TESE: “A INFILTRAÇÃO ONLINE POR MEIO DE MALWARE (POLICEWARE), É MEIO DE PROVA LÍCITO E EFICAZ NO O COMBATE ÀS ORGANIZAÇÕES CRIMINOSAS, À PEDOFILIA E AO CIBERCRIME

PROPONENTE

ROBERTO CARMAI DUARTE ALVIM JÚNIOR (MPRS)

JUSTIFICATIVA

O malware, segundo a doutrina especializada, é “**um software malicioso instalado fisicamente ou remotamente em dispositivo eletrônico, sem o conhecimento ou consentimento do seu proprietário, para extração de dados e obtenção de informações de forma oculta**”. Trata-se de ferramenta crucial no combate a crimes graves, como a atuação de organizações criminosas, pedofilia e cibercrimes.

Ele permite que as autoridades acessem dados criptografados ou escondidos em redes anônimas, como a *deep web*, que de outra forma seriam inacessíveis. Em crimes cibernéticos, organizações criminosas e casos de pedofilia, onde os criminosos utilizam tecnologias sofisticadas para ocultar suas atividades, o uso de malware pode ser a única maneira eficaz de obter provas robustas e suficientes para garantir a condenação dos envolvidos.

Quando aplicada sob rigorosa supervisão judicial, essa técnica respeita o princípio da proporcionalidade, sendo utilizada apenas quando necessária e em casos de crimes graves que justificam a intervenção mais intrusiva. Isso assegura que os direitos fundamentais sejam preservados ao máximo, enquanto se garante a efetividade da aplicação da lei em situações que demandam medidas excepcionais.

O uso de *malware* como ferramenta de infiltração pode não apenas ajudar na coleta de provas, mas também desempenhar um papel preventivo significativo. Ao permitir que as autoridades monitorizem atividades criminosas em tempo real, é possível

interromper crimes em andamento, como a disseminação de material de abuso infantil, e desarticular redes criminosas antes que possam causar mais danos. Além disso, o conhecimento de que as autoridades dispõem de ferramentas avançadas para infiltração digital pode atuar como um elemento dissuasor, desencorajando a prática de crimes cibernéticos.

O uso desse meio de obtenção de prova permite que as autoridades do *law enforcement* superem, ao menos, três das principais dificuldades práticas no combate aos autores dos crimes que utilizem terminais informáticos: a **criptografia das comunicações, a completa identificação/rastreamento dos envolvidos e coleta de provas em ambientes digitais restritos.**

A barreira da criptografia ponta-a-ponta talvez seja a mais comum. Ela está presente em aplicativos de mensagens seguros ou em redes anônimas como a *deep web*. Nesses casos, o *malware* pode ser implantado diretamente no dispositivo do suspeito, permitindo que as autoridades capturem mensagens e dados antes de serem criptografados ou depois de serem descriptografados, facilitando a obtenção de provas que, de outra forma, seriam impossíveis de acessar.

Criminosos cibernéticos frequentemente utilizam técnicas avançadas para ocultar sua identidade e localização, como o uso de *VPNs*, *Tor*, ou outras ferramentas de anonimização. A infiltração por *malware* pode ajudar a superar essas barreiras ao permitir que as autoridades monitorizem atividades em tempo real e rastreiem as origens de comunicações e transações digitais, traçando padrões, identificando os responsáveis mesmo quando eles tentam se esconder por trás de camadas de anonimato.

Em relação aos ambientes digitais restritos, em muitos casos, os criminosos armazenam dados incriminatórios em dispositivos protegidos por senhas ou em locais virtuais de difícil acesso, como pastas ocultas ou *chats*/*chains* privados. O *malware* pode ser usado para obter credenciais de acesso, copiar dados diretamente dos dispositivos, ou mesmo registrar atividades no dispositivo comprometido que incriminem esses investigados.

No Brasil, a Lei 12.850/2013, que trata das organizações criminosas, **permite a infiltração policial online.** No artigo 10, o qual regulamenta a infiltração de agentes, foi

incluída a infiltração digital, determinando que essa prática deve ser autorizada judicialmente. Além disso, estabelece que essa técnica deve ser usada em situações em que a prova não possa ser obtida por outros meios disponíveis, caracterizando-se como uma medida de **última ratio**.

A autorização judicial deve ser fundamentada, especificando o alcance das atividades do agente infiltrado, o período de duração da infiltração (inicialmente por até seis meses, prorrogável), e a necessidade da medida para a investigação. **Defende-se que a infiltração por malware está abrangida pela regulamentação desse dispositivo legal.**

Uma das práticas que muito se assemelha ao uso do *malware* é o que se convencionou chamar de "Espelhamento de *WhatsApp*". Trata-se de expediente que tem sido combinado com a Lei de Interceptação Telefônica e Telemática para a prática de monitorar as práticas criminosas a partir do espelhamento das conversas por meio do WhatsApp Web. Vejamos importante julgado sobre a questão:

PROCESSUAL PENAL. AGRAVO REGIMENTAL NO AGRAVO EM RECURSO ESPECIAL. TRÁFICO E ASSOCIAÇÃO PARA O TRÁFICO. NULIDADE. ESPELHAMENTO DE MENSAGENS POR MEIO DO APLICATIVO WHATSAPP WEB. NÃO OCORRÊNCIA. PROVA LÍCITA. PRECEDENTES. AGRAVO REGIMENTAL NÃO PROVIDO.
1. **É possível a utilização, no ordenamento jurídico pátrio, de ações encobertas, controladas virtuais ou de agentes infiltrados no plano cibernético, desde que o uso da ação controlada na investigação criminal esteja amparado por autorização judicial. A chancela jurídica, portanto, possibilita o monitoramento legítimo, inclusive via espelhamento do software Whatsapp Web,** outorgando funcionalidade à persecução virtual, de inestimável valia no mundo atual. A prova assim obtida, via controle judicial, não se denota viciada, não inquinando as provas derivadas, afastando-se a teoria do fruits of the poisounous tree na hipótese.
2. No ordenamento pátrio, as ações encobertas recebem a denominação de infiltração de agentes. **A Lei que trata acerca de Organizações Criminosas, Lei n. 12.850/2013, prevê que, em qualquer fase da persecução penal, serão permitidos, sem prejuízo de outros procedimentos já previstos em lei, infiltração, por policiais, em atividade de investigação**, mediante motivada e sigilosa autorização judicial. Objetiva-se a outorga, ao agente estatal, da possibilidade de penetrar na organização criminosa, participando de atividades diárias, para, assim, compreendê-la e melhor combatê-la pelo repasse de informações às autoridades.
3. De se destacar, que de acordo com ensinamento doutrinário (Mendroni, Marcelo Batouni. Comentários à Lei de Combate ao Crime organizado - Lei n. 12.850/2013. São Paulo Atlas, 2014. p. 75), a ação controlada, pela via do agente infiltrado, resulta em atuação que visa obter prova para incriminar o suspeito, ganhar sua confiança pessoal, mantendo-se a par dos acontecimentos, acompanhando a execução dos fatos e praticando atos de execução, se necessário, como forma de conseguir a informação necessária ao fim da investigação. O agente infiltrado, portanto, tem, ou pode ter, intervenção direta sobre os atos preparatórios e de execução na prática do crime. Da natureza da figura do agente infiltrado, portanto, ter influência no modo como o crime é praticado. Além da já mencionada lei de organizações criminosas (Lei n. 12.850/2013) admitir ações infiltradas, quando houver indícios atuação de organização criminosa, outras legislações, como a Lei n. 11.343/2006 (Lei de Tóxicos), em seu art. 53, I, contempla a

possibilidade de infiltração de agentes (operação undercover) na persecução penal do tráfico ilícito de entorpecentes, como ocorrido na hipótese.

4. De se mencionar, ainda, que a lei que regulamenta o Marco Civil da Internet (Lei n. 12.965/2014), que estabelece princípios, garantias, direitos e deveres para uso da Internet no Brasil, garante o acesso e a interferência no "fluxo das comunicações pela Internet, por ordem judicial". De idêntica forma, a mesma Lei n. 12.850/2013 (Lei da ORCRIM), com redação trazida pela Lei 13.694/2019, passou a prever, de forma expressa, a figura do agente infiltrado virtual, em seu art. 10-A.

5. De outra banda, a Lei n. 9.296/1996 (Interceptação Telefônica), permite, por suas vez, em seu art. 1º, parágrafo único, a quebra do sigilo no que concerne à comunicação de dados, mediante ordem judicial fundamentada. Nesse ponto reside a permissão normativa para quebra de sigilo de dados informáticos, na hipótese, e, de forma subsequente, para permitir a interação, a interceptação e a infiltração do agente, inclusive pelo meio cibernético, consistente no espelhamento do Whatsapp Web. **A lei de interceptação, em combinação com a Lei das Organizações Criminosas, na hipótese, outorga legitimidade (legalidade) e dita o rito (regra procedimental), a mencionado espelhamento, em interpretação progressiva, em conformidade com a realidade atual, para adequar a norma à evolução tecnológica.**

6. A potencialidade danosa dos delitos praticados por organizações criminosas, pelo meio virtual, aliada a complexidade e dificuldade da persecução penal no âmbito cibernético, como na hipótese, devem levar a jurisprudência a admitir as ações controladas e infiltradas, como na presente hipótese, no mesmo plano virtual. De fato, nos últimos anos, as redes sociais e respectivos aplicativos se tornaram uma ferramenta indispensável para a comunicação, interação e compartilhamento de informações em todo o mundo. Entretanto, essa rápida expansão e influência também trouxeram consigo uma série de desafios e problemas no âmbito da investigação, no meio virtual, tornando-se a evolução da jurisprudência acerca do tema questão cada vez mais relevante e urgente.

7. Nessa esteira, como já mencionado, a Lei n. 9.296/1996, que regulamenta as interceptações, conjugada com a Lei n. 12.850/2013, Lei das Organizações Criminosas, permitem a ação controlada e infiltrada virtual, desde que observadas a cláusula de reserva de jurisdição e a finalidade para investigação criminal, atentando-se para o juízo de ponderação dos valores constitucionais em jogo.

8. Nada obstante se possa levantar problemas de ordem moral na utilização da ação controlada e do agente infiltrado, levantando-se infração a limites éticos, observação feita no bojo do voto condutor do acórdão exarado pelo Tribunal recorrido, fato é que o crescimento e desenvolvimento de novas formas de atuação da criminalidade coloca o processo penal em xeque, na medida em que a persecução penal realizada nos moldes tradicionais, com métodos de investigação já comumente conhecidos, tem se mostrado insuficiente no combate à delinquência organizada moderna.

9. Impositivo se mostra, na hipótese em apreço, o estabelecimento de regras processuais compatíveis com a modernidade do crime organizado, porém, sempre respeitando, dentro de tal quadro, os direitos e garantias fundamentais do investigado. Tal desiderato restou alcançado na medida em que, no ordenamento pátrio, a infiltração, igualmente a outros institutos que restringem garantias e direitos fundamentais, está submetida ao controle e amparada por ordem de um juiz competente, tal como se deu na hipótese dos autos, via decisões exaradas na ação cautelar de n. 0060944-90.2018.8.13.0521, que deferiram a ação controlada e a quebra de sigilo de dados e interceptação telefônica, interceptação telefônica de outros terminais e quebra de sigilo telemático, bem como o mencionado espelhamento, realizando-se o acompanhamento das comunicações do ora recorrente, através de espelhamento, o que permitiu a polícia acompanhar diálogos entre os réus, que supostamente indicava uma possível associação criminosa ligada ao tráfico, bem como permitiu a colheita de elementos informativos, sobre a dinâmica e réus.

10. **Não há empecilho, portanto, na utilização de ações encobertas ou agentes infiltrados na persecução de delitos, pela via dos meios virtuais, desde que, conjugados critérios de proporcionalidade (utilidade, necessidade), reste observada a subsidiariedade, não podendo a prova ser produzida por outros meios disponíveis**.

11. A ação controlada e a infiltração, que se configuram como técnica especial de investigação voltada ao combate da criminalidade moderna, deve ser admitida quando a prova não puder ser produzida por outros meios disponíveis, desde que comprovada sua necessidade.

É o que se dá na hipótese dos autos, com o autorizado espelhamento via software Whatsapp Web, como meio de infiltração investigativa, na medida em que a interceptação de dados direta, feita no próprio aplicativo original do Whastapp, se denota, por vezes, despicienda, em face da conhecida criptografia ponta a ponta que vigora no aplicativo original, impossibilitando o acesso ao teor das conversas ali entabuladas. Concebe-se plausível, portanto, que o espelhamento autorizado via software Whatsapp Web, pelos órgãos de persecução, se denote equivalente à modalidade de infiltração do agente, que consiste, como já asseverado, em meio extraordinário, mas válido, de obtenção de prova.
12. Pode, desta forma, o agente policial valer-se da utilização do espelhamento pela via do software Whatsapp Web, desde que respeitados os parâmetros de proporcionalidade, subsidiariedade, controle judicial e legalidade, calcado pelo competente mandado judicial, como ocorrido na hipótese presente. De fato, como já asseverado supra, a Lei n. 9.296/1996, que regulamenta as interceptações, conjugada com a Lei n. 12.850/2013 (Lei das Organizações Criminosas), outorgam substrato de validade processual às ações infiltradas no plano cibernético, desde que observada a cláusula de reserva de jurisdição.
13. Pode-se argumentar que a prova obtida pela via do espelhamento, através do software Whatsapp Web, como modalidade de investigação, via agente infiltrado, implicaria em malferimento à prerrogativa do acusado de não produzir provar contra si mesmo (against self-incrimiantion) ou ao direito de permanecer em silêncio.
Contudo, o respeito ao acusado, na condição de sujeito processual, tão somente impede que o Estado obrigue o investigado a produzir prova contra si mesmo. Desta forma, se o investigado vem a produzir, de forma espontânea, prova apta a corroborar sua inculpação, referida prova deverá ser valorada no processo, ante sua validade. É o que se dá na hipótese do multimencionado espelhamento.
14. De idêntica forma, a objeção de que a facilidade de manipulação da prova obtida pela via do espelhamento do Whatsapp Web, pelo agente infiltrado, tornaria invalida a evidência por tal meio obtida não merece guarida, na medida em que esta Corte Superior tem adotado entendimento pacífico no sentido de que "é despicienda a realização de perícia a fim de comprovar a fidedignidade das gravações, que são presumidamente autênticas, possuindo fé pública os agentes policiais envolvidos na operação. Tal entendimento independe da forma de transmissão das interceptações, se oriundos de gravações de áudio ou captação de mensagens de texto" (AgRg no RHC n. 129.003/MT, Relator Ministro RIBEIRO DANTAS, Quinta Turma, julgado em 13/10/2020, DJe 20/10/2020), bem como que "o instituto da quebra da cadeia de custódia refere-se à idoneidade do caminho que deve ser percorrido pela prova até sua análise pelo magistrado, e uma vez ocorrida qualquer interferência durante o trâmite processual, esta pode implicar, mas não necessariamente, a sua imprestabilidade" (AgRg no RHC n. 147.885/SP, Relator Ministro OLINDO MENEZES (Desembargador Convocado do TRF 1ª Região), Sexta Turma, julgado em 7/12/2021, DJe de 13/12/2021).
15. No caso dos autos, não houve comprovação de qualquer adulteração no decorrer probatório, nenhum elemento veio aos autos a demonstrar que houve adulteração da prova, alteração na ordem cronológica dos diálogos ou mesmo interferência de quem quer que seja, a ponto de invalidar a prova, salvo, naturalmente, a eventual ingerência e interação que decorre da atuação na ação controlada e da condição de agente infiltrado aqui reconhecida, não podendo referida invalidade ser presumida.
16. Em situações análogas a do autos, no mesmo contexto investigativo, esta Corte Superior já se manifestou pela validade das provas. Confira-se: AREsp 2.460.351/MG, AREsp 2.257.960/MG, AREsp 2.347.548/MG e AREsp 2.257.960/MG.
17. Agravo regimental não provido.
(AgRg no AREsp n. 2.318.334/MG, relator Ministro Reynaldo Soares da Fonseca, Quinta Turma, julgado em 16/4/2024, DJe de 23/4/2024.)

No direito comparado, o uso de *malware* em investigações é utilizado em várias jurisdições, como o Reino Unido (*Investigatory Powers Act 2016*), os EUA (***Remote Forensics*** - *Carnivore* e *Magic Lantern*) a Alemanha (Staatstrojaner) e a Itália (***captatore***

informatico ou ***trojan di stato*****).** Portanto, assim como nesses países, embora lá a criação e a regulamentação tenham sido desenvolvidas pelos mais diversos caminhos - legislativos e judiciais - esse meio de obtenção de prova é plenamente aplicável ao Brasil, dentro do âmbito de regulamentação da Lei de Organizações Criminosas.