ANAIS DO I COLÓQUIO NACIONAL DO IEDC

DIREITO E TECNOLOGIA

GRUPOS DE TRABALHO

ANAIS DO I COLÓQUIO NACIONAL DO IEDC

DIREITO E TECNOLOGIA

GRUPOS DE TRABALHO

BITCOIN E MEDIDAS CAUTELARES PATRIMONIAIS:
análise da operacionalização

Felipe Américo Moraes

Advogado criminalista no Escritório Beno Brandão Advocacia Criminal. Mestre em Direito pela UNICURITIBA. E-mail: felipe@benobrandao.com.br

Isabela Maria Stoco

Advogada criminalista no Escritório Marion Bach Advocacia Criminal. Pós-graduanda em Direito Penal Econômico (PUC) e Compliance (FAE). E-mail: isabela@marionbach.com.br

Resumo: O processo penal moderno – em especial o voltado à apuração de delitos de natureza econômica – passou a ser marcado pela (demasiada) utilização de medidas cautelares patrimoniais. Como se bem sabe, o Código de Processo Penal brasileiro prevê três distintas medidas constritivas reais: (i) sequestro, (ii) hipoteca legal e (iii) arresto. Além disso, há outras existentes na legislação extravagante. Por outro lado, emerge no cenário mundial a operacionalização de transações financeiras por meio de criptomoedas – dentre as quais a mais conhecida, denominada bitcoin – que ocasionaram uma disrupção na forma pela qual se lida com o dinheiro hodiernamente, posto que as transações (i) ocorrem no ambiente digital, (ii) de forma descentralizada e (iii) de forma pseudoanônima. Tais peculiaridades dificultam sobremaneira a operacionalização de cautelares patrimoniais sobre bitcoins, refletindo uma nova preocupação dos agentes estatais. Nesse sentido, traçam-se dois problemas para análise: (i) o Estado somente tem condições de determinar o bloqueio e a apreensão (transferência para uma carteira do próprio Estado) caso os ativos estejam na carteira da *exchange* ou em uma *web wallet* cujo provedor do serviço também tenha acesso às chaves privadas do usuário; (ii) caso estejam em uma carteira cujas chaves pertencem exclusivamente ao usuário, o único método para operacionalização seria a apreensão da carteira física, caso haja, com a imediata requisição da senha de acesso a ela. Mesmo assim, o autor poderia fazer um backup dela em outro lugar e retirar os valores em caso de uma operação policial, inviabilizando a concretização da constrição. Desse modo, vê-se que a operacionalização das cautelares desse ativo não pode ser observada sob lentes simplistas, devendo-se analisar todas as suas peculiaridades técnicas. Assim sendo, o objetivo do presente trabalho é traçar linhas acerca das medidas cautelares patrimoniais no processo penal brasileiro voltadas a constringir criptomoedas – em especial o bitcoin –, que têm em sua acepção diversas peculiaridades, partindo-se dos dois problemas descritos acima. Para tanto, será realizada uma breve exposição a respeito das cautelares na lei brasileira, com a consequente análise das citadas particularidades das criptomoedas. Ao final, será analisada a viabilidade da constrição desses ativos. Para tanto, valer-se-á de pesquisa exploratória bibliográfica doutrinária.

Palavras-chave: Bitcoin. Cautelares. Criptomoedas. Arresto. Sequestro.

Introdução

A origem do Direito Penal Econômico remonta ao período pós-guerra, em que os Estados, diante do colapso financeiro gerado pelos conflitos, passaram a se utilizar de diversos instrumentos para controlar a economia, dentre eles o Direito Penal. O final do século XX, então, foi marcado pelo fenômeno da expansão (e consolidação) do Direito Penal Econômico, que tem, em sua essência, caráter estritamente financeiro.

Por tal razão é que, nos últimos anos, a utilização das medidas cautelares reais passou a marcar os maxiprocessos decorrentes dessa realidade, uma vez que "o cenário atual do combate à criminalidade organizada e institucionalizada acentua o fenômeno da patrimonialização do direito penal"[1], de modo que o debate acerca da constrição patrimonial ganha relevo no âmbito da criminalidade econômica.

Ainda no cenário de expansão econômica, emerge no cenário mundial a operacionalização de transações financeiras com criptomoedas, sobretudo de bitcoins. Trata-se de uma invenção deveras disruptiva, na medida em que subverte a lógica do sistema financeiro atual (e tradicional), visto que permite a realização de transações descentralizadas. Isto é, que independem de um terceiro intermediário para a sua realização, tais como as instituições financeiras.

Em razão de as transações se realizarem de forma pseudoanônima[2], criminosos passaram a se valer das transações com criptomoedas para a prática de crimes, em especial lavagem de dinheiro, sonegação fiscal e evasão de divisas. Por tal razão, a preocupação com a apuração desses delitos ganhou corpo nos últimos anos e, com ela, face à já citada patrimonialização do direito processual penal (econômico), a preocupação com a constrição cautelar desses ativos.

Nesse sentido, a pesquisa em apreço tem por escopo analisar os dois seguintes problemas: (i) é possível ao Estado determinar o bloqueio de valores caso eles

---

1 LUCCHESI, Guilherme Brenner; ZONTA, Ivan Navarro. Sequestro dos proventos do crime: limites à solidariedade na decretação de medidas assecuratórias. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, vol. 6, n. 2, p. 735-764, maio/ago. 2020. https://doi.org/10.22197/rbdpp.v6i2.353

2 Fala-se em pseudoanonimato visto que é possível deanonimizar uma transação realizada com bitcoins. Por essa razão, afirma-se que as transações com bitcoins não são anônimas, mas pseudoanônimas. Os termos não são sinônimos, mas trata-se de técnicas distintas. Enquanto o anonimato trata da absoluta impossibilidade de relacionar os dados coletados com os indivíduos que os produziram, o pseudoanonimato é o processo em que os dados são armazenados de maneira que não podem ser atribuídos inicialmente a determinada pessoa, exceto com o uso de uma informação adicional, que é armazenada separadamente. Enquanto o anonimato é irreversível, o pseudoanonimato, não (CHA, Shi-Cho *et al.* **Privacy enhancing technologies in the Internet of Things: Perspectives and challenges**. IEEE Internet of Things Journal, 2018. p. 2-7).

estejam custodiados em uma *exchange* centralizada ou em uma *web wallet* (serviços cujo provedor tem acesso às chaves privadas do usuário)?; e (ii) é possível ao Estado determinar a constrição de bitcoins custodiados em carteiras privadas, isso é, casos cujas chaves privadas são administradas exclusivamente pelo usuário?

Assim sendo, partindo-se de uma metodologia exploratória bibliográfica documental, busca-se analisar os problemas acima estampados em relação à criptomoeda denominada bitcoin.[3] Para tanto, será realizada uma análise do atual regramento das medidas cautelares no direito processual penal brasileiro para, posteriormente, serem analisados os problemas traçados.

1. Medidas cautelares patrimoniais no processo penal

Inicialmente à análise da operacionalização das cautelares, é importante trazer à tona breves delineamentos acerca das cautelares no processo penal brasileiro, bem como análise dos paradigmas atuais das medidas constritivas patrimoniais.

1.1. Linhas gerais sobre as cautelares no processo penal

A atividade jurisdicional, no Brasil, compreende três espécies de processo: (i) de conhecimento; (ii) de execução; e (iii) cautelar.[4] A última espécie processual, em última análise, objetiva "assegurar a eficácia dos provimentos jurisdicionais de conhecimento ou de execução"[5], na medida em que intenta resguardar, antecipadamente, o resultado útil do processo. No âmbito do processo penal, são divididas em (i) medidas cautelares pessoais; (ii) medidas cautelares probatórias; e (iii) medidas cautelares reais.

---

[3] Eis porque (i) é a moeda mais comum e (ii) cada criptomoeda tem suas próprias regras de circulação.

[4] Neste ponto, importa esclarecer que há divergência doutrinária acerca da existência de um processo cautelar autônomo: segundo André Nicollit, o Código de Processo Penal não regulou autonomamente o processo penal cautelar, mesmo após a (significativa) reforma formulada pela Lei 12.403 de 2011. No entanto, registra, ainda – valendo-se dos argumentos expostos por Afrânio Jardim –, que, mesmo sem criar uma relação jurídica autônoma, existe *pretensão cautelar* nos casos de requerimento das medidas cautelares – sejam elas pessoais ou reais. Ademais, o autor ainda destaca que não se pode admitir que seja considerado processo aquele que unicamente visa atingir condenação (NICOLITT, André. **Processo Penal Cautelar:** prisão e demais medidas cautelares. 2. ed. São Paulo: Revista dos Tribunais, 2015, p. 21). Em sentido contrário, Gustavo Badaró destaca que "na seara penal, a tutela cautelar não é prestada por meio de um verdadeiro processo cautelar, autônomo em relação ao processo principal" (BADARÓ, Gustavo Henrique Righi Ivahy. MEDIDAS CAUTELARES PATRIMONIAIS NO PROCESSO PENAL. *In*: VILARDI, Celso Sanchez; PEREIRA, Flávia Haral Bresser; DIAS NETO, Theodoro. **Direito Penal Econômico**: Crimes Econômicos e Processo Penal. São Paulo: Saraiva, 2008, p. 147).

[5] NICOLITT, André. **Processo Penal Cautelar**. 2. ed. São Paulo: Editora Revista dos Tribunais, 2015, p. 22.

Em apertada síntese, as medidas cautelares pessoais são aquelas que recaem sobre a pessoa do acusado, consubstanciadas, em essência, na restrição da liberdade do indivíduo. Como exemplo, pode-se citar a prisão propriamente dita, a monitoração eletrônica, a restrição do acesso a determinados lugares e as demais listadas no artigo 319 da codificação processual penal. Podem, ainda, representar a restrição de direitos do indivíduo, como as elencadas na Lei Maria da Penha (art. 22).

As medidas cautelares probatórias, por sua vez, consistem no apossamento, por parte do Estado, de elementos que auxiliem na investigação do delito, tal como a busca e apreensão e a produção antecipada de prova cautelar.[6] Alguns doutrinadores ainda elencam outros exemplos, como busca domiciliar, busca pessoal e interceptação telefônica.[7] Outros, porém, dissertam que, se há o entendimento de que o processo cautelar é autônomo, não há que se falar em medidas cautelares probatórias para os últimos exemplos citados, na medida em que independem de um processo.[8]

Por fim – e que verdadeiramente relevam para as linhas abaixo –, há ainda as medidas cautelares patrimoniais, que consistem na constrição de bens (que podem ser provenientes do crime ou não) do investigado. Objetivam, em síntese, (i) resguardar o produto ou proveito do delito e (ii) resguardar o patrimônio lícito do acusado para fins de satisfação do dano causado à vítima em decorrência da prática delituosa.[9] Noutras palavras, pretendem "assegurar a execução dos pronunciamentos patrimoniais de qualquer classe que possa incluir a sentença, não só à restituição de coisas, à reparação do dano e à indenização dos prejuízos, mas também ao pagamento da multa e custas processuais".[10]

Dentre as características da tutela cautelar, a doutrina tem destacado a instrumentalidade hipotética – instrumento para assegurar o resultado de uma

---

6 LIMA, Marcellus Polastri Lima. **A tutela cautelar no Processo Penal**. 2. ed. Rio de Janeiro: Lumen Juris, 2009, p. 128.

7 NICOLITT, André**. Processo Penal Cautelar**. 2. ed. São Paulo: Editora Revista dos Tribunais, 2015, p. 133-149.

8 LIMA, Marcellus Polastri Lima. **A tutela cautelar no Processo Penal**. 2. ed. Rio de Janeiro: Lumen Juris, 2009, p. 128.

9 BADARÓ, Gustavo Henrique Righi Ivahy. MEDIDAS CAUTELARES PATRIMONIAIS NO PROCESSO PENAL. *In*: VILARDI, Celso Sanchez; PEREIRA, Flávia Haral Bresser; DIAS NETO, Theodoro. **Direito Penal Econômico**: Crimes Econômicos e Processo Penal. São Paulo: Saraiva, 2008, p. 147.

10 LOPES JR., Aury. **Direito Processual Penal**. 18. ed. São Paulo: Editora Saraiva, 2021. p. 307

hipotética condenação –, a acessoriedade – o provimento cautelar não é um fim em si mesmo, dependendo do processo principal –, a preventividade – finalidade é prevenir a ocorrência de um dano irreparável ou de difícil reparação –, sumariedade – a tutela cautelar não se baseia em um juízo de certeza – e a provisoriedade – provisório porque seus efeitos perdurarão até a superveniência de um evento sucessivo.[11]

1.2. Cautelares reais na codificação processual penal

O Código de Processo Penal brasileiro prevê três distintas medidas cautelares patrimoniais: (i) sequestro; (ii) hipoteca legal; (iii) arresto. Existem, porém, outras medidas constritivas previstas em leis extravagantes. Sem a pretensão de – ao menos neste momento – esgotá-las, citam-se a (i) Lei 11.343, de 2006 (Lei de Drogas); (ii) Lei 9.613, de 1998 (Lei de Lavagem de Dinheiro); (iii) Lei 13.260, de 2016; (iv) Decreto-lei 3.240, de 1941; (v) Lei 11.346, de 2006; (vi) Lei 13.322, de 2016.

O sequestro é a medida cautelar que recai sobre o patrimônio ilícito do investigado/acusado, ou seja, incide sobre os bens imóveis ou móveis adquiridos com os proventos da infração apurada (arts. 125 e 126 do CPP). Por tal razão, "não se podem sequestrar bens que integrem o patrimônio ilícito do acusado, mas que tenham sido obtidos pela prática de um crime diverso daquele que é objeto do inquérito policial ou da ação penal em que se requereu a medida cautelar".[12]

Pode ser decretada mediante requerimento do órgão acusador e policial ou mediante pedido do próprio ofendido.[13] Recaindo sobre bens móveis, será realizado o registro na matrícula do bem. Se móvel, deverá ser comunicado ao órgão competente (em caso de carros, por exemplo, ao órgão de trânsito).[14] Importa registrar que essa medida tem um requisito negativo, consistente no não cabimento da busca e apreensão da coisa sequestrada.[15]

---

[11] BADARÓ, Gustavo. **Processo Penal**. 6. ed. (ebook). São Paulo: Revista dos Tribunais, 2020.

[12] BADARÓ, Gustavo. **Processo Penal**. 6. ed. (ebook). São Paulo: Revista dos Tribunais, 2020, s.p.

[13] O texto do artigo 127 destaca a possibilidade de decretação da medida em vertente de ofício; importa registrar que a Lei 13.964, de 2019 (popularmente conhecida como Pacote Anticrime), vedou a decretação pelo magistrado de cautelares de ofício. Desse modo, em razão do conflito aparente de normas, entendem estes autores que o Pacote Anticrime deve favorecer face ao conteúdo original da norma, em razão do critério de *temporalidade*.

[14] LOPES JR., Aury. **Direito Processual Penal**. 18 ed. São Paulo: Editora Saraiva, 2021. p. 307

[15] BADARÓ, Gustavo. **Processo Penal**. 6. ed. (ebook). São Paulo: Revista dos Tribunais, 2020, s.p.

A hipoteca legal, por sua vez, tutela especificamente o interesse patrimonial da vítima, uma vez que objetiva garantir os efeitos patrimoniais da sentença penal condenatória – nos termos do artigo 387, IV, do Código de Processo Penal, que assegura a indenização mínima à vítima. Veja-se que ela pode recair sobre bens imóveis lícitos e pode ser requerida em processos que não tenham valores patrimoniais envolvidos (como no caso de um homicídio, por exemplo). Em razão do fim que lhe é proposto, deve ser requerida pela própria vítima ou pessoa que a substitua em seu legítimo interesse.

A última cautelar patrimonial é o arresto. Pode se dar subsidiariamente à hipoteca legal, sobre bens móveis, se o responsável não possuir bens imóveis ou o valor desses não for suficiente (art. 137, CPP), ou previamente à hipoteca legal, cuja especialização e inscrição, não raro, demandam mais tempo.

Diante do exposto, pode-se verificar que as cautelares patrimoniais têm duas finalidades distintas: o sequestro volta-se a assegurar o cumprimento do efeito da condenação consistente na perda do produto do crime. A hipoteca legal e o arresto, por sua vez, intentam a reparação do dano causado pelo delito. Desse modo, "enquanto a primeira medida cautelar impede o lucro ilícito, a duas últimas asseguram a reparação do prejuízo causado à vítima".[16]

1.3. Novos paradigmas nas cautelares patrimoniais

As medidas cautelares patrimoniais, nos últimos anos, ganharam notável relevância, principalmente após a deflagração de megaoperações, tais como "Mensalão" e "Lava-Jato", eis porque "o cenário atual do combate à criminalidade organizada e institucionalizada acentua o fenômeno da patrimonialização do direito penal".[17] Nesse sentido, Aury Lopes Junior proclama que, "durante muito tempo, as medidas assecuratórias permaneceram em profundo repouso, sem utilização, tornando-se ilustres desconhecidas nos foros criminais. Mas isso é passado, e, nas últimas décadas, com a crescente expansão do direito penal econômico e tributário, as medidas assecuratórias estão na pauta do dia".[18]

---

16 BADARÓ, Gustavo. **Processo Penal**. 6. ed. (ebook). São Paulo: Revista dos Tribunais, 2020, s.p.

17 LUCCHESI, Guilherme Brenner; ZONTA, Ivan Navarro. Sequestro dos proventos do crime: limites à solidariedade na decretação de medidas assecuratórias. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, vol. 6, n. 2, p. 735-764, maio/ago. 2020. https://doi.org/10.22197/rbdpp.v6i2.353

18 LOPES JR., Aury. **Direito Processual Penal**. 18. ed. São Paulo: Editora Saraiva, 2021. p. 307

As medidas construtivas ganharam novo relevo após o advento da Lei 13.964, de 2019, notadamente com a inserção do artigo 91-A do Código Penal, que reconhece o (novo) instituto da perda alargada do patrimônio incompatível com a renda do condenado, medida essa antes inexistente no ordenamento jurídico brasileiro.

Sem adentrar no mérito desta, é importante destacar que, com a referida medida, permite-se ao Estado punitivo adentrar no patrimônio do condenado que não esteja diretamente relacionado com o fato delitivo pelo qual ele foi condenado. Tornou-se possível, então, promover o confisco de todos os bens em posse do acusado. Para tanto, o Ministério Público deve demonstrar que o patrimônio do acusado é incompatível com seu rendimento e, ao final, requerê-lo.[19] Nesse contexto, é certo que as medidas cautelares patrimoniais ganham especial relevo, notadamente por assegurarem, ao final do processo, a possibilidade do confisco de bens.[20]

Aliado a isso, a Lei 13.964, de 2019, ainda incluiu o artigo 133-A no Código de Processo Penal, o qual autoriza a utilização dos bens apreendidos, sequestrados ou sob o regime de qualquer outra medida cautelar pelos órgãos públicos. Foi criada, então, a custódia provisória de bem apreendido. Após o trânsito em julgado, o bem poderá ser transferido definitivamente ao órgão que realizava a custódia do bem.[21]

Além dessas preocupações, ainda há, conforme já supracitado, o incremento do uso dos criptoativos para a prática de delitos (como lavagem de dinheiro, evasão de divisas, etc.). Isso aumenta a preocupação dos órgãos de acusação com a incidência das cautelares sobre tais ativos, causada sobretudo pelas dificuldades técnicas para sua operacionalização. É o que se verá nas linhas a seguir.

2. Operacionalização da constrição cautelar no sistema Bitcoin

Para compreender a possibilidade de contrição cautelar de criptoativos é necessário conhecer alguns detalhes sobre o funcionamento técnico do sistema Bitcoin, assim como do ecossistema em que está inserido.

---

19 MENDES, Tiago Bunning; LUCCHESI, Guilherme Brenner. **Lei anticrime** – a (re)forma e a aproximação de um sistema acusatório. 1. ed. São Paulo: Tirant lo Blanch, 2020, p. 153.

20 Neste ponto, importa trazer uma relevante preocupação: não foi criada uma medida cautelar específica para o confisco alargado, e as medidas já existentes parecem não ser compatíveis com esse instituto. Ocorre, porém, que diariamente as cautelares acabam assegurando a questão do confisco alargado.

21 MENDES, Tiago Bunning; LUCCHESI, Guilherme Brenner. **Lei anticrime** – a (re)forma e a aproximação de um sistema acusatório. 1. ed. São Paulo: Tirant lo Blanch, 2020, p. 85-86.

2.1. Breves linhas sobre o sistema Bitcoin e o ecossistema Bitcoin

Apesar de as transações com bitcoins serem frequentemente descritas como "descentralizadas", essa afirmação ignora algumas características do mercado de criptoativos, sobretudo diante dos diversos provedores de serviços de ativos virtuais.

Enquanto as transações clássicas realizadas no sistema Bitcoin[22], operacionalizadas diretamente entre dois usuárias – também chamadas de transações "ponto a ponto" (*peer-to-peer*) –, são verdadeiramente descentralizadas, o mesmo não ocorre com as transações realizadas pelos diversos provedores de serviços de ativos virtuais, como as *exchanges* centralizadas. Ao menos, não no mesmo nível de descentralização. Isso porque esse modelo de transação acaba sendo muito semelhante – se não idêntico – aos realizados dentro do sistema financeiro tradicional. Por essa razão, entende-se que o nível de descentralização em uma transação com criptoativos oscila a depender da forma como é realizada.

Devido à extensão do tema, explicar o funcionamento do sistema Bitcoin escapa à finalidade do presente artigo. Nesta seção será descrita exclusivamente a forma como o sistema permite a custódia da criptomoeda, sobretudo (i) onde os bitcoins estão localizados e (ii) como sua custódia é realizada pelo usuário. Isso permitirá a posterior verificação da operacionalização de uma medida cautelar patrimonial nesse ambiente.

O primeiro ponto de necessário esclarecimento é quanto à localização. Os bitcoins estão localizados no *blockchain*[23], vinculados ao "endereço" de cada usuário. Mais especificamente, os bitcoins são o produto de todos os registros contidos nesse *blockchain*, do qual é possível extrair a informação sobre a quem pertence cada fração da criptomoeda naquele instante (também conhecida como "saídas de transações não gastas", ou "*unspend transaction outputs*" – UTXO).

---

[22] Bitcoin, com a letra "b" maiúscula, é a coleção de conceitos e tecnologias que formam a base de um ecossistema de dinheiro digital. O sistema Bitcoin consiste em a) uma rede descentralizada "ponto a ponto" (*peer-to-peer*); b) um registro público de transações (o *blockchain*); c) um conjunto de regras de validação das translações e emissão de novas moedas; d) um mecanismo que permite o consenso de maneira global e descentralizada para validar o registro público das transações, chamado de algoritmo da "prova de trabalho" (*proof-of-work*). A unidade desse sistema, por sua vez, também é chamada de bitcoin, mas com a letra "b" minúscula, enquanto as frações de bitcoins são chamadas de "satoshis".

[23] O *blockchain* é o banco de dados público e descentralizado que contém todas as transações de bitcoin já realizadas. Cada bitcoin – ou satoshi – armazenado no *blockchain* está sob o formato de uma longa cadeia que tem informação de todos os endereços aos quais aqueles valores já estiveram vinculados desde o momento de sua criação (durante a mineração).

Ou seja, em sentido oposto ao institivamente se imagina[24], os bitcoins não estão armazenados dentro das respectivas "carteiras" (ou *wallets*).

Ademais, o que determina a propriedade de bitcoins pelo usuário não é a posse da "carteira" com saldo positivo, mas a operação que é realizada por esse dispositivo. Em verdade, a propriedade é determinada por aquele que controla o respectivo "endereço" [25] que dá acesso aos bitcoins, determinado pela posse da respectiva chave criptográfica (chave privada). É dizer que a função de uma "carteira de criptoativos" não é armazenar (dentro de si) os bitcoins, mas somente administrar as "chaves criptográficas" necessárias para acessar o "endereço" de cada fração da criptomoeda que o usuário possui.

Para compreender essa dinâmica, é necessário conhecer os tipos de "carteiras" de criptoativos. Existem a) "carteiras *desktop*"*;* b) "carteiras para celular"*;* c) "carteiras *web*"*;* d) "carteiras de *hardware*"; e) "carteiras de papel".[26]

A forma mais básica de armazenamento das chaves criptográficas ocorre em uma "carteira de papel". Ainda que não tenha sido a primeira desenvolvida, é interessante iniciar a explicação a partir dessa "carteira", pois ela permite compreender a simplicidade do sistema. Como o nome indica, a "carteira de papel" é a simples anotação em um pedaço de papel da chave privada e da respectiva chave pública e "endereço". Com somente tais informações é possível ao usuário receber bitcoins (informando a terceiros seu "endereço"); e, quando pretender gastar, poderá utilizar a respectiva chave privada, à qual somente ele tem acesso.

Nessa dinâmica, uma vez perdida ou esquecida a chave privada, perdem-se igualmente todos os bitcoins vinculados àquele endereço. Não à toa, dos 18,5 milhões de bitcoins em circulação, 20% são considerados perdidos.[27]

---

[24] Esse equívoco já foi cometido anteriormente por Bueno, quando disse ser "plenamente possível, por exemplo, o transporte de bitcoins, em montante equivalente a milhões em moeda soberana, dentro do bolso de um casaco (...)" (BUENO, Thiago Augusto. **Bitcoin e crimes de lavagem de dinheiro**. Editora Contemplar, 2020. p. 120).

[25] O "endereço" é resultado de um cálculo matemático (função *hash*) aplicado (duas vezes) em uma "chave privada". Essa função matemática é conhecida como "função arapuca" (ou *trap door function*), que, em síntese, significa uma fórmula matemática que é facilmente calculada em um sentido, mas impossível de ser realizada no sentido inverso. Em resumo: a partir da "chave privada", extrai-se o "endereço". Todavia, é impossível extrair do "endereço" sua "chave privada".

[26] ANTONOPOULOS, Andreas M. M. **Mastering Bitcoin: Programming the open blockchain**. O'Reilly Media, Inc., 2017 p. 7.

[27] POPPER, Nathaniel. **Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes**. The New York Times, 2021. p. 1.

Por essa razão, há dispositivos de *software* e *hardware* dedicados a realizar essa importante tarefa. A primeira se chama "carteira *desktop*", que fica instalada no computador do usuário; a segunda, "carteira *mobile*", instalada no celular.

Independentemente de terem sido desenvolvidas para operar em computadores ou *smartphones*, elas têm a função de administrar as chaves privadas dos usuários e, a partir delas, gerar quantas chaves públicas e endereços forem necessários, os quais ficam armazenados dentro do *hardware* onde o dispositivo foi instalado. Ou seja, o desenvolvedor da aplicação não tem acesso às chaves criptográficas, somente o usuário.

Há, porém, o risco de esses computadores ou celulares serem furtados, ou de a memória dos equipamentos ser corrompida, o que poderia gerar a perda da chave de todos os bitcoins do indivíduo. Todavia, esse risco foi controlado mediante a criação de uma espécie de "chave mestra", chamada de "frase mnemônica". Trata-se do conjunto de 12 ou mais palavras aleatórias (informadas na língua inglesa como *rabbit, helmet, storage, gold* etc.), sugeridas pela própria aplicação de "carteira", a qual serve de origem para extrair as chaves privadas. É chamada de mnemônica justamente pela facilidade de memorizar ou guardar esse conjunto de palavras. Na prática, caso uma pessoa perca sua carteira, ela poderá recuperar todas as suas chaves privadas inserindo sua frase mnemônica em outra.

Portanto, o usuário que tem acesso ao respectivo "endereço" é quem detém a respectiva fração de bitcoins. Em outras palavras, é esse usuário – e somente ele – que detém a custódia das criptomoedas. Com isso, ele pode guardar consigo e transferir a quem quiser, sem depender de qualquer outro indivíduo ou entidade.

Todavia, devido à dificuldade na localização de outros usuários que possuam bitcoins para realizar uma transação, surgiu nesse mercado uma série de provedores de serviços dedicados a facilitar a interação entre os usuários, classificadas por Grzywotz como o "ecossistema Bitcoin"[28]. Umas delas – uma das mais relevantes – são as *exchanges* centralizadas, as quais são responsáveis por grande parte do volume de transações que ocorrem no mercado de criptoativos. Seu modo de funcionamento é bastante semelhante ao das casas de câmbio tradicionais: elas se colocam como intermediadoras no processo de troca de moeda estatal por criptomoedas, ou exclusivamente entre criptomoedas, oferecendo ao usuário uma

---

[28] GRZYWOTZ. Johanna. **Virtuelle Kryptowährungen und Geldwäsche**. Ducker & Humblot GmbH, 2019. p. 51.

alternativa fácil e segura para realizar a conversão. Em vez de haver a necessidade de procurar uma pessoa, basta ir a essa *exchange* e realizar a compra ou venda de maneira direta.[29]

Ao passo que a entrada desse ator no ecossistema passou a permitir um número maior de negociações e maior liquidez no mercado, tornando factível a compra de altas quantidades de criptomoedas, também é responsável por uma recentralização do ambiente. Em verdade, as transações com criptoativos que ocorrem dentro de *exchanges* centralizadas, ou entre diferentes provedores do mesmo ramo, são tão centralizadas quanto as transações do sistema financeiro tradicional.

Nessa dinâmica, merece destaque a forma como a custódia dos bitcoins é realizada pelas *exchanges* centralizadas. Diferentemente das carteiras que operam mediante a instalação de um *software* no computador ou *smartphone*, há "carteiras *web".* Elas são de muito mais fácil uso ao usuário, visto que são disponibilizadas pelo próprio sistema de uma *exchange.* É permitido ao usuário transferir moeda estatal para a conta da *exchange* centralizada, que passa a exibir no *site* a quantia transferida como forma de saldo. Dessa forma, os valores poderão ser convertidos para qualquer espécie de criptomoeda.

Contudo, na prática, essas conversões não implicam que o usuário disponha daquela quantidade de criptomoedas exibidas na "carteira *web*" da *exchange* centralizada, mas que os valores inicialmente enviados em moeda estatal agora acompanham o câmbio da criptomoeda para qual foi convertida. Na realidade, a *exchange* é quem verdadeiramente tem as criptomoedas, ao passo que o usuário somente tem uma espécie de pretensão creditória em face da *exchange*. Ele somente terá a criptomoeda se realizar o saque desses valores da *exchange* para sua carteira pessoal.

É por essa razão que se afirma que as transações realizadas nas *exchanges* centralizadas ocorrem em duas camadas: a) transações que envolvem a aquisição de uma criptomoeda mediante a correspondente anotação da alteração de propriedade na *blockchain*, chamadas de "*on-chain transactions*"*;* b) transações que

---

[29] GRUPENMACHER, Giovana Treiger. **As plataformas de negociação de criptoativos**: uma análise comparativa com as atividades das corretoras e da bolsa sob a perspectiva da proteção do investidor e prevenção à lavagem de dinheiro. São Paulo: Fundação Getulio Vargas, 2019. p. 60-75.

não são gravadas no *blockchain,* mas em um banco de dados interno da própria *exchange*, conhecidas como "*off-chain transactions*".

A primeira conversão de moeda estatal para qualquer criptomoeda, quando realizada pelo usuário dentro da "carteira *web*" da *exchange*, ocorre somente no banco de dados interno da *exchange*; não há alteração no *blockchain.* Apesar de o sistema informar ao usuário que ele tem determinada quantidade de bitcoins, eles, em verdade, pertencem à *exchange* centralizada, sobretudo porque as chaves privadas e o respectivo endereço são administrados pela *exchange*, não pelo usuário.

Assim, o saldo exibido nessas plataformas somente simula a quantidade de bitcoins que o usuário possui, mas não significa que o usuário tem acesso aos "endereços" das respectivas frações de bitcoin. Na realidade, a *exchange* é quem verdadeiramente tem as criptomoedas, ao passo que o usuário somente tem uma espécie de pretensão creditória em face da *exchange*. Ele somente terá a criptomoeda se realizar o saque desses valores da *exchange* para sua carteira pessoal.[30] Por tal razão, foram sugeridas – sobretudo pelo GAFI[31] – duas nomenclaturas para se referir à forma de custódia de bitcoins: a) "carteiras *web*"*,* para o caso das carteiras das *exchanges* centralizadas, cujos usuários não controlam as respectivas chaves criptográficas de seus bitcoins; b) "carteiras privadas", para aquelas cujas chaves criptográficas são administradas exclusivamente pelo usuário.

Mediante a observação dessas duas classes de "carteiras" – as "carteiras web" e as "carteiras privadas" – é possível identificar como uma medida cautelar patrimonial pode ser realizada no ambiente dos criptoativos.

2.2. Constrição cautelar de bitcoins

Delimitadas algumas características do sistema Bitcoin, passa-se ao enfrentamento dos problemas sugeridos. Primeiro será abordada a possibilidade da

---

30 É por essa razão que se afirma que as transações realizadas nas *exchanges* centralizadas ocorrem em duas camadas: a) transações que envolvem a aquisição de uma criptomoeda mediante a correspondente anotação da alteração de propriedade no *blockchain*, chamadas de "*on-chain transactions*"*;* b) transações que não são gravadas no *blockchain,* mas em um baco de dados interno da própria *exchange*, conhecidas como "*off-chain transactions*".

31 Trata-se do Grupo de Ação Financeira Internacional. O GAFI é reconhecido atualmente como o principal órgão no sistema internacional para direção de políticas de combate à lavagem de dinheiro (BLANCO CORDERO, Isidoro. Isidoro. **El delito de blanqueo de capitales**. 4. ed., 2015 p. 158-159). Trata-se de um organismo intergovernamental, que tem 39 países-membros (FATF. *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,* FATF, 2019) e atua na elaboração de padrões internacionais e na monitoração do grau de cumplicidade dos países, além de financiar pesquisas sobre o tema.

constrição cautelar de bitcoins custodiados em *exchanges* centralizadas, nas respectivas "carteiras *web*". Depois, a possibilidade quanto a bitcoins custodiados exclusivamente pelo usuário, em "carteiras privadas".

2.2.1. Medidas cautelares patrimoniais sobre bitcoins custodiados em "carteiras web" de exchanges

A essa altura fica evidente que os bitcoins armazenados nas "carteiras *web*" de *exchanges* centralizadas são muito semelhantes a valores que estão depositados em instituições financeiras. Isso porque os criptoativos do usuário estão somente em forma de saldo, que é determinado pelo banco de dados interno do provedor do serviço. Nessa relação, quem detém verdadeiramente os bitcoins – ou qualquer outro criptoativo – é a *exchange*. Isso porque, ao final, é ela quem tem o acesso a cada um dos "endereços".

Essa característica permite que, assim como no caso das instituições financeiras tradicionais, a *exchange* possa cumprir determinações do Estado para o bloqueio ou envio dos criptoativos pertencentes a seus usuários. Nesse caso, uma vez sabido que determinado acusado ou investigado tem bitcoins custodiados em uma *exchange* centralizada, a autoridade poderá expedir ofício e solicitar que (i) os valores sejam bloqueados na conta do usuário, e/ou (ii) transferidos a uma "carteira privada" controlada pelo Estado.

Dessa forma, é plenamente possível o cumprimento de ordens judiciais para a constrição cautelar de bitcoins – e outros criptoativos – custodiados nesses provedores de serviço.

2.2.2. "Carteira privadas"

Em sentido oposto, bitcoins armazenados em "carteiras privadas" não são suscetíveis a ordem judicial de bloqueio. Apesar de estarem armazenados no *blockchain,* o acesso aos bitcoins ocorre somente por aquele que tem a respectiva chave privada, armazenada em uma "carteira *mobile*", "carteira *desktop*", "carteira *hardware*" ou "carteira de papel".

Assim, a forma de armazenamento apresenta semelhança com a guarda de dinheiro em espécie: somente uma ordem de busca e apreensão realizada no local em que o usuário guarda suas chaves criptográficas (representada pela "carteira" ou pela chave mnemônica) seria capaz de permitir a apreensão dos valores. Isso

pode permitir à autoridade policial localizar, por exemplo, na residência do investigado uma "carteira de papel" onde as informações necessárias – chaves privadas – estejam anotadas. Com isso, é plenamente possível a transferência dos fundos a uma carteira controlada pelo Estado para que fiquem custodiados durante o processo.

O mesmo resultado pode ser alcançado no caso de uma "carteira *mobile*" ou "carteira *desktop*", desde que o sistema consiga ser acessado pela autoridade policial. Uma vez que isso ocorra, passa a ser igualmente possível a transferência dos fundos para um "endereço" relacionado a uma carteira administrada pelo Estado.

Todavia, essas alternativas podem não ser tão simples. Isso porque há métodos de evitar que o Estado consiga realizar a apreensão de bitcoins. Basta pensar na hipótese de o agente ter uma cópia da "carteira", das chaves criptográficas ou da frase mnemônica em outro local. Isso é, ter um *backup*. Nesse caso, ainda que o Estado consiga apreender as informações necessárias para transferir os bitcoins (realizar a apreensão), seria possível ao agente (ou a um terceiro de sua confiança) realizar a transferência a um "endereço" relacionado a uma nova carteira. Consequentemente, o Estado perderia a oportunidade de realizar a constrição patrimonial.

Mais verticalmente, é possível pensar no caso de o agente memorizar – parcialmente ou integralmente – a chave mnemônica de uma carteira de criptoativos. O procedimento se torna mais facilitado em carteiras que têm somente doze palavras, ou seja, uma pequena combinação que permite fácil memorização. Nessa forma de custódia, não há "carteira" ativa, sendo que, em toda oportunidade em que o usuário pretenda realizar uma nova transação, ele deverá realizar um processo de "recuperação" da "carteira", mediante a inserção da "chave mestra".

Nessa hipótese, não haverá referência física dos bitcoins que o usuário tem. Assim, ainda que o Estado tome conhecimento da quantidade de criptomoedas que determinado investigado ou acusado possui, não haverá meio para operacionalizar uma medida cautelar patrimonial. Em uma hipérbole comparativa, ainda que o agente declare em seu imposto de renda os bitcoins que possui, nada poderá fazer o Estado para apreender esses valores. Isso porque o sistema Bitcoin passou a permitir a completa perda da referência física com valores patrimoniais.

Conclusão

1. As medidas cautelares, no processo penal, podem ser (i) pessoais, (ii) probatórias e (iii) patrimoniais. Em razão da sobredita patrimonializacão do processo, as cautelares patrimoniais ganharam relevo nos últimos anos, em especial no âmbito do direito penal econômico. As cautelares patrimoniais previstas no CPP são arresto, sequestro e hipoteca legal, sem prejuízo das demais previstas em legislação extravagante.

2. As transações com bitcoins – e outros criptoativos – não serão sempre descentralizadas. Assim, do ponto de vista da constrição patrimonial, poderão ter um tratamento distinto a depender de como tais ativos estão custodiados pelo indivíduo.

3. Na hipótese de o bitcoin estar na *exchange*, as medidas cautelares serão operacionalizadas de maneira muito semelhante ao que ocorre no sistema financeiro tradicional: a autoridade policial, ou o Poder Judiciário, poderá solicitar o bloqueio do ativo, com a distinção de que, nesse caso, deverá solicitar a transferência a uma carteira de criptoativos controlada pelo Estado.

4. Em relação à hipótese da carteira privada, não é possível a realização de medida cautelar patrimonial. A única forma de o Estado se apossar do ativo é mediante realização de busca e apreensão (enquanto cautelar probatória), procedimento que encontra sensíveis dificuldades materiais de realização. Isso porque, a depender da forma como o armazenamento das chaves criptográficas é feito pelo usuário, é possível que inexista uma referência física dos bitcoins no mundo virtual e no mundo físico (é o que ocorre, por exemplo, na chave que apenas é memorizada pelo usuário – chave mnemônica).

Referências

BADARÓ, Gustavo Henrique Righi Ivahy. MEDIDAS CAUTELARES PATRIMONIAIS NO PROCESSO PENAL. *In*: VILARDI, Celso Sanchez; PEREIRA, Flávia Haral Bresser; DIAS NETO, Theodoro. **Direito Penal Econômico**: Crimes Econômicos e Processo Penal. São Paulo: Saraiva, 2008.

BADARÓ, Gustavo. A TUTELA CAUTELAR NO PROCESSO PENAL E A RESTITUIÇÃO DE COISA APREENDIDA. **Doutrinas Essenciais Direito Penal e Processo Penal**, São Paulo, vol. 6/2015, Jan - Dez/2015.

BLANCO CORDERO, Isidoro. **El delito de blanqueo de capitales**. 4. ed. 2015.