da reserva legal, muitas práticas dessa natureza não poderiam ser enquadradas como crimes.

Para Colli (2010), os crimes virtuais próprios somente poderão ser cometidos com a utilização de ferramentas como computadores e internet, bem como outros recursos tecnológicos que possibilitem o seu acesso. Nos crimes virtuais impróprios o sujeito ativo utiliza-se necessariamente do sistema informático do computador do

sujeito passivo, de modo que o computador é o sistema tecnológico usado como meio para a execução do crime.

Em relação aos bens jurídicos atingidos nos crimes virtuais próprios, pode-se dizer que são a liberdade individual, a privacidade e a intimidade das pessoas de forma geral. É possível complementar essa linha de raciocínio afirmando ainda que são crimes que violam inicialmente a informação ou a privacidade como bem jurídica principal e que de maneira secundária atingem os dados ou sistemas.

Nas palavras de Almeida:

Os crimes virtuais próprios são aqueles em que o sujeito ativo utiliza o sistema informático do sujeito passivo, no qual o computador como sistema tecnológico é usado como objeto e meio para execução do crime. Nessa categoria de crimes está, não só a invasão de dados não autorizados, mas toda a interferência em dados informatizados como, por exemplo, invasão de dados armazenados em computador seja no intuito de modificar, alterar, inserir dados falsos, ou seja, que atinjam diretamente o software ou hardware do computador e só podem ser concretizados pelo computador ou contra ele e seus periféricos. (ALMEIDA. 2015, p. 224)

Alguns exemplos mais comuns de crimes virtuais próprios são o acesso não autorizado ou invasão de um sistema informático, como no caso de um hacker que acessa dados do sistema de uma determinada empresa, por exemplo; a obtenção e transferência ilegal de dados, como através de programas espiões ou vírus embutidos em publicidade; dano informático, que pode ser a bens materiais como computadores e eletrônicos ou bens imateriais como a honra e a imagem de uma pessoa ou empresa; disseminação de vírus e danos ao funcionamento de sistemas, dentre outros (DULLIUS; HIPPLER; FRANCO, 2012).

### **1.3.2 - Os crimes virtuais impróprios**

Os crimes virtuais impróprios, por sua vez são aquelas condutas já conhecidas, ou seja, crimes que já são de conhecimento da sociedade desde muito tempo e que apenas se moldaram a sua versão praticada em meio virtual, tendo em vista que já possuem tipificação pelo ordenamento jurídico penal, podendo ser praticados tanto no meio físico quanto no meio virtual. Para estes delitos, a legislação penal é suficiente, pois a maioria já encontra correspondência em algum tipo penal (CAETANO; MENEZES, 2015).

Para Colli (2010), os delitos virtuais impróprios são aqueles em que o computador é apenas o meio usado para a prática do crime, ou seja, o crime também poderia ser cometido sem o uso do computador. São tipos de crimes que já estão previstos no ordenamento jurídico, mas com o uso da internet para sua prática ganham novas roupagens e novas modalidades, dificultando inclusive a sua nova classificação em relação aos bens jurídicos tutelados. Em resumo, os crimes virtuais impróprios representam os ilícitos penais tradicionais, podendo ser cometidos em um novo formato e de novas maneiras.

De acordo com Dullius, Hippler e Franco:

Delitos Informáticos Impróprios podem ser compreendidos como aqueles nos quais o computador é usado, mas não acontece uma violação em algum bem penalmente tutelado, desde modo, para que se caracterize crime, não é necessário um conhecimento abrangente. Exemplos de crimes informáticos impróprios podem ser calúnia (art. 138 do CP Brasileiro), difamação (art. 139 do CP Brasileiro), injúria (art. 140 do CP Brasileiro), todos podendo ser cometidos, por exemplo, com o envio de um e-mail. (DULLIUS. HIPPLER. FRANCO, 2012, p. 8).

Alguns exemplos mais comuns de crimes virtuais impróprios são a ameaça, que é um crime contra a liberdade individual, a participação em suicídio, como no caso de incentivo ao suicídio pelas redes sociais, por exemplo; a incitação e apologia ao crime e ao criminoso, que também pode ocorrer no uso das redes sociais e que é notadamente comum, principalmente nos grandes centros urbanos; a falsidade ideológica ou falsa identidade, que geralmente ocorre por meio da criação de perfis falsos nas redes sociais, assim como a violação de direitos autorais e a pornografia infantil, que também são englobados nessa categoria.

Ressalte-se que até o ano de 2012 não existia no Brasil qualquer legislação específica sobre crimes virtuais, onde geralmente se utilizava a qualificação penal por analogia a outros tipos de penais. Essa realidade vem mudando com o surgimento de novos dispositivos legais e a criação de mecanismos para investigar os crimes dessa natureza, como é o caso da criação das delegacias especializadas e do desenvolvimento de equipamentos modernos, capazes de localizar e prevenir possíveis crimes virtuais, senão vejamos.

#### 1.4 - A LEGISLAÇÃO BRASILEIRA E OS CYBERCRIMES

De acordo Pinheiro (2013), considerando a necessidade da previsão legal para punição de uma conduta proibida e observados os princípios constitucionais da reserva legal e da legalidade, até o ano de 2012 não havia no Brasil qualquer legislação específica para punir os crimes virtuais próprios, ou aqueles voltados contra os sistemas de informação, ou mesmo os impróprios que apenas eram punidos de acordo com a sua qualificação correspondente no Código Penal, como furto, ameaça ou fraude.

Assim, em decorrência dessa lacuna legislativa e da ocorrência de alguns episódios de natureza grave, foram sancionadas em 30 de novembro de 2012 as leis n. 12.735, que trata da necessidade de criação e instalação de órgãos investigativos especializados e a lei n. 12.737, também conhecida como Lei Carolina Dickmann, através da qual foram incluídos no Código Penal o tipo penal de invasão de dispositivo informático (art. 154 – A) e a regra da ação penal para esse crime (art. 154 – B).

Numa breve análise sobre os novos tipos penais criados pelas citadas leis, Almeida e colaboradores, afirmam que:

O caput do art. 154-A do CP pode ser considerado o maior avanço proporcionado por essa norma. Isso porque, seu objetivo principal é realizar o combate às principais práticas danosas, conhecidas por trazerem transtornos para quem se utiliza ou necessita dessas tecnologias. De mais a mais, os novos artigos inseridos no Código Penal brasileiro pela Lei 12.737/2012 buscam combater a invasão de dispositivos informáticos alheios, conectados ou não à rede de computador. Importante salientar que se entende por dispositivos informáticos: computador de mesa, notebook, laptop, ultrabook, tablete, ipad, smartphone etc. (ALMEIDA. 2015).

Para Pinheiro (2013), o novo tipo penal indica ainda a necessidade do dispositivo de informática possuir algum tipo de segurança, sob pena de ser considerado desprotegido penalmente. Dessa forma, para cometer a conduta ilícita o sujeito ativo deverá invadir ou violar o parêntese alheio sem necessitar estar conectado com a rede de computadores e com o objetivo de obter, adulterar ou destruir dados e informações sem a devida autorização do seu proprietário.

Igualmente, na previsão trazida pelo §1º, que elenca como condutas do tipo normativo, produzir, oferecer, distribuir, vender ou difundir, constituem práticas que dependem das condutas típicas previstas no *caput* do artigo 154 – A, ou seja, para

cometer a conduta prevista no parágrafo, o sujeito deverá reunir todos os elementos objetivos e subjetivos do tipo (ALMEIDA et al., 2015).

Além disso, os §2º ao 5º do mesmo artigo, preveem também forma qualificadas em relação aos resultados, que serão configuradas se a invasão resultar na obtenção de conteúdo de comunicações eletrônicas privadas, como e-mails e mensagens trocadas por redes sociais ou segredos industriais e comerciais, hipóteses em que a pena será de reclusão de seis meses a dois anos combinada com multa. Entretanto, caso haja comercialização ou divulgação por terceiros, a pena poderá ser aumentada de um a dois terços (CAETANO; MENEZES, 2015).

Também se aumenta em um terço a pena se o crime for praticado contra o Presidente da República, Governante estadual ou municipal, Presidente do STF ou da câmara dos deputados ou do senado, da Assembleia Legislativa, o Presidente da câmara legislativa do Distrito Federal e também contra pessoas que possuam cargos máximos relativos a administração pública direta e indireta, independente da esfera.

Não se pode esquecer o art. 154 – B, que também foi acrescentado com a nova redação trazida pela Lei Carolina Dickmann. Este artigo é de suma importância por que traz à identificação da natureza da ação penal, dispondo como regra geral aplicável aos crimes virtuais, a ação penal pública condicionada a representação. Assim, a vítima deverá autorizar expressamente a autoridade policial a realizar as investigações concernentes ao crime e ao Ministério Público para iniciar a persecução penal. Entretanto, a ação será pública incondicionada, quando a conduta for praticada em desfavor da administração pública direta ou indireta em qualquer esfera. (CAETANO; MENEZES, 2015).

Por fim, deve-se destacar ainda que Lei também alterou a redação de dois delitos já existentes no art. 266 CP, com a interrupção ou perturbação de serviço telegráfico, telefônico, informático ou de informação de utilizada pública, bem como no art. 228, CP, que prevê a falsificação de documento particular, passando a equiparar cartão de crédito a esse tipo de documento (ALMEIDA et al., 2015).



## **CAPÍTULO II**

### **2. O CRIME DE LAVAGEM DE DINHEIRO**

A lavagem de dinheiro é um fenômeno de proporções mundiais, onde o processo de globalização, principalmente em relação as questões financeiras não respeita mais qualquer fronteira. As melhores ofertas de condições econômicas e de investimentos fazem com que elevadas quantias de dinheiro sejam movimentadas para outros países em frações de segundos. Entretanto, não é somente no mercado financeiro ou nas bolsas de valores que se busca multiplicar o dinheiro, há outros ramos legais e ilegais que também são observados por potenciais investidores (CALLEGAR; WEBER, 2014).

Este tipo de atividade não traz consequências apenas para a esfera econômica, mas possui reflexos na política econômica de comportamentos internos de cada país. Na verdade, a movimentação de grandes quantidades de dinheiro tem influência direta sobre a vida em sociedade, emperrando a função estatal de buscar o bem comum. Além disso, grande parte desses valores é movimentada por organizações criminosas, advindos de delitos como tráfico de entorpecentes, corrupção política e grandes roubos (BARROS, 2013).

A necessidade de movimentar grandes quantias em dinheiro faz com que as organizações criminosas ou os criminosos de maneira individual, tentem maquiagem a origem ilegal dessas quantias de alguma forma, sobretudo através da prática da lavagem de dinheiro, tema que será abordado em seus conceitos e evolução histórica no presente capítulo.

#### **2.1 - CONCEITOS E ASPECTOS HISTÓRICOS**

De acordo com Barros (2013), em termos históricos, a modalidade criminosa de lavagem de dinheiro surgiu na década de 1920, nos EUA, quando as organizações criminosas do país começaram a tentar disfarçar ou ocultar grandes quantias em dinheiro obtidas por meio de práticas ilícitas. Provavelmente na mesma época surgiu a expressão lavagem de dinheiro, que estaria ligado a uma rede de lavanderias e de lava jatos que teria sido montada para aparentar a procedência lícita do dinheiro obtido com atividades ilegais.

Também foi nessa mesma época que surgiu um dos mais lendários personagens do crime organizado da história – Alphonse Capone, também conhecido com Al Capone. O americano, descendente de italianos, assumiu o controle do crime organizado em Chicago no final da década de 1920. Sua fortuna teve origens basicamente na venda de bebidas ilegais e as suas ações alertaram para os outros criminosos da época sobre a necessidade de lavar o dinheiro sujo, mas sua “carreira” foi interrompida em 1931, quando foi preso (CALLEGARI; WEBER, 2014).

Segundo Aro:

Nos Estados Unidos, os motivos que levaram a criminalização da lavagem remontam ao final do século XX, quando as primeiras formas de organizações criminosas começaram a despontar no mundo, especialmente as máfias. Isso se deu principalmente durante o período de proibição em que vigorava a famosa “lei seca”. Tal lei, ao passo que proibia a fabricação e comercialização de bebidas alcoólicas, gerava um mercado ilegal de fornecimento destas que movimentava milhões de dólares através da exploração de diversas organizações criminosas. (ARO. 2013, p. 168)

Numa rápida analogia, fazendo uma comparação com a época atual, o processo chamado de “proibição” contribuiu significativamente para o desenvolvimento das organizações criminosas nos EUA, organizando o submundo do crime como nunca. Os negócios no mercado negro eram movimentados com grandes somas de dinheiro provenientes do contrabando e venda clandestina das bebidas alcoólicas. Esses valores serviam ainda para financiar a corrupção e outras atividades ilícitas.

Outro personagem importante nessa história foi Meyer Lansky, que para o autor é a figura central para os estudos sobre a lavagem de dinheiro. A ele é imputado a criação do primeiro sistema organizado de lavagem de dinheiro, parecido com os moldes conhecidos atualmente, sem contar com o advento da tecnologia. Entretanto, em relação às ferramentas oferecidas à sua época, pode-se dizer que Lansky realmente incorporou uma das primeiras técnicas de lavagem.

Nas palavras de Aro :

Com o crescimento da exploração dos jogos e tráficos de drogas, o uso de lavanderias e lava-jatos, baseados nas negociações em dinheiro vivo, já não era suficiente para circular o dinheiro ilícito. Então Meyer Lansky, em parceria com Salvatore Luciano, descobriu que a melhor maneira de ocultar ativos ilegais seria colocar o

dinheiro fora do alcance das autoridades do país, buscando uma jurisdição que não cooperasse com os Estados Unidos, para o confisco e restituição, e a Suíça foi um dos primeiros destinos escolhidos, o que deu origem a invenção do *offshore*. (ARO. 2013, p. 169).

Nos bancos suíços, o dinheiro de Lansky e companhia, de origem ilegal, poderia finalmente ser disfarçado por meio de empréstimos, concedido pelos bancos suíços e inclusive ser declarado ao fisco. Trata-se de uma das primeiras técnicas de lavagem de dinheiro, mas que é usada até os dias atuais. Por isso mesmo, em sua época, Lansky conseguiu superar praticamente todos os seus concorrentes, tanto pela sua astúcia, quanto pela forma de gerir as suas redes de relacionamento (RASMUSSEN, 2013).

De acordo com Braga (2013), atualmente a lavagem de dinheiro pode ser entendida como um fenômeno pelo qual uma ou mais pessoas, físicas ou jurídicas, tentam maquiagem ou ocultar a origem de bens, direitos e valores obtidos por meio de atividades ilícitas, através de operações financeiras e comerciais, buscando não atrair a ação repressora do Estado. Ou seja, a lavagem de dinheiro é um processo que visa dar uma origem aparentemente lícita para ativos obtidos por meio da prática de crimes.

É possível encontrar na literatura outras várias definições para o termo, mas a maioria delas tem como base a dissimulação da real origem dos ativos de maneira ilícita. A origem do termo “lavagem de dinheiro” está ligada a tradição anglo-saxônica que consagrou o uso da expressão *Money laundering*, embora nos Estados Unidos, por exemplo, seja usado o termo *laundering of monetary instruments* (RASMUSSEN, 2013).

Segundo Furtado (2011, p. 123):

A lavagem de dinheiro tem como finalidade principal apagar os rastros que possam escancarar a associação de uma determinada quantia de dinheiro (entendido, à luz da legislação brasileira, como bens, direitos ou valores) com a prática anterior de um crime. Destina-se, portanto, a tornar seguro o usufruto do proveito do delito anterior. Esse tipo específico de criminalidade se tornou um segmento de mercado, havendo profissionais especializados em prestar consultoria e auxílio logístico para a prática do branqueamento de capitais, como chamam os portugueses. (FURTADO. 2011, p. 123).

Ressalte-se que no caso brasileiro, o uso da expressão “lavagem” em substituição à expressão “branqueamento” se basicamente a dois motivos. O primeiro deles é pelo da expressão “lavagem de dinheiro” já estar consagrada pela linguagem popular e no vocabulário das operações e instituições financeiras do país, em função do amplo uso da expressão equivalente em inglês. O outro motivo, a expressão branqueamento, além de ter sido recém-inserida no glossário formal brasileiro, pode trazer uma conotação racial, o que motiva discussões (ANSELMO, 2013).

A lavagem de dinheiro é então um processo dinâmico composto ou uma sucessão lógica de transações financeiras e comerciais que objetiva dar aparência legal aos lucros obtidos de forma ilícita. Para disfarçar esses lucros e não comprometer as pessoas envolvidas, o processo é dividido basicamente em três fases, quais sejam o distanciamento dos fundos de sua origem, o disfarce das movimentações e a disponibilização do dinheiro novamente depois de ter sido suficientemente movimento (FURTADO, 2011), conforme descrito a seguir.

## 2.2 - AS FASES DA LAVAGEM DE DINHEIRO

De acordo com Mendroni (2015) a nomenclatura das fases do processo de lavagem de dinheiro não é pacífica na literatura, entretanto a quantidade de fase sim, ou seja, são três fases. Alguns as chamam de ocultação, mascaramento e integração, enquanto outros as chamam de conversão, dissimulação e integração. Há ainda os que as chamam de colocação, ocultação e integração, nomenclaturas que adotadas no presente estudo.

Em relação a primeira fase, ou seja, a fase de colocação, consiste na fase em que os recursos financeiros de origem ilícita são introduzidos no mercado financeiro e no sistema econômico. De maneira astuciosa, o dinheiro em espécie é movimentado através de depósitos ou compra de bens negociáveis, buscando ocultar a sua procedência. É nesta fase que as organizações criminosas procuram se livrar rapidamente das vultosas somas de dinheiro geradas pelas suas atividades ilícitas, como tráfico de armas e drogas, por exemplo. (BARDARÓ; BOTINI, 2017).

Nas palavras de Furtado :

A primeira fase é a da colocação (placement), conversão ou ocultação. Nela, o criminoso promove o distanciamento físico entre o crime anterior (tráfico de drogas, por exemplo) e o produto deste (inúmeras cédulas de baixo valor). Como o manuseio e a guarda de grande quantidade de dinheiro em espécie é difícil e arriscado, é necessário que seja colocado no circuito oficial. Assim, esse distanciamento pode ser feito de inúmeras maneiras como, exemplificando, a compra em dinheiro de um imóvel ou obra de arte e sua venda, introduzindo-se nesse ponto os valores em instituições bancárias e financeiras. (FURTADO. 2011, P. 128)

Segundo Aro (2013), em geral, os valores em dinheiro são introduzidos no sistema financeiro em pequenas quantias, que individualmente não geram quaisquer suspeitas. A essa técnica é dado o nome de *smurfing*. Para o autor, é exatamente por isso que existe uma preocupação dos órgãos de fiscalização em relação aos registros das instituições financeiras. O Banco Central dos EUA, por exemplo, há muitos anos se preocupa em identificar o cliente de uma forma que ele não perceba que está sendo identificado.

Outra técnica de lavagem de dinheiro empregada nessa fase é a utilização de estabelecimentos comerciais que trabalham com o dinheiro em espécie, como restaurantes, hotéis e parques, dentre outros. Ainda pode ser usada a figura do laranja ou do cabodólar, que consiste em uma rede de transferência paralela ao sistema financeiro oficial, onde doleiros e casas de câmbio atuam como intermediários e realizam a transferência de valores de um país para outro sem qualquer tipo de tributação (FURTADO, 2011).

De acordo com Aro:

Nota-se, assim, que a lavagem de dinheiro tanto pode ser mediante a utilização do sistema financeiro, quanto mediante a utilização de outros meios, como mercado imobiliário, estabelecimentos comerciais, jogos legais e ilegais. É na oportunidade da colocação que se exige maior intervenção do Estado, por que o limite temporal entre a prática do crime original e o início da lavagem de dinheiro é muito estreito. (ARO. 2013, P. 172).

Em relação à segunda fase da lavagem de dinheiro, esta é definida como a fase de ocultação ou dissimulação. Essa fase consiste no disfarce ou eliminação dos rastros que o dinheiro sujo eventualmente possa deixar. A prática consiste em dificultar o rastreamento contábil dos recursos ilícitos. Nesta fase, as organizações criminosas se concentram na quebra de evidências, caso haja alguma investigação

sobre a origem de dos valores. Preferencialmente, buscam movimentar os valores por contas de aluguel, ligadas a laranjas ou pessoas fantasmas (ANSELMO, 2013).

De acordo com Rasmussen (2013), o objetivo nessa fase é separar os recursos de suas origens, através de um sistema complexo de transações financeiras, destinado a apagar os dados contábeis das transações realizadas com dinheiro sujo. É uma etapa complexa, talvez a mais difícil de operar, exigindo o auxílio de pessoas especializadas, com conhecimentos econômicos, financeiros e tributários e ainda afinidade com a legislação de vários países.

Na fase de ocultação, as evidências das transações financeiras realizadas são camufladas, com uma série de negócios e operações financeiras, a fim de dificultar ou impossibilitar qualquer rastreamento contábil dos lucros ilícitos. Pode-se dizer que a fase onde ocorre a lavagem de dinheiro propriamente dita, tendo em vista que se dissimula a origem dos valores para que a sua procedência não seja identificada.

As transações realizadas anteriormente são multiplicadas, com vários tipos de transferências e criação de empresas e contas correntes para simular uma atividade lícita. É realizado o saque do dinheiro em espécie e seu depósito é realizado em uma nova instituição. Hoje em dia a realidade é ainda mais complexa, tendo em vista os recursos tecnológicos e as operações financeiras internacionais, que facilitam a manipulação de dados e viabilizam a ocorrência da prática da lavagem de dinheiro (ANSELMO, 2013).

Segundo Aro:

Um dos métodos de ocultação mais avançados é a venda fictícia de ações na bolsa de valores (o vendedor e o comprador, previamente ajustados, fixam um preço artificial para as ações de compra). É comum nesta fase também a transformação das quantias em bens imóveis ou móveis; quanto a esses, costuma-se adquirir bens que possam ser postos em circulação rápida em diferentes países como ouro, joias e pedras preciosas. (ARO. 2013, P. 173).

Por fim, a terceira fase do processo de lavagem de dinheiro é a chamada integração. De acordo com Furtado (2011), essa é a etapa final da lavagem de dinheiro, onde ocultada a origem do dinheiro sujo, o capital retorna para as mãos dos criminosos, dessa vez formalmente incorporados ao sistema econômico. Assim, as organizações criminosas podem investir o dinheiro, aparentemente de origem

lícita em outros empreendimentos que facilitem as suas atividades, podendo até prestarem serviços entre si.

Entre as práticas mais realizadas nessa fase encontram-se o empréstimo de regresso, a falsa especulação imobiliária, a falsa especulação em obras de arte ou pedras preciosas, dentre outras. O empréstimo de regresso é a simulação de empréstimos com dinheiro que já pertence ao lavador de empresas localizadas em território nacional ou internacional, com os mesmos proprietários. Já a falsa especulação utiliza-se tanto de obras de arte como de pedras preciosas, simulando valores superiores aos reais (ARO, 2013).

De acordo com Rasmussen:

Na última fase, a organização procura investir em negócios que gerem a continuação de suas atividades delituosas, como, por exemplo, Setores Econômicos que fazem a movimentação de enormes quantias de dinheiro em espécie, com a finalidade de confundir com o dinheiro de origem criminosa, como, por exemplo, lojas de revenda de carros novos ou seminovos, postos de gasolina, hotéis, etc., há também, o investimento em Agências de Transporte que são destinadas ao itinerário de dinheiro, drogas, produtos químicos (empregados na preparação de entorpecentes) ou diversos bens de contrabando, ou ainda, Empresas de Viagem, que possuem a finalidade de comercializar diversos produtos contrabandeados. (Rasmussen, 2013, p. 7)

Na verdade, em termos técnicos não se pode dizer que há lavagem de dinheiro nessa fase, tendo em vista que o dinheiro já possui uma máscara de licitude. Entretanto, cabe ressaltar que nem sempre a lavagem de dinheiro precisa passar necessariamente pelas três fases, bastando a fase de colocação, conforme posicionamento recente firmado pelo Supremo Tribunal Federal (FURTADO, 2011). Além disso, é notório o fato de que todos os dias surgem novas modalidades de lavagem de dinheiro, inclusive pelos meios virtuais, conforme será demonstrado no presente estudo.

### 2.3 - PRINCIPAIS TIPOLOGIAS

Para proceder com a lavagem de dinheiro exige-se o conhecimento prévio sobre o sistema financeiro. Portanto, nesse tópico, busca-se informar os nomes e fazer uma breve explanação sobre algumas técnicas empregadas para a lavagem de dinheiro, sem esgotar a matéria.

A primeira tipologia que se pode citar, diz respeito à compra de ativos e instrumentos monetários. De acordo com Barros (2013), nessa modalidade específica, o criminoso ou a organização criminosa se utilizam de grandes quantidades de dinheiro em espécie, com origem relacionada à prática de atividades ilícitas para adquirir bens como carros, motos, barcos, aeronaves, apartamentos, metais preciosos ou ações na bolsa de valores. Geralmente o vendedor sabe das conexões ilegais do seu cliente ou mesmo trabalha para a organização criminosa.

Já o contrabando de moedas é uma técnica que envolve o envio de grandes quantias em espécie para o exterior. Funciona da seguinte forma: O dinheiro de origem ilícita é colocado em bolsas ou compartimentos secretos no meio de transporte utilizado, que geralmente traz algumas limitações, como o tamanho do carro, na tentativa de evitar qualquer tipo de suspeita. O sucesso dessa modalidade traz grandes vantagens para as organizações criminosas em razão da dificuldade da polícia ou órgãos fiscalizadores em conseguir vincular o dinheiro à determinada origem (VIVIANI, 2005).

Outro tipo comum de lavagem de dinheiro ocorre através da compra de prêmios de loterias. A organização criminosa, por meio de seus informantes, consegue localizar eventuais ganhadores de prêmios milionários na loteria e oferecem um valor maior pelo bilhete premiado. Como a proposta é boa, o ganhador vende o bilhete premiado e um representante da organização criminosa se diz o verdadeiro vencedor, de maneira que aquele dinheiro agora ganha ares lícitos. Nas palavras de Mamede (2014, p. 25), nesse tipo ação:

A organização criminosa utiliza o dinheiro proveniente das suas atividades ilícitas para “comprar” os prêmios de loterias dos beneficiários iniciais, por um valor superior ao que os beneficiários receberiam da entidade responsável pelo sorteio. A organização criminosa efetua o pagamento ao beneficiário inicial utilizando-se de recursos ilícitos, e posteriormente recebe da entidade responsável pelo sorteio o pagamento do prêmio (origem lícita), justificando o aumento de seu patrimônio. (MAMEDE. 2014, P. 25).

A transferência eletrônica de fundos também é uma prática bastante utilizada para lavar dinheiro no Brasil e no mundo. De acordo com Barros (2013), trata-se da utilização da rede eletrônica bancária para a transferência de recursos para dentro ou fora do país. Para o autor, é uma das técnicas mais importantes para as organizações criminosas, tanto em relação ao volume de dinheiro, quanto em



relação a quantidade de transações, por que é possível transferir elevadas quantidades em um curto período de tempo.

Outro meio comumente utilizado pelas organizações criminosas que detém a propriedade sobre empresas em geral, que ocorre através da criação de faturas falsas de importação e exportação. A técnica consiste basicamente em aumentar o valor da importação ou exportação, onde a diferença paga ou recebida a mais acoberta o dinheiro sujo. Se o valor de uma importação for superestimado em uma fatura, por exemplo, quando ela for paga, a diferença acima do valor real dos bens poderá ser compensada com recursos de origem lícita.

Mamede (2014, p. 25), cita um exemplo:

Uma empresa brasileira oferece a prestação de serviço exportável e celebra um contrato fictício com um cúmplice (que pode ser uma pessoa física ou jurídica) localizado no exterior. A empresa simula a exportação do serviço cumprindo os requisitos formais e legais exigidos para a atividade. O suposto contratante do serviço no exterior ordena o pagamento do serviço por meio de intermediários contratados. Em geral são exportações de serviços cuja prestação ou valor comercial no mercado internacional é de difícil verificação ou quantificação devido a seu caráter intangível, como por exemplo, serviços de computação, serviços de arquitetura e engenharia etc. (MAMEDE. 2014, p. 25).

A criação de empresas de fachada ou empresas fictícias são outras modalidades comuns de lavagem de dinheiro. A empresa de fachada é uma organização legalmente ativa, que aparenta desenvolver um negócio de natureza lícita, mas que serve de escudo para a realização de operações fraudulentas, como a lavagem de dinheiro. Já a empresa fictícia só existe no papel, ou seja, não participa do mercado financeiro. Seu objetivo geralmente é mascarar a movimentação do dinheiro sujo (VIVIANI, 2005).

Mamede (2014) cita ainda as vendas fraudulentas de propriedades imobiliárias, que consistem na compra de determinada propriedade imóvel com dinheiro sujo, declarando um valor de mercado inferior ao real, onde a diferença é paga ao vendedor, em espécie. Depois, o imóvel será negociado pelo valor real, fazendo com que o lucro obtido de maneira criminosa seja justificado como ganho de capital. Antes de serem revendidos, os imóveis são utilizados para festas de luxo e ostentação de poder.

Também é possível citar a figura do “laranja”. O “laranja” é aquele intermediário que efetua as transações financeiras e comerciais em seu nome, ocultando a identidade do verdadeiro beneficiário das transações. Em muitos casos esse intermediário tem total ciência do que está fazendo, inclusive recebendo contraprestações para tal. Em outros casos são usados os nomes de pessoas idôneas, leigas, as vezes sequer alfabetizadas.

Segundo Mamede (2014, p. 27) cita outro exemplo:

Uma empresa brasileira oferece a prestação de serviço exportável e celebra um contrato fictício com um cúmplice (que pode ser uma pessoa física ou jurídica) localizado no exterior. A empresa simula a exportação do serviço cumprindo os requisitos formais e legais exigidos para a atividade. O suposto contratante do serviço no exterior ordena o pagamento do serviço por meio de intermediários contratados. Em geral são exportações de serviços cuja prestação ou valor comercial no mercado internacional é de difícil verificação ou quantificação devido a seu caráter intangível, como por exemplo, serviços de computação, serviços de arquitetura e engenharia etc. (MAMEDE. 2014, p. 27)

Por fim, é possível citar ainda a cumplicidade de agentes internos. De acordo com Barros (2013), alguns funcionários de instituições financeiras ou empresariais são atraídos pelas organizações criminosas em troca de dinheiro e facilitam as transações realizadas com o dinheiro sujo. Em linhas gerais, o funcionário corrupto executa operações não permitidas pela instituição, ou deixa de cumprir determinados procedimentos de segurança, facilitando a vida do lavador.

#### 2.4 - A LEGISLAÇÃO BRASILEIRA

No ano de 1998, o governo brasileiro apresentou a sociedade a sua Lei de combate e prevenção à lavagem de dinheiro, qual seja a Lei n. 9.613/98. Entretanto, ao longo dos anos as autoridades, polícias e órgãos fiscalizadores passaram a encontrar dificuldades para fazer o bom uso de seus dispositivos, de maneira que o citado dispositivo legal conseguisse atingir os seus objetivos, prevenindo a ocorrência de lavagem de dinheiro no país (BADARÓ; BOTINI, 2017).

De acordo com Furtado:

A lavagem de dinheiro é uma atividade danosa à tranquilidade socioeconômica, necessitando, portanto, da reprimenda estatal. Para lograr êxito, o Estado brasileiro deve, ao lado da participação em foro

de cooperação internacional, fortalecer a estrutura de combate interna, em especial por meio de uma legislação flexível e eficaz. Quanto ao aspecto legislativo, o Brasil, ao lado de Grécia e Portugal, e diferentemente da grande maioria dos países europeus, incluiu o tipo penal da lavagem de dinheiro em uma lei específica, Lei Federal nº 9.613/1998, - que se tornou, assim, a lei de regência da matéria - e não no próprio Código Penal. (FURTADO. 2011, P. 129).

De fato, o objetivo da Lei n. 9613/98 era de criminalizar a lavagem de dinheiro, tendo em vista que o Brasil é signatário da Convenção de Viena. Por ser signatário de tal documento, naquele momento, o país optou por construir uma lei de segunda geração, cuja classificação tem como pressuposto os crimes que são considerados como antecedentes (BARDARÓ; BOTINI, 2017).

Dessa forma, o Estado que optar pela criação de uma lei de lavagem de dinheiro de primeira geração limita as suas origens apenas ao tráfico de drogas. Na verdade, as organizações evoluíram e passaram a buscar recursos em vários outros tipos de atividades criminosas. Por isso, a legislação também evoluir e passara a considerar as outras modalidades de lavagem de dinheiro. Nesse sentido, os países juridicamente mais desenvolvidos, relacionam o crime de lavagem de dinheiro a qualquer delito que estimulasse a legalização do dinheiro sujo.

No mês de julho do ano de 2012, foi promulgada a Lei n. 12.683, que alterou e atualizou a lei anterior, trazendo maior eficiência a persecução penal em relação ao crime de lavagem de dinheiro. Além disso, com a promulgação da Lei n. 12.850 de 02 de agosto de 2013, que define organização criminosa, a lei de lavagem de dinheiro ganhou mais respaldo, por que agora não haveria mais lacunas em relação à representação legal de organização criminosa no ordenamento jurídico brasileiro, o que, diga-se de passagem, ocorreu de forma tardia (BARDARÓ; BOTINI, 2017).

Dentre as mudanças mais relevantes do texto em relação à Lei n. 9.613/98, encontra-se a possibilidade de ocorrência de dolo eventual, ou seja, nos casos em que o agente utilize bens ou valores provenientes da atividade ilegal, da qual teria obrigação de conhecer a origem, também estará cometendo o crime de lavagem de dinheiro. Além disso, foi excluído o rol taxativo de crimes que poderiam preceder a lavagem de dinheiro. Dessa forma, qualquer infração penal que gere rendimento cuja natureza localização, movimentação ou propriedade são ocultas, poderá caracterizar lavagem de dinheiro (CALLEGARI; WEBER, 2014).

Ambas as alterações citadas são consideradas benéficas para a sociedade e para o sistema financeiro nacional, tornando a prevenção e persecução penais mais efetivas. Entretanto, há um ponto que ainda gera controvérsias. Trata-se do art. 17 – B, que afeta principalmente os envolvidos com comércio eletrônico e provedores de dados. O artigo dispõe que a autoridade policial e o MP poderão ter acesso aos dados cadastrais dos clientes investigados, mantidas por provedores de internet, empresas telefônicas e administradores de cartões de crédito independente de autorização judicial para tal.

Na opinião de Aro:

Esse dispositivo fere inofismavelmente os direitos fundamentais previstos na Constituição Federal, como devido processo legal e direito à privacidade. Dessa forma, os consumidores que partilham seus dados em essas empresas podem se sentir lesados ao terem seus dados fornecidos para a autoridade pública sem uma decisão anterior que a autorize. Com isso, poderia haver compartilhamento de informações desnecessárias ou de usuários inocentes, equívocos seriam cobrados judicialmente às empresas envolvidas e ao próprio Estado. (ARO. 2013, p. 175)

Além disso, alguns dos dados listados no art. 17 – B da referida lei, não são informações exigidas para o cadastro usual das empresas, tais como filiação. Dessa forma, não haveria como as empresas fornecerem essa informação. A classificação de provedores de internet também é muito vaga, sendo que muitos *players* da economia digital não possuem muitos dados de seus clientes, e poderiam ser prejudicados na busca por elas, se lhes fosse exigida tal obrigação (ARO, 2013).

É claro que a elaboração de novos mecanismos, políticas públicas e leis para prevenção e combate à lavagem de dinheiro é estritamente necessária, mas deve-se ponderar as exigências feitas à terceiros para a colaboração na elucidação de tais crimes. Com o advento da Lei n. 12.683/12, esse balanceamento não ocorreu de forma correta, entretanto, a lei trouxe saldos positivos.

O problema é que como citado anteriormente, as organizações criminosas têm se especializado ainda mais na lavagem de dinheiro, trazendo lacunas legais, principalmente em relação à lavagem de dinheiro praticada por meio virtual, conforme será descrito no capítulo adiante.

## CAPÍTULO III

### 3. OS CRIMES VIRTUAIS E AS NOVAS MODALIDADES DE LAVAGEM DE DINHEIRO

De acordo com Andrade (2017) a popularidade do uso das moedas virtuais, no Brasil, tem um grande potencial para alavancar a economia e o mercado financeiro nacional, ajudando o país a acompanhar o desenvolvimento e novidades do setor a nível mundial. Entretanto, esse tipo de serviço também cria um grande desafio para as autoridades que atuam no combate ao crime de lavagem de dinheiro. A complexidade dos sistemas que utilizam as moedas virtuais e a proteção usada para garantir a isonomia das transações pode servir de ferramenta para lavar dinheiro ou ocultar o patrimônio das autoridades públicas.

Atualmente a moeda virtual mais utilizada em todo o mundo é o *bitcoin*, que já atingiu a marca de um milhão de adeptos no Brasil. No início do mês de fevereiro de 2018 a Polícia Federal conseguiu realizar a prisão inédita de uma organização criminosa que utilizava a moeda virtual para fazer o envio de dinheiro ilegal para o exterior. Em um desdobramento da famosa operação lava jato, as autoridades descobriram que a quadrilha fraudava licitações para fornecimento de merenda escolar e já havia enviado mais de R\$ 300 mil ao exterior utilizando os *bitcoins*.

Outra ferramenta que vem sendo constantemente utilizada pelas organizações criminosas para a lavagem de dinheiro é a chamada *Deep web*. Além da internet comum, em que é possível acessar as redes sociais e sites de notícias ou mesmo fazer compras, existe uma camada mais profunda, um mercado negro que somente é acessível por meio de endereços direcionais. Por lá também ocorrem transações com moedas virtuais, além do tráfico de drogas, armas e lavagem de dinheiro advinda dessas atividades (MARTINS; BRAGA, 2016).

Mesmo possuindo um espaço de armazenamento de informações menor que a internet comum a chamada *Deep web* já reúne milhões de usuários no Brasil. A Polícia Federal já conseguiu identificar operações de lavagem de dinheiro utilizando-se desse mecanismo, mas não conseguiu identificar os agentes por causa da barreira do anonimato e da impossibilidade de acessar os dados dessas pessoas. Assim, a lavagem de dinheiro continua ocorrendo sem maiores problemas.

Visando contextualizar essas novas ferramentas e analisar o seu uso voltado para a lavagem de dinheiro, esse capítulo trará uma abordagem conceitual para

ambas, além de tratar da legislação pertinente, ou da ausência dela, e dos mecanismos de prevenção e repressão à nova modalidade de lavagem de dinheiro através do meio virtual.

### 3.1 - AS CRIPTOMOEDAS COMO INSTRUMENTO DE LAVAGEM DE DINHEIRO

Antes de iniciar a discussão sobre como o *bitcoin* é utilizado para a lavagem de dinheiro, é necessário explicar o que é, como é criada e como funciona a moeda virtual. O *bitcoin* foi criado no ano de 2008 por uma pessoa ou grupo cuja a identidade ainda é desconhecida, apesar de algumas pessoas já terem publicamente reivindicado a autoria. Encontra-se dentro da teoria de criptomoedas, tendo o prefixo “cripto” (*Kryptos*) de origem grega e que significa oculto, escondido. Na realidade, a criptomoeda é uma moeda constituída por códigos digitais (LIMA; SANTANA, 2016).

De acordo com Silva e Pereira:

O *Bitcoin* é uma moeda, como dólar, real, libra, porém na forma digital, que possui código aberto e independe de uma autoridade central e sua descentralização do sistema de pagamentos é o que mais se destaca e difere das outras. Trata-se do primeiro sistema de pagamentos global que é completamente descentralizado. Essa moeda foi criada em 2008 por uma pessoa que usa o pseudônimo de Satoshi Nakamoto, porém nunca foi identificado. A moeda fica armazenada em carteiras digitais, controladas por sites, mas também pode ser guardada em computadores, pen drives e outros dispositivos de armazenamento. (SILVA; PEREIRA. 2016, P.2).

A mineração de *bitcoins* é realizada através do uso de *hardwares* e *softwares* especializados, tendo em vista que as operações matemáticas necessárias para a criação das moedas são baseadas em números primos, como por exemplo 2, 3 e 5. Entretanto, após certo tempo, os números primos não são tão intuitivos, surgindo a necessidade de usar programas especializados para realizar seu cálculo e mineração. O gasto energético é tão alto para a sua criação, que no Brasil se tornou inviável, dado os preços pagos pela energia elétrica no país (ANDRADE, 2017).

Segundo Silva e Pereira (2016), essa maneira de funcionar é o principal motivo que permite que a moeda seja utilizada para fins de lavagem de dinheiro. Na realidade, não existe qualquer controle para a criação de *bitcoins* e qualquer pessoa com conhecimentos suficientes pode produzi-los, o que torna a moeda

descentralizada, sem vinculação ao Estado ao Banco Central. As informações sobre quem possui esse tipo de moeda e em qual quantidade ainda são uma interrogação para os governos, dificultando o controle estatal e facilitando as práticas criminosas.

Além de ser uma moeda descentralizada, o *bitcoin* e as suas transações realizadas *peer to peer* ou seja, de pessoa para pessoa, elimina qualquer intermediário. Não existe uma instituição financeira regulando as transações envolvendo esse tipo de moeda, por que estas ocorrem exclusivamente entre os indivíduos que estão comprando, ou vendendo. Também não existem taxas bancárias para realizar as transações, havendo apenas uma taxa de rede. Os *bitcoins* também podem ser adquiridos por intermédio de corretoras, semelhante as corretores que negociam ações (ANDRADE, 2017).

Ressalte-se que no mundo digital o fluxo e a segurança das informações são fatores essenciais para o sucesso das transações. Para isso, o sistema de *bitcoins* se utiliza do sistema da *blockchain*. Trata-se de uma cadeia de blocos, em tradução livre, que serve como um registro digital público e que é compartilhado entre os computadores. Os dados gravados se constituem em gravações imutáveis, ou seja, é praticamente impossível apagar o registro digital das transações feitas anteriormente (LIMA; SANTANA, 2018).

A volatilidade também é uma das características marcantes do *bitcoin*, responsável pela concentração cada vez maior de investidores que se utilizam dessa moeda, que tem um alto grau de variação em seus preços. Em Janeiro de 2017, por exemplo, o valor da moeda era de aproximadamente U\$ 1.000,00 (mil dólares), alcançando em novembro do mesmo, onze vezes esse valor, o que demonstra o imenso nível de variação possível, sendo a moeda predominantemente deflacionária, ou seja, a tendência é que seu valor aumente.

Nas palavras de Lima e Santana:

O caráter extremamente volátil do bitcoin, desse modo, é algo notório, gerando debates se seria possível ter uma moeda com tal aspecto. A volatilidade é, como pode ser compreendido, consequência da descentralização da moeda, já que não há um banco central para regular o valor da moeda e garantir sua constância. Além disso, outros fatores, como a lei da oferta e demanda, colaboram para o caráter deflacionário da moeda. A descentralização e volatilidade serão os dois principais atributos para que o bitcoin seja, nos dias de hoje, uma ferramenta excelente para a realização da lavagem de capitais, como posteriormente será visto. (LIMA; SANTANA, 2018, P. 12).

Em relação à lavagem de dinheiro, viu-se a a modalidade é dividida basicamente em três etapas que são a olocação, a estratificação e a integração do capital à economia. Ressalte-se que o objetivo dessa divisão em etapas é apenas auxiliar a compreensão do processo, tendo em vista que elas podem não ocorrer em momentos distintos e podem aparecer superpostas. Em relação ao uso do *bitcoin* para a lavagem de dinheiro as três fases também são notórias, havendo algumas peculiaridades quando comparado aos mecanismos tradicionais de lavagem de dinheiro (SILVA; PEREIRA, 2016).

Conforme citado anteriormente, a colocação é fase em que o agente busca inserir o dinheiro proveniente de atividades ilícitas no mercado financeiro, o que geralmente ocorre através de depósitos em bancos, com a utilização do nome de laranjas, e por meio do fracionamento do dinheiro em quantias menores, na tentativa de evitar qualquer suspeita a respeito da movimentação.

De acordo com Andrade (2017), no caso ods *bitcoins*, ao invés de fazer uso de instituições bancárias comuns, as organizações criminosas compram quantidades da criptomoeda. Evidentemente, a organização crimnosa ou o criminoso não comprará toda a quantidade de *bitcoins* que pretende adquirir apenas com uma carteira, tendo em vista que a ideia é realizar operações que não levantem qualquer suspeita.

Note-se que no caso das criptomoedas, além de não ser necessário um banco, o criminoso não precisa fazer uso de laranjas, mas apenas de IP's ou computadores diferentes para a aquisição de difeirentes carteiras.

No segundo momento, ocorre a fase de ocultação, isto é, a criação de múltiplas camadas de transações que distanciam o dinheiro de sua origem inicial. No caso dos *bitcoins*, por não serem utilizadas operações bancárias, faz-se o suo de *mixers*, ou seja, misturadores que são serviços que se utiliza para misturar os fundos de uma pessoa com os de outra. Esta mistura ocorre quando o usuário envia seu dinheiro para um serviço anônimo que logo responderá e enviará a mesma quantia, composta por criptomoedas que pertenciam a outros usuários (SILVA;PEREIRA, 2016).

Já a utlima fase, que é a de integração, integra-se o dinheiro ao emrcado financeiro, sendo extremamente difícil provar que aquele montante de moedas está



ligado à prática de crimes, tendo em vista que por meio da utilização dos *mixers*, a história das transações se torna uma nuvem de nebulosidade.

Lima e Santana (2017, p. 15), trazem um excelente exemplo de como funcionam as fases da lavagem de dinheiro através do uso de *bitcoins*, senão vejamos:

João, traficante de drogas, possui um montante de R\$ 100.000,00 obtidos legalmente por meio da venda de um apartamento, tendo, além desse valor, a quantia de mais R\$ 100.000,00 provenientes de sua atividade ilícita. Para esconder a ilicitude do dinheiro oriundo do mercado das drogas, João compra R\$ 200.000,00 em bitcoins, usando o fato de que o valor da moeda no momento da compra era de R\$ 2.000,00 e no mês anterior era de R\$ 1.000,00, fazendo com que o criminoso possa alegar que a quantia proveniente do tráfico é, em realidade, oriunda de seu investimento, feito um mês antes. Todavia, caso João simplesmente compre bitcoins, ao realizar a sua declaração de imposto de renda, poderia constatar-se, por meio dos dados públicos da blockchain, que o momento real de sua compra foi no mês em que a moeda já estava no valor de R\$ 2.000,00 e, destarte, não teria gerado o afirmado lucro. Para mascarar o momento de sua compra, o traficante utiliza o serviço mixer, tornando-se, destarte, extremamente difícil para o Estado alegar o real momento de sua compra, já que tal data foi ocultada por inúmeras transações entre diversas pessoas. (LIMA; SANTANA. 2017, p. 15)

Com base no exemplo trazido pelos autores, fica devidamente claro que a volatilidade do *bitcoin* foi utilizada para esconder a origem ilícita do do capital proveniente do tráfico de drogas, bem como a descentralização da moeda dificultou o controle do Estado em relação às transações realizadas e a identificação do envolvidos, tendo-se o uso do *mixer*, tornando ocultas e escassas as informações que podem ser obtidas sobre as transações realizadas.

### 3.2 A LAVAGEM DE DINHEIRO ORIUNDA DO TRÁFICO DE DROGAS E ARMAS NA *DEEP WEB*

O termo *deep web*, que em tradução simples significa “web profunda”, se tornou o termo geral utilizado para se referir a determinado conjunto de sites e servidores de internet. Originalmente o termo era utilizado para se referir aos sites invisíveis, ou páginas que por quaisquer motivos não apareciam nos sites de busca comuns. Eram páginas que para serem localizadas, necessitavam do uso de

diversos mecanismos de busca em conjunto, além de ferramentas adicionais (SILVA; PEREIRA, 2016).

O termo acabou se popularizando e ganhou uma definição mais compacta para se referir ao acesso à sites que necessitam do uso de programas ou ferramentas específicas para poderem ser acessados. O mais popular atualmente entre todos eles é o Tor, mas existem outros softwares que também são empregados com frequência. O emprego do termo *deep web* seria incorreto nesse contexto, e o emprego correto seria *dark web*.

De acordo com Almeida e Roque:

O espaço virtual em sua estrutura completa é análogo a imagem de um iceberg. A parte visível deste é denominada de Surface Web enquanto sua parte imersa simboliza a Deep Web, representando diversos aspectos que diferenciam o ciberespaço. Um exemplo dessa discrepância se dá nos navegadores específicos usados para ambos. Softwares conhecidos como o Google Chrome e o Firefox, enquanto específicos da Surface Web, não conseguem captar o conteúdo da Deep Web em que são utilizados navegadores como o TOR. (ALMEIDA; ROQUE. 2017, P. 166).

Apesar das autoridades ainda afirmarem que a *deep web* possui uma capacidade menor de armazenamento de informações em comparação à internet comum, alguns autores pesquisados afirmam que na verdade ela já é 500 vezes maior e com a média de três vezes mais qualidade de funcionamento. O total de número de sites na *deep web* provavelmente excede hoje os 220.000 e continua crescendo em ritmo assustador. Ressalte-se que mais de 90% das informações da *deep web* são acessíveis sem qualquer restrição, mas 10% delas são praticamente inacessíveis, como os dados dos usuários (ALMEIDA; ROQUE, 2017).

Nesse sentido, os crimes virtuais, incluindo a lavagem de dinheiro, chegaram ao seu grau máximo de complexidade perante o direito virtual em relação ao uso da *deep web*, por que não deixam sequer rastros da atuação criminosa. Dessa forma, os criminosos virtuais se aproveitam da fragilidade da legislação, da ausência de fronteiras e fiscalização do uso da tecnologia para manterem suas atividades delituosas tornando-lhes cada vez mais lucrativas e menos suscetíveis ao fracasso (ANDRADE, 2017).

De acordo com Martins e Braga (2016), não há sequer como falar em ocultação de fundo ilícitos, que seria a primeira fase da lavagem de dinheiro, quando

a moeda corrente que materializa esses fundos, que é o caso dos *bitcoins* na *deep web*, não integra o sistema monetário oficial, estando portanto, necessariamente oculta da fiscalização do sistema financeiro desde a sua origem até a sua destinação final.

Suponha-se por exemplo que um traficante de drogas expõe a sua “mercadoria” à venda em um mercado virtual da *deep web*. Ao obter *bitcoins* com a venda da droga e depois converter a moeda em dinheiro em espécie, perante a legislação brasileira, o mesmo não poderia ser acusado de lavagem de dinheiro, tendo em vista que nada ocultou ou dissimulou. Abre-se então uma lacuna importante, em relação à inserção desse dinheiro na economia formal, o que pode ocorrer se esse dinheiro for usado para a compra de um carro, por exemplo (MARTINS; BRAGA, 2016).

Esse panorama é ainda mais preocupante diante do fato de que recentemente uma empresa norteamericana desenvolveu caixas eletrônicas que possibilitam, mediante a leitura de dispositivo eletrônico de cada usuário, o saque em dinheiro em espécie a partir da conversão de seus *bitcoins* em qualquer lugar do mundo onde o caixa esteja instalado. A tecnologia já está presente nas principais cidades dos EUA e da Europa, facilitando a vida dos usuários e dificultando ainda mais o trabalho das autoridades em relação à eminente possibilidade de lavagem de dinheiro através dessa prática (LIMA; SANTANA, 2018).

Segundo Martins e Barga:

A preocupação em torno da matéria já assola as autoridades norte-americanas. Relatório da Seção de Inteligência do FBI revela que a rede bitcoin disponibiliza aos indivíduos campo fértil para a produção, transferência, lavagem e até mesmo subtração de recursos financeiros de forma anônima; sua natureza descentralizada agrega dificuldades adicionais para os investigadores em relação às demais moedas virtuais, asseverando que os *bitcoins* já vem sendo aceitos como forma de pagamento por criminosos, os quais utilizam-se de sistemas de pagamentos virtuais para compra e venda de bens e serviços e lavagem de dinheiro. Ainda de acordo com o FBI, *bitcoins* continuarão atraindo criminosos cibernéticos que vem na moeda digital uma forma de subtrair ou movimentar fundos de forma anônima, ou mesmo fazer doações a grupos dedicados a atividades ilícitas. (MARTINS; BRAGA, 2018, P. 8)

Ressalte-se ainda que os mercados negros da *deep web* oferecem ainda dinheiro à venda, o que revela a utilização de *bitcoins* na rede oculta para a lavagem

de dinheiro. Assim, aquela pessoa que detém dinheiro oriundo do tráfico de armas e drogas, por exemplo, tem a possibilidade de comprar *bitcoins* através de uma carteira virtual, cuja a transação é garantida pelo anonimato da rede, ou ainda existe a possibilidade de fazer a venda do seu dinheiro, que poderá ser comprado com outros *bitcoins* que posteriormente serão utilizados para a compra de dinheiro oficial, em operações irrastráveis (ALMEIDA; ROQUE, 2017).

De acordo com Andrade (2017), em virtude do fato de não possuir uma autoridade central regulatória, não é possível exigir da rede de *bitcoins* que as suas atividades sejam pautadas de acordo com as regras do mercado financeiro ou das autoridades centrais responsáveis pelo monitoramento de atividades suspeitas, ou exigir-lhe a adoção de práticas combativas à lavagem de dinheiro, e até mesmo endereçar-lhe eventuais ordens judiciais de sequestro de bens ou medidas coercitivas.

O absoluto anonimato protege as transações financeiras que ocorrem na *deep web*. Entretanto, os serviços que operam na rede como o uso das moedas virtuais, poderiam condicionar suas transações ao fornecimento de dados pessoais e informações bancárias dos clientes, sujeitando-se as obrigações estipuladas pela legislação de combate à lavagem de dinheiro. Ao possibilitar a identificação do agente e podendo a moeda virtual ser considerada ativo passível de ser convertido em dinheiro, seria mais fácil caracterizar o crime e punir os agentes.

Dessa forma, não restam dúvidas de que as operações financeiras levadas a efeito pelos narcotraficantes na *deep web* por meio das moedas virtuais dificultam os trabalhos das autoridades encarregadas da persecução penal, principalmente no que diz respeito à identificação dos agentes, detecção de atividades suspeitas e obtenção de dados de transações realizadas, o que atrai os criminosos dedicados à lavagem de dinheiro e que desejam evitar qualquer tipo de suspeita conduzindo suas operações pelo mundo virtual.

### 3.3 - A ESCASSEZ DE LEGISLAÇÃO ESPECÍFICA NO BRASIL

Com todo o avanço tecnológico e o uso da internet e computadores e outros dispositivos eletrônicos para a prática do crime de lavagem de dinheiro, e conseqüentemente a ausência de uma legislação completa com abrangência para essa nova modalidade de crimes virtuais, os crimes dessa natureza permanecem,

em sua maioria, sem qualquer tipo de punição. Infelizmente, em relação ao aspecto legislativo, o Brasil ainda permanece muito atrasado, por que ainda não possui uma legislação específica para o crime de lavagem de dinheiro realizado por meio virtual, enquanto outros países até menos desenvolvidos já a possuem (CARVALHO; SOUZA; COSTA, 2014).

De acordo com Oliveira e colaboradores (2017), até o final da década de 1990 não havia no Brasil qualquer legislação específica sobre crimes virtuais, utilizando da analogia para tipificar esse crime, como por exemplo o furto de dados se enquadrava no crime de furto do Código Penal, o que também ocorria com crimes de estelionato e extorsão, por já haver previsão no Código Penal, diferenciando-se apenas em relação ao meio utilizado para a sua prática.

Atualmente, a legislação brasileira que trata do assunto de crimes de natureza virtual está pautada na Lei nº. 12.737/12 que alterou o Código Penal e tipificou os crimes dessa natureza, além de deixar claro que as práticas de invadir ambientes, violar dados e divulgar informações contidas em qualquer dispositivo informático, poderá ter como consequência o pagamento de multas ou até mesmo a privação da liberdade. Cabe ressaltar que a referida lei foi fruto de muitas discussões pertinentes a área e da criação de muitos projetos de leis que chegaram a tramitar no Congresso Nacional por mais de dez anos (JOANINE, 2017).

De acordo com Oliveira e colaboradores:

A lei 12.737/12 ficou popularmente conhecida como “lei Carolina Dieckmann” em virtude do episódio com a atriz, que em maio de 2012, teve seu computador invadido por criminosos que divulgaram 36 fotos íntimas da mesma, causando um grande transtorno e constrangimento à vítima. A pena para esse tipo de crime prevê de seis meses a dois anos de reclusão, conforme o art. 154-A do código penal: “Aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas. (OLIVEIRA. 2017, P. 126).

Observe-se que nos casos em que o crime for cometido contra a figura de políticos ou resultar em prejuízos financeiros, a pena poderá ser aumentada, tendo em vista que a propriedade é fortemente defendida pelo direito brasileiro. A lei também visa punir crimes como furtos de dados e clonagens de cartões de crédito, bem como proibir a produção ou divulgação de softwares que permitam a invasão de aparelhos eletrônicos. No entanto percebe-se que a referida alteração não foi

suficiente, sendo necessária a criação da Lei nº. 12.965/14, conhecida como Marco Civil da Internet (JOANINE, 2017).

Na realidade, a internet apresenta cada dias mais desafios para aplicação das regras jurídicas, que podem servir de justificativa para que o Estado deixem de tentar intervir naquela dinâmica, regulamentando objetos e condutas de interesse público e social.

Nesse sentido, a lei do Marco Civil da Internet foi criada na tentativa de suprir as lacunas que havia na legislação em relação aos crimes virtuais. Os princípios que norteiam o referido diploma legal são a liberdade, neutralidade e privacidade, estabelecendo garantias, direitos e deveres em relação ao uso da internet no Brasil. Entre os direitos dos usuários podem-se destacar a inviolabilidade de sua intimidade e vida privada, do sigilo do fluxo de suas informações pela internet, não suspensão da conexão com a internet e a manutenção controlada. As solicitações de informações dessa natureza somente poderão ser solicitada mediante ordem judicial para tal (OLIVEIRA et al, 2017).

Por outro lado, observa-se que essas normas específicas não abrangem todos os campos de atuação dos criminosos na internet, restando mutos lacunas, como no caso da lavagem de dinheiro que ocorre através do meio virtual, bem como de transações realizadas pelo meio virtual como transferencias bancárias e compras pela internet em que o comprador necessita de algum auxílio do poder judiciário, o que ainda é regulamentado pelo Código do Consumidor, mas deveria ter uma legislação própria (JOANINE, 2017).

Assim, muito embora o Marco Civil tenha trazido algumas vantagens e uma evolução em relação ao uso da internet para a prática de alguns crimes, ainda não é o suficiente para coibir as práticas como a lavagem de dinheiro, que necessitaria da criação de um novo tipo penal, já que as autoirdades ainda não contam com um sistema de suporte jurídico, preparo e habilidades necessárias, facilitando as ações dos criminosos que já atuam na área atraindo outras organizações que visam lavar o dinheiro oriundo do tráfico de drogas, armas, prostituição, contrabando, dentre outros.

A legislação brasileira não acompanha o crime virtual, e a internet vem ampliando o alcance da criminalidade e auxiliando na expansão dos negócios de natureza ilícita. Além da legislação escassa, inexistem agências especializadas na investigação dessa nova modalidade delituosa. As únicas prisões realizadas em

fevereiro do corrente ano foram feitas pela Polícia Federal, provavelmente a partir de delações premiadas relacionadas a outras investigações. Além disso, mesmo estando os criminosos presos, ainda não há condenação e tampouco material jurisprudencial que verse sobre a temática.

De acordo com Joanine (2017), uma das possíveis mudanças e melhorias em relação ao crime de lavagem de dinheiro que ocorre por meio virtual, seria a aprovação do novo projeto do Código Penal que ainda se encontra no Senado (Projeto de Lei do Senado – PLS 236/2012) mas ainda não foi apresentado. Tal projeto é fruto de uma proposta apresentada por uma comissão de juristas e tramita no Senado Federal desde julho de 2012. A matéria já foi aprovada por uma comissão responsável da casa, mas ainda não foi votada.

O que poderia mudar é que o projeto que trata do assunto tem um capítulo específico sobre os crimes cibernéticos, inspirado na Convenção de Budapeste, incluindo condutas que ainda não estão previstas no Código Penal vigente, como por exemplo, o acesso sem autorização a sistema de informática, o aumento da pena em razão da utilização e divulgação dessas informações, sabotagem informática, estelionato virtual e lavagem de dinheiro.

#### 3.4 - PROPOSTAS DE AÇÕES PREVENTIVAS E REPRESSIVAS

De acordo com Carvalho (2017), é preciso considerar que a prevenção ainda é o melhor caminho para anular as ações criminosas, realizando ações que interponham obstáculos no caminho da delinquência. A organização da sociedade e dos órgãos públicos que investigam e fiscalizam, principalmente da polícia e órgãos de inteligência, com a criação de uma polícia virtual, por exemplo, contribuiriam para o trabalho de prevenção da lavagem de dinheiro por meio virtual, controle do ciberespaço e vigilância da rede.

A prevenção dos crimes que ocorrem na rede tem como estrutura principal a intensificação de ações que visem facilitar a identificação e localização dos agentes responsáveis pela manutenção dos sistemas de lavagem de dinheiro que utilizam a internet e suas ferramentas para desenvolver a atividade criminosa. Outro aspecto importante diz respeito ao uso da criptografia, como ocorre no caso dos *bitcoins*, em que a quebra de um desses sistemas é bastante complexa e exige trabalho demasiado, o que não compensa para o crime organizado (LOPES JR, 2016).

Ressalte-se que a consciência social também é essencial no auxílio a essa prevenção, além de ser uma aliada para todos os internautas, que não deveriam de forma alguma expor os seus dados nas redes por meio de senhas pessoais, correndo grande risco de serem lesados em seu patrimônio.

Nas palavras de Carvalho:

A justiça social constitui um meio de prevenção para a criminalidade, devendo ser construída através de programas de governamentais e não com simples meio repressivo policial ou judiciário, pois é incoerente uma sociedade que permite, com o sua vulnerabilidade o surgimento e crescimento dos criminosos, exigindo assim, depois dos grandes estragos, um castigo, que mais uma vez lesa os cidadãos, uma vez que, gera custos dos contribuintes manter mais um preso ou mais gastos com o sistema de fiscalização. (CARVALHO. 2017, p. s/p).

Existem ainda outras formas simples de prevenir essa modalidade de crime, como campanhas educativas nas chamadas mídias de massa como rádio e televisão e jornais e até no próprio meio virtual, como já ocorre com outras problemáticas. Não raro, ao entrar nas redes sociais, depara-se com campanhas do Governo Federal contra a prostituição e pornografia infantil, ou sobre pedofilia, por exemplo. Então por que não criar uma campanha sobre o uso consciente das criptomoedas ou o não uso da *deep web*?

Pode-se destacar ainda a atuação das instituições que atuam diretamente na detecção e prevenção do crime de lavagem de dinheiro no Brasil como o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional – DRCI, subordinado à Secretaria Nacional de Justiça – SNJ, mas principalmente do Conselho de Controle de Atividades Financeiras – COAF, que faz parte do GAFI e do Banco Central do Brasil – BACEN.

Em relação ao COAF, Moraes (2015, p.14), explica que:

Esse órgão tem a atribuição de coordenar e propor mecanismos de cooperação e de troca de informações que viabilizem ações rápidas e eficientes no combate à ocultação ou dissimulação de bens, direitos e valores. Para a consecução deste objetivo, tem competência para requerer aos órgãos da Administração Pública as informações cadastrais bancárias e financeiras de pessoas envolvidas em atividades suspeitas e, caso conclua pela existência de crime previsto na Lei de Lavagem de Dinheiro, de fundados indícios de sua prática, ou de qualquer outro ilícito, deve dar ciência



às autoridades competentes para que elas instaurem os procedimentos cabíveis. (MORAES, 2015, p. 14).

Além disso, o Banco Central, poderia agir no sentido de regular e fiscalizar o sistema financeiro por meio virtual, de forma que fossem obedecidas as boas práticas no setor, principalmente em relação ao cadastramento dos clientes e dos controles internos das corretoras que trabalham com *bitcoins*, além de analisar a compatibilidade entre a movimentação desse tipo de recurso, atividade econômica e capacidade financeira dos agentes que o utilizam, da mesma forma que já ocorre com uma pessoa física ou jurídica que possui uma conta bancária, por exemplo (MORAES, 2015).

Por outro lado, em relação aos métodos de repressão, diante da ausência de legislação específica sobre a ocorrência da lavagem de dinheiro por meio virtual, até o ano de 2003, a investigação de crimes contra o sistema financeiro e de lavagem de dinheiro de grande repercussão, eram atribuídas à Coordenação Geral de Combate ao Crime Organizado. Atualmente, tanto o processo de investigação quanto as diligências em busca de prender eventuais operadores pertencentes à organizações criminosas, ainda cabem à Polícia Federal, que não dispõe de um grupo especializado nesse tipo de crime específico (LOPES JR, 2016).

Ressalte-se que existem espalhadas por todo o País Delegacias Especializadas, em defraudações, repressão a crimes financeiros, crimes patrimoniais e em alguns casos até em crimes virtuais. Entretanto, a atuação da polícia civil encontra várias barreiras, principalmente no fato de que as operações de lavagem de dinheiro usando *bitcoins* são realizados em âmbito internacional, fora de sua competência, o que dificulta a investigação e conseqüentemente a prisão desses criminosos.

Vale lembrar que as investigações sobre a lavagem de dinheiro, além da comprovação da autoria e da materialidade do crime, exige das autoridades a localização e recuperação dos ativos lavados, com a representação da autoridade policial à Justiça Federal, o que também exige cooperação internacional, tendo em vista que muitas vezes esses ativos encontram-se em outros países ou paraísos fiscais.

## CONCLUSÃO

Nas últimas duas décadas foi possível observar uma evolução tecnológica em um ritmo jamais experimentado pela humanidade. A cada dia são lançados novos produtos que trazem funções inovadoras e facilidades para o dia a dia. Nesse contexto, a internet possui um papel de destaque tendo em vista a sua influência social e a rapidez no processamento, envio e recebimento de informações. Em contrapartida, da mesma forma que as novas tecnologias criam benefícios no campo social, existem também más consequências, como a criação de novas ferramentas para a criminalidade e o aumento do número de crimes virtuais.

A literatura pesquisada mostrou que os crimes virtuais são todos aqueles delitos realizados com a utilização de algum dispositivo tecnológico e que possam atingir algum bem jurídico de um terceiro, quer seja na esfera material ou moral. Nota-se que algumas características dessa modalidade delituosa podem dificultar o processo de investigação e repressão, como a facilidade de usar um computador, a volatilidade dos dados transmitidos e armazenados, a facilidade de destruição dos vestígios e provas e a dificuldade em identificar os autores do crime, requisitos necessários para uma eventual condenação.

Também foi possível identificar diversas modalidades de crimes virtuais, ou crimes cibernéticos, restando claro que a cada dia crescem em quantidade e variedade, já que a cada dia cresce também o número de usuários e transações realizadas pela rede mundial de computadores. Dentre as principais modalidades de crime virtual é possível citar o estelionato, as fraudes financeiras, pornografia infantil, crimes contra a honra, tráfico de drogas e armas e atualmente a lavagem de dinheiro, que foi objeto desse estudo.

Conforme demonstrado no estudo, o crime organizado é detentor de grandes quantias de dinheiro, mas esses recursos podem ser considerados inúteis, caso deixem algum vestígio em relação à sua origem ilegal ou propriedade. É por essa necessidade de “legalização” dessas quantias, para posterior utilização em outras atividades criminosas e ilegais, que foi desenvolvido o processo de lavagem de dinheiro. O dinheiro lavado, com origem aparentemente legal, pode então ser investido sem levantar qualquer suspeita, contribuindo para o enriquecimento ilícito de seus detentores, sob a cobertura de atividades lícitas e honráveis.

No caso dos crimes virtuais, a pesquisa mostrou que a lavagem de dinheiro no meio virtual ocorre atualmente de duas formas principais: através do uso das criptomoedas ou *bitcoins* e do tráfico de drogas e armas por meio da *deep web*. Em relação aos *bitcoins* as dificuldades de detecção das atividades suspeitas envolvendo a moeda se devem ao fato de que as transações não ocorrem no sistema bancário oficial. Além disso, os *bitcoins* podem facilmente ser convertidos em dólar, euro, real, ou qualquer outra moeda corrente sem grandes dificuldades, já sendo possível encontrar até caixas eletrônicos que possibilitam a conversão imediata e o saque nos lugares onde estão instalados.

Outro fator preocupante em relação à lavagem de dinheiro utilizando os *bitcoins* diz respeito à proteção criptográfica dessas moedas, o que representa uma enorme barreira para a persecução penal, tendo em vista que os meios tecnológicos disponibilizados para as autoridades públicas ainda são arcaicos e não lhes permite elidir as referidas proteções virtuais, restando, nos poucos casos ainda são investigados, a utilização de recursos clássicos como a infiltração policial ou as denúncias anônimas e delações premiadas.

No tocante à *deep web* é necessário ressaltar que se trata de um universo ainda muito obscuro, de onde se detém pouquíssimas informações. Trata-se de um mercado oculto, onde é possível encontrar coisas que são encontradas pesquisando no Google, por exemplo. São produtos e serviços não indexados pelos robôs de busca e que precisam de programas específicos de autenticação ou até mesmo de um convite para o acesso. Embora tenha uso legítimo e legal em alguns países, sobretudo por pessoas que preferem manter suas identidades em sigilo, o uso mais comum da *deep web* ainda é para fins criminosos.

Dessa forma, o tráfico de armas e drogas na *deep web*, até mais diversificado que no “mercado” presencial facilita o crime de lavagem de dinheiro por que impossibilita a identificação dos vendedores e compradores, a identificação da origem dos produtos e a investigação policial, já que não existe nenhuma delegacia ou curso especializado na área. Assim, as organizações criminosas podem facilmente contratar hackers e profissionais da informática para realizar suas transações pela *deep web*, e transformar o dinheiro de origem ilegal em dinheiro “limpo”, inclusive usando também a ferramenta do *bitcoin* conjuntamente.

Diante dessa nova realidade, o estudo evidenciou que a lavagem de dinheiro através do meio virtual deteriora a segurança pública, permitindo que

narcotraficantes, falsificadores e estelionatários expandam seus negócios; corrompe funcionários de instituições financeiras, além de autoridades e advogados; desvia recursos que poderiam ser investidos em outras políticas públicas; aumenta o custo do governo na execução de projetos; coloca em cheque a efetividade das leis e das forças de segurança e fragiliza a sociedade em todos os aspectos.

Por isso, é indispensável que além da atuação conjunta dos órgãos responsáveis pela prevenção e repressão aos crimes virtuais e de lavagem de dinheiro, haja também uma mudança no pensamento político e na consolidação das leis voltada à temática. É indispensável também que a sociedade brasileira possa repensar as políticas de tolerância de consumo à drogas e a compra e venda de produtos as margens da lei. É necessário um esforço conjunto do Estado, das instituições, da força policial, agências de inteligência e principalmente da sociedade principalmente na fiscalização e prevenção.

A legislação brasileira precisa urgentemente se adequar as inovações advindas da tecnologia, como a lavagem de dinheiro por meio virtual. A inexistência de um sistema normativo eficaz que regule a utilização de moedas ou mercados negros virtuais pode resultar em operações policiais frustradas, aumento da impunidade, não identificação dos agentes da lavagem de dinheiro e trazer prejuízos até mesmo para a estabilidade da moeda brasileira dentro e fora do país.

## REFERÊNCIAS

ABREU, K. C. K. **História e usos da internet**. 2008. Disponível em <<http://www.bocc.ubi.pt/pag/abreu-karen-historia-e-usos-da-internet.pdf>> acesso em: 10 abr. 2018.

ALMEIDA, J. J. et al. Crimes cibernéticos. **Ciências humanas e sociais UNIT**, v. 2, n. 3, p. 215 – 236, 2015. Disponível em <<https://periodicos.set.edu.br/index.php/cadernohumanas/article/viewFile/2013/1217>> acesso em: 20 mar. 2018.

ALMEIDA, J. S; ROQUE, B. V. S. Desafios do direito na regulamentação das relações jurídicas na *deep web* e dos crimes. **Anais do VII COMBRADEC**, 2017. Disponível em <<http://revista.unicuritiba.edu.br/index.php/percurso/article/viewFile/2449/1472>> acesso em: 08 mai. 2018.

ANDRADE, M. D. Tratamento jurídico das criptomoedas: a dinâmica dos bitcoins e o crime de lavagem de dinheiro. **Revista brasileira de políticas públicas**, v. 3, n. 7, 2017.

ANSELMO, M. A. **Lavagem de dinheiro e cooperação jurídica internacional**. São Paulo: Saraiva, 2013.

ARO, R. Lavagem de dinheiro – Origem histórica, conceito, nova legislação e fases. **Revista jurídica da Universidade do Sul**, v. 3, n. 6, p. 166 – 177, 2013. Disponível em <[http://www.portaldeperiodicos.unisul.br/index.php/U\\_Fato\\_Direito/article/download/1467/1123](http://www.portaldeperiodicos.unisul.br/index.php/U_Fato_Direito/article/download/1467/1123)> acesso em 29 abr. 2018.

BADARÓ, G. H; BOTINI, P. C. **Lavagem de dinheiro: aspectos penais e processuais penais: comentários à lei 9613/1998, com alteração da Lei 12.683/2012**. São Paulo: Editora Revista dos Tribunais, 2017.

BRASIL. Constituição Fderal (1988). **Constituição da República Federativa do Brasil**. São Paulo. Editora Saraiva. Vade Mecum Saraiva. 25ª edição.

\_\_\_\_\_. Código Penal. **Decreto – Lei Nº. 2.848 de 7 de dezembro de 1940**. São Paulo. Editora Saraiva. Vade Mecum Saraiva. 25ª edição.

\_\_\_\_\_. Código de Processo Penal. **Decreto – Lei Nº. 3.689 de 3 de outubro de 1941**. São Paulo. Editora Saraiva. Vade Mecum Saraiva. 25ª edição.

BARROS, M. A. **Lavagem de capitais e obrigações civis correlatas: com comentários, artigo por artigo, à Lei 9.613/1998**. 4. ed. São Paulo: Editora Revista dos Tribunais, 2013.

\_\_\_\_\_. **Lavagem de capitais: crimes, investigação, procedimento penal e medidas preventivas**. 5. ed. Curitiba: Juruá, 2017.

BRAGA, R. R. P. **Lavagem de dinheiro**: fenomenologia, bem jurídico protegido e aspectos penais relevantes. 2. ed. Curitiba: Juruá, 2013.

CAETANO, A. M. P; MENEZES, J. R. V. **Crimes virtuais: aplicação, falibilidade e impunidade**. Artigo apresentado ao curso de Direito da Universidade Tiradentes – MT, 2015. Disponível em <<http://openrit.grupotiradentes.com/xmlui/bitstream/handle/set/1195/TCC%20-%20Crimes%20Virtuais.pdf?sequence=1>> acesso em: 18 mar. 2018.

CALAZANS, J. H; LIMA, C. A. R. Sociabilidades virtuais: Do nascimento da internet à popularização dos sites de redes sociais online. **9º Encontro Nacional de História da Mídia**, 2013. Disponível em < <http://www.ufrgs.br/alcar/encontros-nacionais-1/9o-encontro-2013/artigos/gt-historia-da-midia-digital/sociabilidades-virtuais-do-nascimento-da-internet-a-popularizacao-dos-sites-de-redes-sociais-online>> acesso em: 10 abr. 2018.

CALLEGARI, A. L; WEBER, A. B. **Lavagem de dinheiro**. São Paulo: Atlas, 2014.

CAMPOS, L. D. A. **Classificação do crime de lavagem de dinheiro na legislação brasileira**. 2015. Disponível em <<http://www.conteudojuridico.com.br/artigo,classificacao-do-crime-de-lavagem-de-dinheiro-na-legislacao-brasileira,50613.html>> acesso em: 21 mar. 2018.

CARNEIRO, A. G. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. **Revista Eletrônica Âmbito jurídico**, n. 99, 2012. Disponível em < [http://www.ambito-juridico.com.br/site/?n\\_link=revista\\_artigos\\_leitura&artigo\\_id=11529](http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529)> acesso em: 20 mar. 2018.

CARVALHO, M. S. R. A trajetória da internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança. Dissertação apresentada ao curso de Engenharia de sistemas da computação da Universidade Federal do Rio de Janeiro, 2006. Disponível em < <http://www.cos.ufrj.br/uploadfile/1430748034.pdf>> acesso em: 06 abr. 2018.

CARVALHO, R. S. Políticas preventivas ao crime cibernético. 2017. Disponível em < <http://domtotal.com/direito/pagina/detalhe/29712/politicas-preventivas-ao-crime-cibernetico>> acesso em: 29 abr. 2018.

CARVALHO, D. L; SOUZA, M. A; COSTA, H. R. Crime virtual: crescimento e falta de leis específicas. 2014. Disponível em < [http://revistapensar.com.br/tecnologia/pasta\\_upload/artigos/a13.pdf](http://revistapensar.com.br/tecnologia/pasta_upload/artigos/a13.pdf)> acesso em: 10 mai. 2018.

COAF. Fases da lavagem de dinheiro. 2014. Disponível em: <<http://www.coaf.fazenda.gov.br/links-externos/fases-da-lavagem-de-dinheiro>> . acesso em: 10 abr. 2018.

COLLI, M. **Cibercrimes**: limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá, 2010.

CRESPO, M. X. F. **Crimes digitais**. São Paulo: Saraiva, 2011.

CUNHA, R. S. **Manual de Direito Penal – Parte Geral**. 3. ed. Salvador: JUSPODIUM, 2015.

DULLIUS, A. A; HIPPLER, A; FRANCO, E. L. Dos crimes praticados em ambientes virtuais. Santa Rosa, 2012. Disponível em <<http://www.conteudojuridico.com.br/artigo,dos-crimes-praticados-emambientes-virtuais,38483.html>> acesso em: 12 abr. 2018.

FURTADO, G. R. Lavagem de dinheiro: aspectos históricos e legais. **Arquivo jurídico**, v. 1, n. 1, 2011. Disponível em <<http://www.revistas.ufpi.br/index.php/raj/article/download/1078/864>> acesso em: 25 abr. 2018.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas. 2008.

GRECO, R. **Curso de Direito Penal**. 17 ed. Rio de Janeiro: IMPETUS, 2015.

JOANINE, B. Crimes virtuais e a necessidade de uma legislação específica. **Conteúdo Jurídico**, Brasília – DF, 2017. Disponível em <<http://www.conteudojuridico.com.br/artigo,crimes-virtuais-e-a-necessidade-de-uma-legislacao-especifica,588942.html>> acesso em: 08 mai. 2018.

LEMOS, A. **O futuro da internet**: Em direção a uma ciberdemocracia planetária. São Paulo: PAULUS, 2010.

LIMA, S. P. Crimes virtuais: uma análise da eficácia da legislação brasileira e desafio do direito penal na atualidade. **Âmbito Jurídico**, Rio Grande, XVII, n. 128, 2014. Disponível em <[http://www.ambitojuridico.com.br/site/index.php?n\\_link=revista\\_artigos\\_leitura&artigo\\_id=15260&revista\\_caderno=3](http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=15260&revista_caderno=3)> acesso em: 10 mai. 2018.

LIMA, D; SANTANA, G. O. C. **BITCOIN**: uma nova tecnologia e a sua utilização para lavagem de dinheiro. **Derecho y cambio social**, 2018. Disponível em <<https://www.derechoycambiosocial.com/revista052/BITCOIN.pdf>> acesso em: 10 mai. 2018.

LOPES, J. R. Mecanismos de cooperação internacional de repressão e combate aos crimes cibernéticos. 2016. Disponível em <<http://esamcuberlandia.com.br/revistaidea/index.php/idea/article/viewFile/134/105>> acesso em: 01 mai. 2018.

MAMEDE, D. C. B. Prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo: legislação e tipologias. Monografia apresentada ao curso de especialização em Direito da Universidade Católica de Brasília, 2014. Disponível em <<https://repositorio.ucb.br/jspui/bitstream/10869/4452/1/Daniela%20Castello%20Branco%20Guimar%C3%A3es%20Mamede.pdf>> acesso em: 29 abr. 2018.

MARCONI, M. A; LAKATOS, E. M. **Fundamentos da Metodologia científica**. 6. ed. São Paulo: Atlas, 2011.

MARTINS, F. E. L; BRAGA, R. R. P. O fenômeno da lavagem de dinheiro e o tráfico de drogas na *deepweb*: avanço da criminalidade virtual. **Revista Brasileira de Ciências criminais**, v. 125, 2016.

MENDRONI, M. B. **Crime de lavagem de dinheiro**. São Paulo: Atlas, 2015.

MORAES, S. A. S. Combate ao crime de lavagem de dinheiro no Brasil. **Revista JURI**, n. 1, 2015. Disponível em <<http://www.atenas.edu.br/Faculdade/arquivos/NucleoIniciacaoCiencia/REVISTAJURI2015/n1/13%20Mecanismos%20de%20Preven%C3%A7%C3%A3o%20de%20Crimes%20de%20Lavagem%20de%20Dinheiro.PDF>> acesso em: 03 mai. 2018.

NUCCI, G. S. **Manual de direito penal**. 7. ed. São Paulo: Revista dos Tribunais, 2011.

OLIVEIRA, B. M. et al. Crimes virtuais e a legislação brasileira. **(RE) Pensando direito**, v. 7, n. 13, p. 119 – 133, 2017. Disponível em <<http://local.cneccsan.edu.br/revista/index.php/direito/article/view/468/342>> acesso em: 19 mar. 2018.

PINHEIRO, P. P. **Direito digital**. São Paulo: Saraiva, 2013.

RECUERO, R. **Redes sociais na internet**. 2. ed. Porto Alegre: SULINA, 2011.

RASMUSSEN, A. Evolução da lavagem de dinheiro. **Carpe Diem – Revista cultural e científica da UNIFASSEX**, v. 11, n. 11, 2013. Disponível em <<https://periodicos.unifacex.com.br/Revista/article/download/358/112>> acesso em: 29 abr. 2018.

SILVA, L. W. L; PEREIRA, M. F. Relação entre a moeda *bitcoin* e os crimes de lavagem de dinheiro. 2016. Disponível em <[http://www.cedipe.com.br/3cbpj/docs/resumos\\_pdf/04\\_MOEDA%20BITCOIN\\_LAVAGEM%20DE%20CAPITAIS.pdf](http://www.cedipe.com.br/3cbpj/docs/resumos_pdf/04_MOEDA%20BITCOIN_LAVAGEM%20DE%20CAPITAIS.pdf)> acesso em: 29 abr. 2018.

VIVIANI, A. K. **Combate à lavagem de dinheiro**. 2005. Disponível em <<https://jus.com.br/artigos/6739/combate-a-lavagem-de-dinheiro>> acesso em: 02 mai. 2018.

WERTHEIM, M. **Uma história do espaço de Dante à internet**. Rio de Janeiro: Jorge Zahar: 2001.