https://doi.org/10.54795/rejub.n.1.193

A UTILIZAÇÃO DO MALWARE COMO FERRAMENTA DA INFILTRAÇÃO VIRTUAL NA INVESTIGAÇÃO DA CRIMINALIDADE ORGANIZADA: UMA REALIDADE NORMATIVA POSSÍVEL?

THE USE OF MALWARE AS A VIRTUAL INFILTRATION TOOL IN THE INVESTIGATION OF ORGANIZED CRIME: IS ITS REGULATION A POSSIBLE REALITY?

ULISSES AUGUSTO PASCOLATI JUNIOR
Doutor em Direito Penal pela Universidade de São Paulo – USP. Mestre em Direito Penal pela Pontifícia Universidade Católica de São Paulo – PUC/SP. Especialização em Direito Público pela Escola Paulista da Magistratura – EPM, em Direito Penal pela Universidade de Salamanca – USAL e em Raciocínio Probatório pela Universidade de Girona – UDG. Graduado em Direito pela Universidade Presbiteriana Mackenzie. Juiz de direito do Tribunal de Justiça do Estado de São Paulo.
https://orcid.org/0000-0003-4647-4028

RESUMO

O Estado está diante de uma moderna criminalidade organizada. As organizações criminosas atualmente se utilizam de avançada tecnologia para garantir o desenvolvimento de suas atividades. Os tradicionais meios de produção de prova disponíveis ao Estado não são suficientes para ultrapassar as barreiras de proteção tecnológica utilizadas pelas organizações para ocultamento das atividades e dos bens. O Estado não pode continuar a depender da apreensão física dos dispositivos informáticos para ter conhecimento integral das organizações

criminosas. O presente texto tem a finalidade de tentar demonstrar que o *malware* – como meio de prova atípico – é importante ferramenta para o enfrentamento da criminalidade organizada e que sua utilização pelo Estado é uma realidade normativa possível quando conjugadas as disposições internacionais e nacionais relativas à possibilidade da infiltração virtual.

Palavras-chave: investigação; crime organizado; novas tecnologias; *malware*; infiltração virtual.

ABSTRACT

The State is faced with a modern organized crime. Criminal organizations currently use advanced technology to ensure the development of their activities. The traditional ways to produce evidence that are available to the State are not enough to overcome the technological protection barriers used by organizations to conceal activities and assets. The State cannot continue to depend on the physical seizure of computer devices in order to have full knowledge of criminal organizations. The purpose of this article is to try to demonstrate that malware - as an atypical form of evidence - is an important tool to fight the organized crime and that its use by the State is a possible normative reality when combined with international and national rules regarding the possibility of virtual infiltration.

keywords: investigation; organized crime; new technologies; malware; virtual infiltration.

Recebido: 14-3-2022
Aprovado: 28-4-2022

SUMÁRIO

1 INTRODUÇÃO

A sociedade contemporânea enfrenta uma dicotomia: como aceitar os bônus de uma sociedade global na qual há um intercâmbio de facilidades, representadas pelo fácil trânsito de mercadorias, serviços e, sobretudo, dados de informação e, ao mesmo tempo, conviver com o fato de que estas mesmas facilidades fomentam e facilitam o crime organizado numa dimensão de cybercriminalidade.

A globalização é um dado objetivo, realidade para a qual não há retrocesso. Há necessidade, portanto, de convivermos com esse fenômeno que cada vez mais aproxima as pessoas e colabora com o próprio crime organizado. O problema das sociedades modernas é como enfrentar, dentro desse contexto, o crime organizado caracterizado por uma delinquência não convencional, que se expande por todos os continentes, fomentado por redes de intercâmbio de informações e atividades ilícitas facilitado pela evolução tecnológica.

O crime organizado também se globalizou, pois ultrapassou as fronteiras físicas dos países. Atualmente, a criminalidade organizada "navega" em uma "realidade" informacional, impulsionada pela internet, utilizando-se de sistemas e programas que são obstáculos – verdadeiras barreiras virtuais – às investigações criminais, pois dificultam a identificação e a localização do usuário. São utilizados diferentes tipos

de aplicativos de encriptação de ponta a ponta, comunicações que se assentam no protocolo IP e que correspondem às denominadas Voice Over Internet Protocol – VoIP, programas anonimizadores a exemplo do navegador TOR – The Onion Router, o que propicia o acesso a "*deep web*", e, por sua vez, torna mais dificultosa a localização de ativos que trafegam entre paraísos fiscais, *offshore* ou, especialmente, na forma de criptoativos.

As diversas aplicações e programas, em que pese não tenham sido criados para utilização ilícita, pelo contrário, são ferramentas enormemente utilizadas pelas organizações criminais uma vez que permitem técnicas antirrastreamento e antiforenses. Assim, ao mesmo tempo em que o ambiente digital impulsiona o crime organizado, sua utilização deixa rastros digitais, os quais são fonte de prova para que o Estado possa desvendar não apenas a estrutura do próprio crime organizado, como exige a legislação (art. 2º c/c art. 1º, § 1º, da Lei n. 12.850/2013), bem como a localização de ativos confiscáveis vinculados ao delito, ou de ativos não vinculados a determinado delito, mas adquiridos com dinheiro oriundo do ilícito e, ainda, os sofisticados mecanismos de operação de branqueamento de capital.

Diante desse quadro, a verdade é que os institutos tradicionais disponíveis para persecução penal se mostram obsoletos a enfrentar esta delinquência contemporânea e não convencional. Ainda, diante da constante evolução da tecnologia, os modernos meios de investigação autorizados pelo art. 3º da Lei n. 12.850/2013 também se mostram, em determinada medida, ultrapassados. Não obstante a possibilidade de quebras de sigilo telefônico, de dados e telemáticos em *clouds*, *e-mails*, captação ambiental, buscas e apreensões etc. O fato é que a persecução penal ainda depende, em muito, da apreensão física dos dispositivos nos quais as informações são gravadas (quando são gravadas), como

telefones celulares, *tablets*, computadores, *notebooks*, *pen drives*, HDs externos, cartões de memória, máquinas fotográficas etc.

É neste cenário que se propõe a utilização do *malware* como ferramenta de investigação a ser utilizada pelas agências de persecução penal no afã de romper as barreiras encriptadoras e anonimizadoras utilizadas pela criminalidade organizada. Entretanto, é dever consignar que, diferentemente de outros países que possuem a autorização legal para a utilização desse meio excepcional, e aqui registramos, a título de exemplos, Espanha e Itália, a legislação brasileira, até o presente momento, é silente. Contudo, temos que, conjugando-se disposições internacionais estabelecidas na Convenção de Palermo e de Budapeste, com a regulamentação atinente a infiltração virtual – meio este de produção de provas autorizado pelo art. 10-A e seguintes da Lei n. 12.850/2013 – é possível a utilização desta importante ferramenta de investigação representada pelo *malware* quando o objeto de investigação for eventual organização criminosa.

2 FALSO DILEMA: EFICÁCIA E GARANTIA

Não há um verdadeiro dilema estabelecido entre eficácia da persecução penal e preservação de direitos e garantias do acusado. Esse modo de ver eficiência e garantia na busca de segurança social e preservação de direitos objetivando um "justo equilíbrio" (FERNANDES, 2009, p. 226) decorre de equivocada premissa relativa aos fins do processo penal, ou seja, que processo eficiente é aquele que, de modo célere, alcança a condenação de determinada pessoa.

O sistema jurídico processual se mostrará eficiente na medida em que preservar os direitos do acusado ou investigado. Não se trata de escolha de uma dimensão ou outra. Processo dito garantista não

implica impunidade, da mesma forma que processo eficiente não espelha necessária condenação. Processo eficiente é aquele que, respeitando a ordem jurídica, consegue alcançar uma reconstrução histórico-fática que permita ao Estado a imposição da pena. Portanto, trata-se da escolha de outra premissa consistente em se perguntar qual a finalidade do processo penal?

Saliente-se, inicialmente, que a apuração da verdade "é o objetivo fundamental da atividade probatória no processo judicial" (FERRER-BELTRÁN, 2021, p. 46). Nesse sentido, a finalidade epistêmica do processo penal é a busca da verdade, não de uma verdade adjetivada como de real ou material, mas sim de uma verdade que seja aproximada e que corresponda (verdade como correspondência) (RAMOS, 2021, p. 42) a uma determinada reconstrução fática demonstrada pelas provas legalmente apresentadas aos autos, as quais, portanto, permitem, após devida valoração, a superação do postulado da presunção de inocência, sempre com respeito aos direitos e às garantias individuais assegurados pelo ordenamento.

A verdade como correspondência é o próprio fim do procedimento probatório; em outras palavras, "a prova tem com a verdade uma relação teleológica (é um meio para se obter o fim verdade)" (RAMOS, 2021, p. 42; FERRER-BELTRÁN, 2017, p. 72-77). Essa relação de instrumentalidade somente é alcançada quando todas as regras escolhidas democraticamente pelo legislador forem respeitadas. O limite à descoberta da verdade fática aproximada está no respeito aos postulados legais e constitucionais. A descoberta da verdade, destarte, não sugere desrespeito às regras processuais nem deve ser buscada a qualquer custo, como um fim em si mesma. Isto é prática em processos autoritários, como instrumentos de estados igualmente autoritários. Em estados democráticos, a verdade é trazida ao sistema jurídico processual por meio de provas (e meios) legalmente produzidas

pelos atores processuais e, com base nelas, é que o juiz profere as respectivas decisões. Portanto, não vemos incompatibilidade entre "garantismo" e "eficiência" que um processo é tanto mais eficiente na busca da verdade ou de eventual defesa social quanto mais respeitar os direitos dos sujeitos processuais dentro do esquadrinhamento legal trazido tanto pela Constituição quanto pelo legislador ordinário.

No caso da criminalidade organizada, não há dúvidas de que se trata de uma moderna criminalidade que a cada dia se utiliza mais e mais de meios tecnológicos para, com a utilização de ferramentas anonimizadoras e encriptadoras, não apenas garantir a própria existência, mas também para garantir maior desenvolvimento das atividades lícitas e, acima de tudo, tornar seguro o proveito do crime. Assim, para esse tipo de criminalidade, o legislador estabeleceu e permitiu meios probatórios excepcionais. Para situação excepcional, meio excepcional de enfrentamento. Eis uma relação de proporcionalidade estabelecida. Respeitar as balizas do legislador nestes meios de prova excepcionais, que buscam maior eficiência, é dimensão garantista, até porque, o respeito aos cânones dito garantistas não é sinal de impunidade, mas de Estado Democrático comprometido com os Direitos Humanos.

Portanto, o que se tem, em verdade, é um falso dilema, visto que a persecução penal para ser eficiente não induz o desrespeito a direitos e a integral observância dos postulados constitucionais traduzidos pelo legislador ordinário, mesmo no universo da criminalidade organizada excepcional, deve levar a responsabilidade penal daquele é que culpável e a não responsabilização do sujeito inocente. O inverso até pode acontecer, mas por erro, infelizmente, e não porque o processo deve ser mais eficiente e a verdade buscada a qualquer preço.

3 ALGUMAS TECNOLOGIAS À DISPOSIÇÃO DO CRIME ORGANIZADO

As organizações criminais antes vistas como associações estáveis de pessoas cuja atividade era "artesanal" e restrita a determinado território sempre existiram e continuarão existindo, agora moduladas pelas novas tecnologias. Conforme observa Callegari (2016, p. 12), esse fenômeno criminal "sofreu um desenvolvimento extraordinário como consequência das novas tecnologias, avanços tecnológicos em informática e telecomunicações". Assim, as atividades empresariais ilícitas levadas a cabo pelas organizações criminosas passaram de negócios localizados a negócios gerenciados internacionalmente.

O Estado encontra dificuldades em enfrentar – e às vezes até mesmo compreender – esta nova realidade. Pode-se citar, a fim de se demonstrar as dificuldades encontradas pelo Estado na persecução desta nova dimensão das organizações criminosas, algumas tecnologias que, em que pesem sejam voltadas a fins lícitos eis que permitem maior proteção da privacidade do usuário, também estão a serviço das organizações criminosas. Chama-se atenção para as tecnologias de anonimização, as quais permitem às pessoas – e aqui nos referimos aos integrantes das organizações ou a quem com elas estabelecem negócios – não apenas manterem contato seguro e anônimo por meio de troca de mensagens, como também acessar o ambiente virtual sem deixar rastro. Também não se pode deixar de citar as possiblidades de negócios por meio de criptomoedas.

A encriptação representa o "processo de transformação da informação num formato seguro para protegê-la do acesso não autorizado ou de modificações por parte de terceiros" (CAMPOS, 2021, p. 43). Trata-se de tecnologia utilizada pelos principais aplicativos de troca de mensagens instantâneas, como, principalmente, WhatsApp e

Telegram, dentre outros. Representam, em verdade, um obstáculo para a investigação criminal no ambiente digital, posto que, diferentemente das comunicações telefônicas, as quais, segundo Campos (2021, p. 44), assentam-se no protocolo Global System for Mobile Communications – GSM e, por esta razão, ainda que haja encriptação, os "fornecedores de serviços espelham a informação desencriptada", o mesmo não acontece com os:

> [...] *e-mails* que utilizam diferentes tipos de encriptação, com as comunicações que assentam no Protocolo IP e que correspondem às denominadas Voice Over Internet Protocol – VoIP, bem como com o envio de mensagens escritas e de outros dados através de aplicações de mensagens instantâneas. (CAMPOS, 2021, p. 44).

Logo, à exceção do *e-mail* que permite interceptação telemática e, portanto, o acesso ao conteúdo da comunicação, inclusive, por exemplo, se estiver armazenado em determinada *cloud:*

> [...] as principais plataformas de comunicação utilizadas recorrem a denominada "end-to-end encryptions" (encriptação de 'ponta-a-ponta'), o que significa que, mesmo que a comunicação passe através de um servidor, este não tem acesso ao seu conteúdo, pois só o dispositivo receptor tem a chave para a desencriptação daquele. (CAMPOS, 2021, p. 44).

Destarte, qualquer tentativa de interceptação do conteúdo destas comunicações, a exemplo do que acontece com as escutas telefônicas, "é desprovida de efeito útil" (CAMPOS, 2021, p. 45). Nesse sentido, a única forma de lograr o conhecimento do conteúdo da troca

de mensagens, o que pode ajudar não apenas na compreensão da estrutura da organização e o conhecimento da função de cada membro, mas também saber o destino dos bens e valores, é apreendendo os dispositivos, com o acesso físico. Estes dispositivos, ainda, cumpre anotar, em determinados casos são protegidos com senha e com programas de autodestruição, os quais apagam o conteúdo antes da análise forense (*wiping*).

No tocante a programas anonimizadores que permitem navegação na rede mundial sem deixar rastros destaca-se o The Onion Router – TOR, o qual surgiu em 2003 e consiste:

> [...] en un servicio *online* que mediante un *software* específico, de código abierto y multi-plataforma, permite conectarse a una rede de comunicaciones de baja latencia que brinda anonimato para consumir y publicar contenido en internet a quien lo desee. (SALLIS, 2021, p. 604).

A rede TOR é dinâmica e composta por máquinas (roteadores) conectadas à internet, distribuídas ao redor do mundo que constantemente mudam, sendo que esse serviço é responsável por desenhar a rede e seus componentes a cada momento que um navegador TOR exigir. Assim, o navegador TOR seleciona máquinas de entrada, máquinas intermediárias e máquinas de saída. Os conteúdos são consumidos e publicados a partir das máquinas, nunca de forma direta com o destino da comunicação. As máquinas se comunicam entre si, cifrando a comunicação de modo que cada máquina do percurso informacional somente conheça uma porção de tráfego na internet que lhe corresponda. “De esta manera, técnicamente, no hay forma de rehacer el camino hacia atrás, por lo que el anonimato del origen de la comunicación está garantizado” (SALLIS, 2021, p. 605). A rede TOR permite uma conexão tipo “cebola”, pois a mensagem

trafega por distintos roteadores, o que gera a proteção da identidade "de várias capas" – daí surge o nome "cebola" (TEMPERINI; MACEDO, 2021, p. 485). Ademais, a rede TOR muda a cada dez minutos e nunca utiliza as máquinas de saída que estejam em um mesmo país que o restante das demais máquinas fazendo com que, se alguém (agências de persecução, p. ex.) possui alguma forma de escutar o tráfego na rede TOR, nunca irá escutar a "história completa". Somente quem tem acesso aos dados completos da informação é o navegador TOR que está justamente instalado no dispositivo da pessoa que quer resguardar o anonimato (SALLIS, 2021, p. 606). Assim, graças a esse complexo mecanismo de intercomunicabilidade, o TOR oculta a identidade do sujeito, eis que mascara os endereços de IP e oculta dados pessoais, além de ser capaz de bloquear a tentativa de acesso ao computador por meio de *hackers*. Portanto, somente com o acesso físico ao equipamento, via medida de busca e apreensão ou eventual prisão em flagrante, torna-se possível ao Estado conhecer toda a atividade desenvolvida pelo alvo da investigação.

O navegador TOR também permite o acesso ao ambiente da *deep web* – outro mecanismo muito utilizado pelas organizações para o fomento de suas atividades. Ao contrário da *clear web*, cujo conteúdo pode ser acessado por qualquer pessoa por meio de qualquer buscador, como Google, por exemplo, na *deep web* encontra-se todo conteúdo, em geral ilícito, que, além de não ser encontrado por qualquer meio de busca (não há indexação), as pessoas que publicam e oferecem são acobertadas pelo anonimato. É neste ambiente que o crime organizado encontra seu "habitat natural" uma vez que, por meio dos "*black markets*", é possível a comercialização de drogas, armas, dinheiro, documentação, metais preciosos, informação, *malwares*, contratação de matadores, pornografia infantil, entre outros (SALLIS, 2021, p. 611). Assim, sendo a navegação livre, anônima, criptografada e dificilmente detectável é que urge ao Estado a utilização de novas ferramentas. Nesse sentido, Sallis (2021, p. 609):

> [...] el conjunto de personas y organizaciones criminales que se mueven en este entorno hacen que sea muy complejo utilizar los mismos métodos y técnicas de investigación que se usan en la web superficial, haciendo que sea muy difícil saber quién consume contenidos ilegales, o quién o quiénes los publican.

Não pode passar despercebido, eis que é ferramenta deveras importante não apenas para fomento dos negócios ilícitos, mas, especialmente, para se garantir o proveito do crime e a transformação do dinheiro em criptoativos. A utilização de criptomoedas pelas organizações criminosas vem crescendo exponencialmente. As moedas virtuais (criptomoedas) operam mediante um sistema criptográfico por fora do circuito financeiro tradicional e não pertencem a nenhum governo ou banco central (SAIN, 2021, p. 256). O sistema, conforme assevera Silveira (2018, p. 98), "permite pagamentos através da internet, de uma parte a outra parte, sem a intervenção de qualquer instituição financeira". Nesse sentido, tais moedas trafegam em um mercado desregulado e descentralizado, o que permite relativo anonimato. Nesse sentido:

> [...] la idea es ofrecer un sistema de pago seguro y anónimo a los usuarios para que acrediten su identidad para la realización operaciones de compraventa y tanferencias. Las transaciones se realizan de usuario a usuario sin intermediación de bancos u otras instituciones oficiales, son públicas y quedan registradas con un código alfanumérico único y irrepetible, sin dejar rastros. (SAIN, 2021, p. 257).

Ainda que haja um sistema de *blockchain* reconhecido por instituições financeiras que funciona como um banco de dados público que registra o histórico de movimentações dos usuários de criptomoedas, não se pode olvidar que tais moedas podem se

movimentar semelhantemente a um título ao portador, bastando que a pessoa entregue sua *wallets* a outra pessoa ou mesmo realize uma troca. Segundo Silveira (2018, p. 98):

> [...] a possibilidade de anonimato, entretanto, pode vir a assegurar que sua rastreabilidade venha a ser minimizada, caso, *v.g.*, determinado portador de criptomoedas viesse a ter inúmeras carteiras eletrônicas (*wallets*), a ponto de estas mesmas servirem de objeto de escambo ou entrega.

Não obstante, estas tecnologias, saliente-se novamente, não tenham sido desenvolvidas genuinamente para atividades ilícitas, não há dúvidas de que elas, em primeiro lugar, apresentam grande interação entre si e, em segundo lugar, tornaram as organizações criminosas potencialmente mais perigosas e cada vez mais distantes da persecução penal tradicional dos estados.

4 DEFINIÇÃO E ESPÉCIES DE MALWARE

As tecnologias referidas anteriormente dificultam o acesso aos dados de comunicação, quando esses estão em trânsito, uma vez que durante a transmissão da mensagem ponto a ponto esta está encriptada. Assim, é necessário para as agências de investigação a apreensão do dispositivo antes do envio da mensagem ou após o recebimento, visto que, nesse caso, o dispositivo receptor desencriptará o conteúdo da comunicação. Deve ser levado em conta também que os programas anonimizadores dificultam a localização do usuário e a verificação das atividades desenvolvidas. Sem contar, como referido anteriormente, a possibilidade da existência de programas que apagam o conteúdo armazenado nos dispositivos eletrônicos. Nesse sentido, visando superar estas barreiras, mostra-

se necessário o acesso virtual a esses dispositivos para que se possa conhecer as atividades desenvolvidas sem necessidade de apreensão.

Uma solução possível seria a autorização judicial para uma espécie de "hackeamento estatal". O Estado, independentemente da apreensão física do dispositivo, poderia explorar as vulnerabilidades do sistema ou do usuário, por meio de *software* de vigilância, e, assim, acessar o conteúdo das mensagens ou mesmo as operações realizadas, por exemplo, com criptoativos. Uma das vantagens é que todas as informações aportadas no processo penal teriam uma fonte que fora autorizada judicialmente. Essa forma de investigação deixaria de lado qualquer ideia de secretismo e, especialmente, malabarismos processuais das agências de investigação para legalizar determinada informação que adredemente possui, até porque estas tecnologias (programas espiões) são facilmente encontradas no mercado. Interessante a observação de Blanco (2020, p. 94):

> [...] por el contrario, la intervención de dichas comunicaciones es posible para quien cuente con las capacidades técnicas necesarias para "infectar" los puntos de entrada o salida (esto es, el celular o computadora usada por alguna de las personas involucradas en la conversación) con un software de vigilancia especialmente designado para ello, para capturar las comunicaciones en formato de áudio, vídeo y texto sin encriptar (toda vez que los datos se encriptan cuando están en trânsito, no cuando entran o salen del dispositivo receptor o emissor). No se trata de uma mera hipótesis: de hecho, las agencias policiales y de inteligência de EE.UU y otros paíeses ya están recurriendo a este método.

O *malware* – neste contexto, com base nas lições de Campos (2021) e nos conceitos do manual básico da Europol (EUROPEAN CYBERCRIME CENTER, [20--]) – trata-se de um programa informático malicioso que

se aproveita de vulnerabilidades existentes no sistema informático e, em alguns casos, do próprio utilizador. Ele pode ser instalado *in loco* ou remotamente (pela internet), sem consentimento e esclarecimento do alvo. O interessante é que, uma vez instalado, o programa pode levar a efeito um conjunto de tarefas e funcionalidades, em função do que se busca, por exemplo, desvendar a estrutura da organização ou mesmo as formas nas quais ela lava o capital e, sobretudo, a localização dos bens dos integrantes. Por meio do programa, é possível recolher informação interna do sistema informático (dados armazenados, não armazenados – exemplo de um *e-mail* que seria escrito e o armazenador resolveu apagar – ou produzidos em tempo real ou informação externa, p.ex. ativação da *webcam* ou do microfone de modo a captar o que está ao redor.

O *malware* – meio atípico de produção de provas – destarte, com autorização judicial, é uma ferramenta "camaleônica" que permite "uma extensa possibilidade de monitoramento da atividade do alvo e de recolha de dados do sistema informático de forma subreptícia (*surreptitious surveillance*), "consoante o tipo e respetivas funcionalidades que estejam a ser utilizados" (CAMPOS, 2021, p. 40).

Chamo a atenção a dois grupos de *malware*: a) aqueles que, para a instalação, dependem da interação do alvo (utilizador), p.ex. cavalo de Troia*, rootkis* e o *spyware*; e b) aqueles no qual a interação não é necessária (p.ex. *worm*). Em resumo, no primeiro caso, o *malware* surge com a aparência de um *software* legítimo ou verificado e leva o alvo investigado a proceder à instalação, a qual, por sua vez, depende da abertura de um anexo de um *e-mail*, do *download* ou da execução de um arquivo de determinado *website* (uma imagem, p.ex.). Na segunda forma, o programa se autorreplica sem a interação do utilizador. Ele invade os computadores que estejam ligados à mesma rede e ainda não infectados. Pode eliminar

arquivos, enviar documentos via *e-mail*, realizar *downloads* e instalar outros tipos de *malware*.

Nessa senda, a técnica intrusiva, seja a vigilância na fonte ou a captação de dados, poderá, como fonte de provas, trazer ao conhecimento do Estado elementos para que seja possível ao magistrado uma aproximada demonstração das hipóteses fáticas descritas pela acusação e, por conseguinte, afastar o postulado da presunção de inocência. Considerando que direitos constitucionais serão restringidos em prol da investigação, como a intimidade, a privacidade pessoal – art. 5º, inciso X – às vezes a privacidade familiar, esta na dimensão da "invasão domiciliar virtual" – art. 5º, inciso XI –, a autodeterminação comunicacional – art. 5º, inciso XII – e a autodeterminação informacional – necessidade de proteção de dados nos meios digitais (art. 5º, inciso LXXIX, inserido pela Emenda Constitucional n. 115, de 10 de fevereiro de 2022), a pergunta a ser formulada é se o sistema jurídico nacional, nos moldes atuais, permitiria referida técnica?

5 DIMENSÃO INTERNACIONAL E O DIREITO COMPARADO

Como mencionado anteriormente, uma das características da criminalidade organizada é a transnacionalidade. As fronteiras não são mais os limites físicos, pois a execução dos delitos não encontra qualquer limitação territorial, especialmente por conta do tráfego de informações propiciadas pela intercomunicabilidade de dados. Nesse sentido, é que houve a necessidade de imposições internacionais objetivando entre os estados democráticos certa uniformidade do tratamento penal e processual penal do crime organizado.

O enfrentamento do crime organizado e dos delitos conexos (lavagem de ativos, tráficos de pessoas, órgãos, drogas, armas e

animais), os quais movimentam quantias astronômicas de valores, sem dúvida é um dos maiores desafios do mundo moderno. Em razão disso, e objetivando estândares normativos comuns, é que houve a necessidade da transnacionalização das regulações jurídicas e, portanto, da ingerência internacional na busca de uma harmonização penal e processual penal.

A Convenção das Nações Unidas contra a delinquência organizada transnacional (Convenção de Palermo, aprovada em dezembro de 2000, com vigência em 29 de setembro de 2003), assinada pelo Brasil em 12 de dezembro de 2000, ratificada pelo Congresso Nacional em 29 de janeiro de 2004, com caráter vinculante, em resumo, buscou harmonizar as leis penais e processuais penais em todo o mundo e, o que é mais importante, evitar paraísos de impunidade, vale dizer, locais nos quais o crime organizado possa fincar bandeira e desenvolver atividades ilícitas.

A Convenção de Palermo alinhou cinco eixos sobre os quais deveria haver a atuação legislativa dos estados. São eles:

> a) la tipificación ordenada y conjunta de conductas vinculadas con esa forma de criminalidad organizada; b) la tipificación de conductas relacionadas de manera conexa con las actividades llevadas a cabo por esas organizaciones criminales; c) el incremento sustancial de las medidas de injerencia en él ámbito de la privacidad de los indivíduos mediante la aplicación de las nuevas tecnologícas; d) el endurecimento de las condiciones de libertad procesal y la limitación en el ejercício del derecho de defensa, y, por último, e) el agravamento de las condiciones de ejecución de la pena mediante la regulación de medidas postdelictuales. (ABOSO, 2019, p. 84).

Considerando a finalidade do presente trabalho, vale notar o eixo da letra "c" que é referente às técnicas especiais de investigação previstas no art. 20, cujo objetivo é "combater eficazmente a criminalidade organizada". Determinou a normativa internacional dentro dessa linha de autuação mudanças no processo com o incremento de medidas de ingerência no âmbito da privacidade, mediante a utilização de novas tecnologias (vigilância eletrônica e outras fontes de vigilância), além de operações de infiltração de agentes.

Outro documento internacional que merece destaque é a Convenção de Budapeste – Convenção sobre Delitos Cibernéticos – de 23 de janeiro de 2001 – que fora promulgada no Brasil por meio do Decreto-Legislativo n. 37/2021, em 12 de dezembro de 2021. Esta Convenção também é um marco importante no âmbito de luta contra a cibercriminalidade tendo em conta abordar problemas ligados a delitos praticados por meio das redes telemáticas. A convenção, ainda, traça as linhas principais de uma política criminal destinada a sentar as bases de uma harmonização integradora das leis penais e processuais nos países subscritores (ABOSO, 2018, p. 59-60). Esta convenção, com os olhos voltados também à lavagem de dinheiro, ao tráfico de pessoas, drogas e terrorismo, tratou de questões atinentes à produção de prova eletrônica. E, nessa seara, depreende-se dos arts. 19 a 21 que devem os estados estabelecerem medidas relativas ao acesso e busca e apreensão de dados armazenados; à coleta em tempo real dos dados de tráfego e, ainda, à interceptação de dados de conteúdo. Essas medidas podem e devem ser alcançadas com a utilização pelo Estado de *malware* como ferramenta de investigação, eis que com isto se torna possível ultrapassar as barreiras de proteção tecnológica utilizadas no desenvolvimento das atividades ilícitas pelas organizações criminosas.

Diferentemente do Brasil que, a despeito da necessária observância dos dois documentos internacionais mencionados, não possui uma legislação expressa sobre essa forma de intervenção na privacidade, essa técnica de investigação é realidade em alguns países e aqui, a título de ilustração, serão citados Espanha e Itália[1].

A Espanha, por meio da reforma legislativa de 2015 (Ley Orgánica 13/2015, de 5 de ocutubre), mesmo admitindo o maior alcance e potencial de vulneração da intimidade pessoal, previu e permitiu, para alguns crimes – relacionados em *numerus clausus* –, o que garante a proporcionalidade da medida (SALT, 2021, p. 165) o acesso remoto a sistemas informáticos. No art. 588, septies a) no qual estabelece os pressupostos, estabeleceu-se que o juiz poderá autorizar a utilização de dados de identificação e códigos, assim como a instalação de um *software* que permita, de forma remota e telemática, o exame a distância e sem conhecimento do seu titular ou usuários do conteúdo de um computador, dispositivo eletrônico, sistema informático, instrumento de armazenamento de dados informáticos em massa ou base de dados, sempre que se persiga determinados delitos, dentre eles, delitos cometidos por organizações criminosas. O legislador, ainda, estabeleceu os requisitos necessários para a medida determinada judicialmente, notadamente o esclarecimento do *software* que será utilizado para a medida de intrusão.

A Itália caminhou no mesmo sentido. Por meio da Reforma de Orlando (2016, aprovada em 2017), previu-se de forma expressa a utilização do *malware* como meio de obtenção de provas. Esta medida procurou dar ao Estado ferramentas mais modernas para o enfrentamento de uma criminalidade igualmente moderna, mais

[1] A Alemanha também permite referida técnica. Remetemos o leitor para as lições de Salt (2021, p. 166-169); Aboso (2018, p. 489-508) e Campos (2021, p. 105-142). Em relação à professora Juliana Campos, frise-se que há importantes considerações também referentes a Itália, Estados Unidos e Espanha.

agressiva e sofisticada, como é o caso da criminalidade organizada. Nesse sentido:

> foi contemplada no n. 2 do artigo 266 e n. 2-bis do art. 266 do CPPenale, no Cap. IV, relativo à 'intercettazioni di conversazioni o comunicazioni' sob a designação de 'captatore informatico' (sensor ou coletor informático). (CAMPOS, 2021, p. 109).

Tal qual o legislador espanhol, o italiano também estabeleceu o rol de crimes – os menos nos quais é possível a interceptação telefônica – e os requisitos aos quais deve estar adstrita a autorização judicial.

6 PROPOSTA DE SOLUÇÃO: FERRAMENTA AUTORIZADA NA INFILTRAÇÃO VIRTUAL

Como mencionado, no Brasil não há previsão expressa da utilização do *malware* como meio de investigação. Entretanto, temos que, a título de proposta, essa novel forma de investigação, adotada em outros países, poderia aqui ser utilizada considerando os dispositivos e as autorizações legais em vigor, sem prejuízo de, em uma visão multinível, considerarmos que a autorização para a produção deste meio de prova atípico decorra das convenções internacionais adrede mencionadas.

A verdade é que o Estado brasileiro, que tem o dever de investigar as organizações criminosas, não pode ficar à mercê simplesmente da sorte, vale dizer, contar que, seja na realização de uma prisão em flagrante, seja no cumprimento de eventual mandado de busca e apreensão, em algum dispositivo informático apreendido, haja informações relevantes em relação à estrutura de determinada

organização, aos crimes por ela praticados ou, ainda, sobre o destino do produto dos crimes ou bens adquiridos com o dinheiro oriundo do ilícito. A persecução penal deve ser feita de maneira legal, sem secretismos, inteligente, organizada e contando com os instrumentos adequados. A sorte – como evento incerto – é deveras importante, entretanto, não pode ser o centro de qualquer investigação.

Nesse sentido, temos que toda normativa atinente à infiltração de agentes, com destaque para a infiltração virtual, pode ser utilizada objetivando dar segurança jurídica e justificar a flexibilização dos direitos individuais que certamente serão atingidos com esta medida de investigação que é sobremaneira invasiva.

Antes, todavia, cumpre salientar que essa medida somente pode ser utilizada quando, de fato, tratar-se de crime organizado e houver elementos robustos de provas que demonstrem que a autoridade está defronte a uma criminalidade organizada nos moldes exigidos pela lei (art. 1º da Lei n. 12.850/2013). Esta medida não pode ser utilizada para qualquer tipo de criminalidade sob pena de banalização desse meio de produção de provas. Conforme aduz Hassemer (apud COUTINHO, 2017, p. 112) ao tratar dos limites do Estado de Direito para o combate à criminalidade organizada, não se deve utilizar canhões contra pardais ("no se deberia – justo en el campo de los ataques jurídicos del derecho estatal – disparar con cañones a los gorriones").

E mais, em atenção ao princípio da subsidiariedade, essa medida jamais poderá ser a primeira adotada pelo Estado na persecução. Somente após esgotadas todas as medidas possíveis de investigação e sendo, ainda, necessária a continuação da persecução investigativa para desvendar e comprovar a estrutura da organização, sua composição, os crimes praticados ou o destino dos bens, é que se torna possível ao Estado socorrer-se do *malware*.

A Lei n. 12.850/2013 (BRASIL, 2013), no art. 10 e seguintes, estabelece toda a regulamentação da infiltração de agentes. A lei, a seu turno, prevê dois tipos de infiltração: a) a presencial; e b) a virtual. O procedimento da infiltração virtual não difere muito do procedimento da infiltração presencial. Tornam-se necessárias a observância dos pressupostos relativos a: i – legitimidade; ii – autorização judicial; iii – distribuição sigilosa; iv – prazo de duração; v – fixação de limites; vi – controle judicial e do Ministério Público; e vii – apresentação de relatórios circunstanciados (NUCCI, 2021, p. 135-138; MASSON; MARÇAL, 2020, p. 406-447).

A infiltração presencial é mecanismo de produção de provas deveras custoso para o Estado na medida em que é necessária a formação do agente, além de um treinamento social e psicológico, até porque o agente de polícia dependerá da interação dissimulada – com identidade oculta – com membros da organização visando ganhar a confiança para, a partir de então, passar a recolher elementos de prova. Não se pode perder de vista, portanto, que se trata de meio altamente perigoso ainda mais se considerarmos que um dos mecanismos de manutenção da *omertà* das organizações criminosas é a prática da violência. Nesse sentido, é clara a alta probabilidade de insucesso da medida. Destarte, neste contexto, a infiltração virtual mostra-se um meio mais econômico e seguro para o Estado persecução.

A infiltração virtual, no que interessa e nos limites do presente texto, está disposta especialmente no art. 10-A no qual o legislador estabelece os requisitos necessários para a medida (BRASIL, 2013). Assim, devem ser demonstrados os elementos que indiquem tratar-se de uma organização criminosa e os crimes por ela praticados, incluindo os conexos como a lavagem de dinheiro; o alcance das tarefas dos policiais; dados indicativos das pessoas investigadas (nomes e apelidos) e, sendo possível, dados de conexão ou cadastral.

Além desses requisitos, para a autorização judicial, é necessário que a autoridade policial ou o Ministério Público apresentem um plano operacional para a realização da infiltração virtual. Neste plano, salientamos, a autoridade deverá delimitar a espécie de *malware* que utilizará e quais os objetivos que pretende alcançar com a infiltração virtual mediante a utilização de determinado *malware*.

Cumpre anotar que, a título de argumentação, caso se tratasse de infiltração presencial, no mandado de infiltração o juiz delimitaria (ou deveria fazê-lo) as atividades que o agente poderia realizar, como, por exemplo, a possibilidade de apreensão de documentos. Todavia, não é incomum, a depender da especificidade da infiltração, que o agente tenha que utilizar outros meios de investigação, como a realização de escutas e/ou filmagens ambientais em locais públicos ou privados, eis que, ressalte-se, não haveria tempo, diante da dinamicidade da infiltração, para, toda vez que necessitasse o agente realizar referidas investigações, parasse a produção probatória e pedisse autorização do magistrado. Nesse caso, o magistrado também estabeleceria no mandado de infiltração quais métodos de captação de provas estaria o agente infiltrado autorizado a fazer. Assim, se na infiltração pessoal é possível a busca de provas por outros meios igualmente invasivos da intimidade do sujeito, por que haveria óbice na infiltração virtual com a utilização de *malware*?

E mais, além dos limites fixados pelo magistrado, nos termos do art. 10-D, todos os atos eletrônicos – e aqui a recolha da prova por meio do *software* – devem ser registrados, gravados, armazenados e encaminhados ao juiz. Neste ponto, a fim de se garantir minimamente a cadeia de custódia digital, deverá haver um código *hash* que assegurará que o que foi recompilado é efetivamente o apresentado ao magistrado.

Sem contar, outrossim, que dentro do prazo da infiltração (até 6 meses) a critério do magistrado, poderá, como medida de controle, serem requisitados relatórios circunstanciados pelo magistrado ou pelo Ministério Público para aferição das atividades desenvolvidas ou em curso.

Cumpre anotar também que, além da infiltração ser mantida em sigilo, somente as provas produzidas que interessarem à investigação serão mantidas nos autos. Quanto às demais, notadamente as que tragam situações relativas à intimidade, deverão ser destruídas. Por fim, qualquer ato do agente que ultrapasse os limites da investigação e atente contra o interesse público deverá ser reprimido pelos meios legais.

7 CONCLUSÃO

Para o Estado enfrentar delitos cada vez mais complexos, sobretudo quando os ilícitos são praticados por organizações criminosas que se utilizam da tecnologia para desenvolver suas atividades e para tornar seguro o proveito do crime, mostra-se necessária uma adaptação e atualização tecnológica das ferramentas de investigação utilizadas pelos órgãos de persecução.

Os meios tradicionais de produção de prova cada vez mais se tornam obsoletos para superarem as barreiras impostas pela tecnologia. São *softwares* e aplicativos que, não obstante tenham sido desenvolvidos com finalidade lícita, utilizados pelas organizações para fomentar e ocultar a atividade delitiva.

Nesse sentido é que se insere o *malware* como método atípico de produção de provas. Por meio da utilização do *malware* é possível ao Estado superar os obstáculos criados pelos programas e aplicativos

anonimizadores e de criptografia e, por conseguinte, alcançar o desiderato que é descobrir a localização dos membros da organização, suas funções, estrutura do concerto delitivo e o destino que fora dado aos bens oriundos ou adquiridos com os proventos do crime.

Entretanto, em que pese não haja uma autorização expressa para utilização do *malware*, como se vê em outros países, temos que o emprego é possível se esse meio for utilizado como ferramenta da infiltração virtual, meio este de produção de provas autorizado pela lei. Ainda, não é despiciendo afirmar que as convenções internacionais, numa tentativa de harmonização das regulações penais e processuais penais, dispõem sobre estas novas técnicas de vigilância e captura de dados.

Com este novel meio de produção de provas, nos limites estritos da infiltração virtual e da autorização judicial, somente para casos nos quais haja elementos que, de fato, mostrem se tratar de organização criminosa, tendo o Estado esgotado os meios de investigação, será possível ao magistrado autorizar a medida que buscará elementos de prova, os quais, posteriormente valorados, tornarão possíveis ao magistrado uma reconstrução histórica dos fatos, dentro das regras do Estado de Direito.

REFERÊNCIAS

ABOSO, Gustavo Eduardo. **Criminalidad organizada y derecho penal**. Buenos Aires: IBdef, 2019.

ABOSO, Gustavo Eduardo. **Derecho penal cibernético**: la cibercriminalidad y el derecho penal en la moderna sociedad de la información y la tecnologia de la comunicación. Buenos Aires: IBdef, 2018.

BLANCO, Hernán. **Tecnología informática e investigación criminal**: uso de hackers por el estado - spyware legal - nuevas tecnologías de vigilancia - acceso remoto a datos informáticos - búsquedas transfronterizas - desencriptación compulsiva - anonimización y agente encubierto digital - big data y software predictivo - obtención, resguardo y análisis forense de la evidencia digital - deep fakes - prueba informática aportada por hackers. Buenos Aires: La Ley, 2020.

BRASIL. **Lei n. 12.850, de 2 de agosto de 2013**. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei n. 9.034, de 3 de maio de 1995 [...]. Brasília, DF: Presidência da República, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 12 mar. 2022.

CALLEGARI, André Luís. Controle social e criminalidade organizada. *In*: CALLEGARI, André Luís (org.). **Crime organizado**: tipicidade – política criminal – investigação e processo – Brasil, Espanha e Colômbia. 2. ed. Porto Alegre: Livraria Advogado, 2016. p. 11-24.

CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção da prova em processo penal**: a investigação oculta em ambiente digital. Coimbra: Almedina, 2021.

COUTINHO, Jacinto Nelson de Miranda. Hassemer e os "límites del estado de derecho para el combate contra la criminalidad organizada". *In:* INSTITUTO BRASILEIRO DE CIÊNCIAS CRIMINAIS *et al*. **IBCCRIM 25 anos**. Belo Horizonte: D'Plácido, 2017. p. 109-129.

EUROPEAN CYBERCRIME CENTER. **Malware basics**. [*S. l.*]: EUROPOL, [20--]. Disponível em: https://www.europol.europa.eu/cms/sites/default/files/documents/malwarebasicscomplete.pdf. Acesso em: 12 mar. 2022.

FERNANDES, Antonio Scarance. O equilíbrio entre a eficiência e o garantismo e o crime organizado. *In*: TOLEDO, Otávio Augusto de Almeida; LANFREDI, Luís Geraldo Sant'ana; SOUZA, Luciano Anderson de; SILVA, Luciano Nascimento (org.). **Repressão penal e crime organizado**: os novos rumos da política criminal após 11 de setembro. São Paulo: Quartier Latin, 2009. p. 226-265.

FERRER-BELTRÁN, Jordi. **Prova e verdade no direito**. Tradução de Vitor de Paula Ramos. São Paulo: Revista dos Tribunais, 2017. (Coleção o Novo Processo Civil).

FERRER-BELTRÁN, Jordi. **Valoração racional da prova**. Tradução de Vitor de Paula Ramos. Salvador: Juspodivm, 2021. (Coleção Raciocínio Probatório).

MASSON, Cleber; MARÇAL, Vinícius. **Crime organizado**. 5. ed. Rio de Janeiro: Forense, 2020.

NUCCI, Guilherme de Souza. **Organização criminosa**. 5. ed. Rio de Janeiro: Forense, 2021.

RAMOS, Vitor de Paula. **Prova testemunhal**: do subjetivismo ao objetivismo, do isolamento científico ao diálogo com a psicologia e a epistemologia. 2. ed. Salvador: Juspodivm, 2021. (Coleção Raciocínio Probatório).

SAIN, Gustavo. Criminalidad organizada e internet: el uso de tecnologías digitales para el blanqueo ilícito de capitales. *In*: DUPUY, Daniela (dir.); KIEFER, Mariana (coord.). **Cibercrimen**: aspectos de derecho penal y procesal penal. cooperación internacional. recolección de evidencia digital. responsabilidad de los proveedores de servicios de internet. Buenos Aires: IBdef, 2021. p. 249-276.

SALLIS, Ezequiel. Desafíos de la investigación de los delitos informáticos en la "deep & dark web". *In*: DUPUY, Daniela (dir.); KIEFER, Mariana (coord.). **Cibercrimen**: aspectos de derecho penal y procesal penal. cooperación internacional. recolección de evidencia digital. responsabilidad de los proveedores de servicios de internet. Buenos Aires: IBdef, 2021. p. 601-616.

SALT, Marcos G. Allanamiento remoto ¿un cambio de paradigma en el registro y secuestro de datos informáticos? *In*: DUPUY, Daniela (dir.); KIEFER, Mariana (coord.). **Cibercrimen II**: nuevas conductas penales y contravencionales. inteligencia artificial aplicada al derecho penal y procesal penal. novedosos medios probatorios para recolectar evidencia digital. cooperación internacional y victimologia. Buenos Aires: IBdef, 2021. p. 151-181.

SILVEIRA, Renato de Mello Jorge. **Bitcoin e suas fronteiras penais**: em busca do marco penal das criptomoedas. Belo Horizonte: D'Plácido, 2018.

TAVAREZ, Juarez; CASARA, Rubens. **Prova e verdade**. 1. ed. São Paulo: Tirant lo blanch, 2020.

TEMPERINI, Marcelo; MACEDO, Maximiliano. Nuevas herramientas de investigación penal: el agente encubierto digital. *In*: DUPUY, Daniela (dir.); KIEFER, Mariana (coord.). **Cibercrimen**: aspectos de derecho penal y procesal penal. cooperación internacional. recolección de evidencia digital. responsabilidad de los proveedores de servicios de internet. Buenos Aires: IBdef, 2021. p. 481-516.