

O uso de *malware* como meio de obtenção de provas no processo penal brasileiro: da necessidade de lei específica e a impossibilidade do uso análogo de outros dispositivos processuais

The use of malware as a means of obtaining evidence in brazilian criminal proceedings: the need for specific law and the impossibility of analogous use of other procedural devices

Simone Silva Prudêncio¹
Gabriel Rodrigo de Sousa²
Flávia Maria Gomes Campos³

Resumo: O presente estudo tem por objetivo analisar a possibilidade de utilização de *malware* como meio oculto de obtenção de prova no processo penal brasileiro, investigando sua compatibilidade com os direitos fundamentais à privacidade, à intimidade, à inviolabilidade das comunicações e à legalidade estrita. Para tanto, adota-se o método hipotético-dedutivo, sustentado por revisão bibliográfica especializada e pela análise do precedente paradigmático do Superior Tribunal de Justiça no RHC 99.735/SC, no qual se discutiu a licitude de técnicas digitais invasivas de investigação. A partir desse percurso metodológico, os resultados evidenciam que a inserção de *malware* em sistemas informáticos – por permitir acesso a dados pretéritos, presentes e futuros, além de possibilitar monitorização domiciliar mediante câmeras e microfones – extrapola o regime jurídico da Lei nº 9.296/1996 e não encontra amparo em normas processuais penais vigentes, inviabilizando qualquer aplicação analógica ou interpretação extensiva que legitime tais práticas. Ademais, demonstra-se que o STJ, ao reconhecer a natureza híbrida e juridicamente atípica desses meios tecnológicos, reafirmou o princípio da legalidade processual, bem como a necessidade de tutela reforçada da intimidade em contexto de “provas de terceira geração”. As conclusões alcançadas indicam que, embora o *malware* represente instrumento altamente eficiente diante da sofisticação da criminalidade digital, sua utilização no Brasil demanda regulamentação legislativa específica, capaz de delimitar hipóteses taxativas de emprego, requisitos de proporcionalidade e salvaguardas adequadas de controle jurisdicional, sob pena de violação ao Estado Democrático de Direito e às garantias essenciais do processo penal.

Palavras-chave: Malware. Provas. Processo penal

¹ Profa. Associada de Dir. Processual Penal na Universidade Federal de Uberlândia, Doutora em Direito das Relações Sociais pela PUC-SP

² Advogado. Bacharel em Direito pela UFU. Mestre em Direito pela UFU. Especialista em Direito Penal pela EBRADI. Especialista em Direitos Humanos CEI. Doutorando em Direitos Humanos UNESP. Bolsista CAPES(DS) pelo Programa de Doutorado da UNESP.

³ Bacharela em Direito pela UFLA. Mestranda em Direitos Humanos UNESP. Advogada.

Abstract: This study aims to analyze the possibility of using *malware* as a covert means of obtaining evidence in Brazilian criminal proceedings, examining its compatibility with the fundamental rights to privacy, intimacy, the inviolability of communications, and the principle of strict legality. To this end, the research adopts the hypothetical-deductive method, grounded in a specialized literature review and in the analysis of the paradigmatic precedent of the Brazilian Superior Court of Justice in RHC 99.735/SC, in which the legality of highly intrusive digital investigative techniques was assessed. The results indicate that the installation of *malware* in electronic systems—by enabling access to past, present, and future data, as well as permitting domestic monitoring through cameras and microphones—goes beyond the scope of Law No. 9.296/1996 and lacks support in the current procedural criminal framework, thereby preventing the use of analogy or extensive interpretation to legitimize such practices. Moreover, the study shows that the Superior Court of Justice, upon recognizing the hybrid and atypical legal nature of these technological instruments, reaffirmed the principle of procedural legality and the need for enhanced protection of intimacy within the context of “third-generation evidence.” The conclusions reached demonstrate that, although *malware* constitutes a highly effective investigative tool in light of the increasing sophistication of digital crime, its use in Brazil requires specific legislative regulation capable of establishing exhaustive hypotheses for its application, proportionality requirements, and adequate judicial oversight safeguards, lest the practice compromise the Democratic Rule of Law and the essential guarantees of criminal procedure.

Keywords: *Malware. Evidence. Criminal procedure.*

1. Introdução

A vida social, cuja significância representa a própria vida humana, existe, na medida em que só se pode conceber a ideia de humanidade enraizada e empenhada dentro de uma sociedade, somente na presença de outros indivíduos que propiciam a sensação de semelhança e pertencimento. Nesse sentido, a comunicação torna-se a própria ferramenta, demasiadamente humana, utilizada como mecanismo de intervenção na natureza, refletindo as diferentes concepções de mundo, de cada lugar, época e valores.

Nesse sentido, a história da tecnologia também marca o desenvolvimento de diferentes formas de comunicação, que exigem regulamentação e intervenção jurídica. Outrossim, como as cartas demarcavam uma importância singular exigindo que fosse garantida a sua

inviolabilidade, atualmente as redes sociais e aplicativos de mensagens assumem esse posto, e reclamam também a mesma atuação do Direito.

A partir dessa premissa, deve-se considerar que, além da esfera dos Direitos Fundamentais, as discussões sobre os novos mecanismos de comunicação são extremamente relevantes para o Processo Penal, já que em uma sociedade amparada e cada vez mais dependente de tecnologias de informação, a criminalidade assume formas diversas. Ademais, se torna mais sofisticada e com capacidade ímpar de adaptação em meios que os agentes estatais não conseguem chegar, exigindo do legislador dispositivos específicos de normatização, visto que antigos e tradicionais diplomas legais, como a Lei nº 9296/96, são incapazes de regulamentá-los.

Além disso, toda esta dependência produz vestígios que permanecem armazenados em sistemas informáticos, revelando não somente dados sensíveis e protegidos pelo direito à intimidade e a vida privada, mas também a prática de delitos. Por outro lado, a violação de diversos direitos fundamentais resultaria na inutilidade da prova produzida, considerando que o nível de ingerência e de poder contido nas mãos dos investigadores nestes casos exorbitaria as disposições legais pátrias. Igualmente, como atualmente delimitado pelo Superior Tribunal de Justiça (STJ) no advento do julgamento do RHC 99.735-SC, o espelhamento de aplicativos de comunicação resultaria em um tipo híbrido de obtenção de prova, um misto de interceptação telefônica e de quebra de sigilo de e-mail, o que padeceria de ausência de previsão legal.

Neste íterim, este breve estudo se ocupará do uso de *malware* como ferramenta de meio de prova para a persecução penal, a sua inserção em dispositivos informáticos, que já se encontra usual em alguns países, e a sua compatibilidade com o ordenamento jurídico brasileiro. Pode-se definir o *malware* como um *software* instalado em um equipamento eletrônico, sem o conhecimento do utilizador investigado. A intromissão e a devassa na vida privada por meio destes mecanismos de investigação são tão expressivas, que no ano de 2006, o Tribunal Constitucional Federal Alemão criou o conceito,

através da via jurisprudencial, de direito fundamental à confidencialidade e integridade dos sistemas informáticos.

Algumas questões serão suscitadas nessa investigação a saber: se é possível afirmar pela legislação brasileira vigente, em especial a Lei de Interceptações Telefônicas (Lei nº 9296/96), que o ordenamento jurídico brasileiro abarca a possibilidade de utilização do *malware* como fonte legítima da produção de provas; perscrutar o estado de discussão da matéria em relação a jurisprudência do STJ e inferir a natureza jurídica do uso dessa modalidade, em especial sob a ótica do princípio da legalidade, classificando-o como meio legítimo de prova ou não.

A metodologia a ser utilizada nessa pesquisa será a de cunho hipotético-dedutivo, a partir de uma revisão do tema com o estudo de caso do RHC 99.735-SC do STJ, no qual a 6ª turma do Tribunal assentou o entendimento de que o espelhamento de informações via WhatsApp criaria verdadeiro tipo híbrido de obtenção de prova, sem previsão legal. Outrossim, essa opção se justifica porque há ainda no ordenamento jurídico lacunas em relação ao uso da *malware*, em especial nos entraves encontrados no princípio da legalidade e no respeito ao contraditório e ampla defesa na utilização de um sistema de provas não previsto na legislação e, portanto, imprevisível ao réu.

As conclusões esperadas, diante do exposto, são as seguintes: a utilização de *malware* como meio legítimo de obtenção de prova carece, no ordenamento jurídico pátrio, de regulamentação constitucional e infraconstitucional e, pela ótica do princípio da legalidade processual, não pode ser tolerado em um processo penal democrático e garantista. Ademais, demonstrar que o atual estado de coisas na matéria impede a aplicação analógica e complementar de instrumento legais a fim de suprimir as lacunas existentes sobre a aplicação do *malware* como meio legítimo de obtenção de provas no processo penal brasileiro.

2. A sociedade de informação e o uso do *malware* como meio de obtenção de prova.

A capacidade dos indivíduos de se organizarem socialmente se distingue de outras associações naturais, já que a possibilidade de se comunicar produz e reproduz representações e símbolos compartilhados das quais dependem os grupos humanos (SERRANO, 2009, p. 13). A sociedade nunca esteve tão dependente das tecnologias da informação, já que basicamente todas as atividades essenciais, sejam econômicas, culturais, políticas ou afetivas, circundam e dependem de certa forma da rede e de aparelhos digitais. Esta relação simbiótica fragiliza e expõe a vida privada de uma forma que representa uma facilitação para a prática de novos crimes.

Neste cenário, o Estado deve reconhecer a existência de um novo terreno de atuação, no qual grande parte da vida está inserta, resultando em uma verdadeira relação de simbiose entre o ser humano e a tecnologia (CAMPOS, 2018, p. 14). O Estado tem também se curvado ao uso de sistemas de informação para facilitar e desburocratizar seus serviços. Este contexto traz ao menos dois benefícios, quais sejam: a digitalização de serviços estatais e privados que permite diminuir custos e aumenta a participação dos cidadãos que não mais precisam se deslocar (SILVEIRA, 2016, p.6).

Em razão deste contexto, o campo delitivo passou a atuar de maneira categórica nestes cenários, atraindo a atenção do legislador e dos órgãos persecutórios a fim de repensar métodos mais eficazes e capazes de combater a nova criminalidade. Assim, a prova digital e a busca por sua colheita e preservação têm obtido especial relevância, pois o acesso ao ambiente do crime exige o respeito a outros direitos fundamentais recentemente concebidos, sob pena de inadmissão desta prova em Juízo. Não somente, outro desafio que se concebe é a preservação da cadeia de custódia da prova, que de forma totalmente diversa da prova física, a prova colhida em ambiente digital pode não deixar rastros de qualquer alteração.

Em suma, Kerr alerta para o fato de que o mundo virtual é diferente do mundo material, de modo que nem a semelhança conceitual das infrações, do bem jurídico afetado por elas, e nem a identidade terminológica em ambos os mundos, são capazes de ultrapassar essa diferença. E principalmente, o autor alerta que no plano processual, a prova digital não pode ser considerada como uma derivação da prova física, pois tratam-se de realidades distintas que deverão ser objeto de diferentes enquadramentos jurídicos, livres de amarras da analogia e da subsidiariedade de regimes planejados para a prova física. Em razão disso, a prova digital deve ser dotada de um regime autônomo, com mínimas e apenas necessárias remissões para normas aplicáveis ao mundo físico, tendo em vista o conjunto de especificidades pertencentes a prova e ao mundo digital, tornando imperioso a existência de normas que contemplem estas especificidades, incluindo garantias de fidedignidade na recolha e preservação da cadeia de custódia da prova recolhida. (MARTINEZ, 2018, p. 18-19).

Nesse contexto, no plano internacional, surgiu a Convenção sobre Cibercrime em 2001, durante a Conferência Internacional sobre Cibercriminalidade, em Budapeste, no qual traçaram como objetivos aos países ratificantes, a criação de tipos penais comuns entre os Estados, a criação de medidas processuais para o recolhimento da prova em ambiente virtual e, por fim, a cooperação internacional, já que esta espécie de criminalidade não respeita fronteiras (BATISTA, 2018, p.19). Assim, mais precisamente dentro do segundo objetivo traçado na Convenção, isto é, como meio de obtenção de prova, está a inserção de *malware* em dispositivos eletrônicos de pessoas investigadas a fim de captar os rastros digitais que eventualmente se encontram armazenados em seus dispositivos.

Este meio de obtenção de prova consubstancia na inserção *in locu* ou via internet no aparelho informático visado, sem o conhecimento e a vontade da pessoa perquirida, propiciando aos investigadores amplos poderes, como o acesso à conteúdos já produzidos, assim como dados produzidos em tempo real. Quanto a este método, não obstante o combate à nova criminalidade legitime os novos meios de obtenção de prova, não se pode perder de vista que a obtenção da prova digital, assim como os meios para tal, representam violações aos direitos e garantias previstos no texto Constitucional, e em razão disso, devem ser utilizados somente quando absolutamente necessário, dentro

dos ditames da proporcionalidade e do dever de fundamentação das decisões judiciais (OLIVEIRA, 2017, p.27).

Isto pois, a inserção do *malware* em sistemas informáticos transcende a mera interceptação telefônica, já que permite ao investigador não somente o acesso em tempo real aos dados daquela máquina, assim como seus dados pretéritos e futuros. Não somente, permite uma monitorização domiciliar e direta dos indivíduos, com a ativação de câmeras e microfones (BATISTA, 2018, p. 25).

O conceito *malware* surge da conjugação entre o adjetivo “malicioso” e o substantivo “software”, ou seja, é um dispositivo especialmente criado para se infiltrar ou danificar um sistema informático sem conhecimento nem consentimento do seu proprietário (...). Por outras palavras, o *malware* é um software, aparentemente inofensivo que, no fim de instalado num determinado sistema informático, permite ao ‘atacante’ aceder à informação nele contida, monitorizar a sua atividade, desativar ou ativar as funcionalidades de hardware e apropriar-se, eliminar e/ou alterar dados informáticos. Existem vários tipos de *malware*, isto é, vários géneros de softwares que podem ser instalados e utilizados secretamente e sem autorização do seu utilizador, de modo a comprometer as funções do sistema informático (BATISTA, 2018, p. 25-26).

É elementar, ainda, que esta intervenção, seja de qualquer espécie ou grau de ingerência, esteja submetida à jurisdição, já que é atribuição do Poder Judiciário assegurar a proteção dos direitos fundamentais face ao interesse público, ou sacrificá-lo quando estritamente necessário, conforme dita o art. 5º, inciso XII da Constituição Federal. Por outro lado, exige-se dos meios de obtenção de prova, ainda mais aqueles que violam direitos constitucionalmente assegurados, o respeito à legalidade estrita. À exemplo da pena e do tipo penal, as diligências persecutórias que visam instruir a investigação devem estar previstas em Lei (GUARDIA, 2012, p. 150).

Portanto, resta claro que através do *malware*, a investigação criminal em espaço virtual ganha uma dimensão extremamente eficaz, já que garante um acesso ilimitado, de acordo com a espécie infiltrada naquele dispositivo. Por outro lado, traz alguns desafios preocupantes, como por exemplo a necessidade de se preservar a cadeia de custódia da prova, além disso, como

será melhor enfrentado a seguir, não há no ordenamento jurídico brasileiro qualquer norma que permita, expressamente, o uso de inserção de instrumentos ocultos em sistemas informáticos (SILVEIRA, 2016, p. 18). Ademais, existe a discussão sobre a possibilidade de aplicação de outras normas em analogia, encontrando uma base legal no ordenamento pátrio que permita a utilização de *malware* como meio de obtenção de prova.

Diante dessas lacunas, qualquer legislação que busque regulamentar o procedimento deve guardar atenção à proporcionalidade, já que o meio utilizado deve ter justificção ante a sua finalidade, isto é, o delito investigado necessariamente deverá ser grave, e aquele meio de obtenção de prova a última guarida da persecução.

A necessária justificção teleológica consubstancia a noção de justo no processo. A imposição de uma medida gravosa ao investigado não pode dissociar-se do valor de justiça. Assim, o escopo constitucionalmente legítimo é aquele que mais se aproxima da realização da segurança nacional, da segurança pública, do bem-estar econômico do Estado, da defesa da ordem e da prevenção das infrações penais, da defesa da saúde e das liberdades públicas, e sobretudo da dignidade do homem.

(...)

Absolutamente vedada a intervenção voltada a investigações genéricas de possíveis infrações, medida própria do sistema inquisitivo e incompatível com as garantias do processo segundo os ditames do *due processo of law*. A quebra do sigilo das comunicações não se presta ao desiderato de prevenir ou descobrir delitos sem que haja base fática concreta (GUARDIA, 2012, p.151).

Interessante, por fim, destacar que para Campos (2019), além da possível violação da cadeia de custódia da prova, o mencionado método oculto de prova possui vasta danosidade social, já que permite uma busca vaga e genérica, verdadeiro exercício de *fishing expedition*, atingindo um número elevado de pessoas, que transcende a figura do investigado, violando sigilos bancários, de correspondência e a privacidade. Ademais, faz-se possível o recolhimento de enorme quantidade de informações armazenadas no dispositivo e àquelas produzidas em tempo real.

3. A impossibilidade do uso análogo de outros dispositivos normativos e o princípio da reserva legal

É consentâneo que o Código de Processo Penal brasileiro adotou o sistema de liberdade de meios de provas, isto é, que a parte processual produzirá as provas sem ficar adstrito ao rol constante em lei. Primeiramente, deve-se entender como meios de prova os instrumentos processuais e materiais aptos a trazer ao processo a convicção da existência ou inexistência de um fato. No Código de Processo Penal, em seus arts. 158 a 250, estão listados os meios legais de prova que não se tratam de um rol taxativo, desde que não violem princípios e garantias fundamentais. Tanto na doutrina e jurisprudência é uníssono que não vigora no processo penal um sistema rígido de taxatividade dos meios de prova, portanto, são admissíveis meios de prova não disciplinados em lei, desde que não violem direitos e garantias fundamentais previstos na Constituição Federal e a própria Lei (BADARÓ, 2016, p. 344).

Nesse sentido, conforme mencionado alhures, os meios de prova atípicos estão subordinados aos limites constitucionais e legais, tais como, a vedação das provas obtidas sob tortura, coação, com ofensa da integridade pessoal, com violação à intimidade da vida privada, ao domicílio, às correspondências e telecomunicações (SILVEIRA, 2016, p. 16). Todavia, quando houver a necessidade de violação a qualquer direito ou garantia fundamental, estará vigente o princípio da reserva legal, isto é, somente será admissível caso houver previsão legal, conforme denota-se no caso do uso de *malware*. Nesse sentido, imperioso destacar a lição doutrinária:

Nesse sentido, não se pode admitir que um meio de obtenção de prova que fere de maneira inquestionável, e talvez até incomparável, a área nuclear e inviolável da intimidade e a confidencialidade e integridade dos sistemas informáticos, explore os silêncios e lacunas da lei e venha a ser legitimado pelo interprete do direito com base nos dispositivos analisados anteriormente, que não dão azo suficiente para que a medida marque presença no cotidiano dos tribunais e dos cidadãos. Mas da mesma maneira, não pode o

legislador fechar os olhos para esse problema e abrir mão da utilização de um recurso tão eficiente para obtenção de prova, que pode se mostrar como uma verdadeira arma no combate aos tipos mais extremos de criminalidade (MARTINEZ, 2019, p. 118).

Por se tratar de um meio oculto e representar elevado sacrifício de direitos fundamentais, deve estar expressamente sob a exigência de reserva de lei, já que a lei deixará claro o bem jurídico e o direito fundamental lesado ou atingido, assim como o grau de sacrifício que deve sofrer este bem jurídico, as finalidades e os limites dentro da proporcionalidade constitucional. Em caso contrário, serão admitidas pesquisas excessivas e exploratórias que violem a proporcionalidade e a subsidiariedade, transcendendo qualquer necessidade legítima de investigação. Posto isso, não há como se admitir o uso análogo de outras normas para legitimar métodos de busca de provas extremamente intrusivos, incumbindo ao legislador definir os limites e momentos em que devem ser usados. É incumbência do Estado definir até onde a *persecutio criminis* e o *ius puniendi* pode afetar direitos, liberdades e garantias de cidadãos presumivelmente inocentes para obtenção de provas (MARTINEZ, 2019, p. 120).

O primeiro direito fundamental violado através da inserção de *malware* em equipamentos informáticos é o direito à intimidade. O referido direito encontra guarida no artigo 12 da Declaração Universal dos Direitos do Homem e no artigo 17 do Pacto Internacional de Direitos Políticos e Civis. No ordenamento jurídico brasileiro, este direito é tutelado no art. 11 ao 21 do Código Civil e no art. 5º, inciso X da Constituição Federal.

Silveira (2016, p. 24), com base na doutrina e jurisprudência alemã, faz uma distinção de três áreas da vida que merecem observância: a vida íntima, a vida privada e a vida pública. A vida íntima se relaciona aos aspectos da vida que devem ser protegidos em absoluto, não se admitindo qualquer intromissão, tampouco qualquer juízo de proporcionalidade. Por outro lado, a vida privada se refere aos acontecimentos compartilhados com um pequeno nicho de pessoas. Diante disso, ante à disponibilidade pelo próprio indivíduo,

poderá ser sacrificada em sede de prova em processo penal, desde que adstrita aos princípios da proporcionalidade e subsidiariedade.

O Tribunal Constitucional também já por múltiplas vezes se pronunciou sobre o conteúdo da reserva da intimidade da vida privada, cabendo dar destaque à noção adoptada no Acórdão n.º 128/92: “o direito de cada um ver protegido o espaço interior ou familiar da pessoa ou do seu lar contra intromissões alheias. (...) neste âmbito privado ou de intimidade está englobada a vida pessoal, a vida familiar, a relação com outras esferas de privacidade (v.g. a amizade), o lugar próprio da vida pessoal e familiar (v.g. o lar ou o domicílio), e bem assim os meios de expressão e comunicação privados (a correspondência, o telefone, as conversas orais, etc.) (SILVEIRA, 2016, p. 25).

É possível identificar, também, violação ao direito fundamental à inviolabilidade do domicílio e da correspondência, presentes no ordenamento jurídico brasileiro no art. 5.º, XI e inciso XII, ambos da Constituição Federal. Quanto à inviolabilidade do domicílio, SARLET e NETO (2016, p. 547) conceituam a ideia de domicílio de forma mais ampla, como um espaço elementar para o livre desenvolvimento da personalidade:

Quanto ao primeiro ponto (a), ou seja, qual o conceito de domicílio para efeitos da delimitação da proteção com base no art. 5.º, XI, da CF, há que retomar a vinculação da inviolabilidade do domicílio com a proteção da vida privada e garantia do livre desenvolvimento da personalidade. A inviolabilidade do domicílio constitui direito fundamental atribuído às pessoas em consideração à sua dignidade e com o intuito de lhes assegurar um espaço elementar para o livre desenvolvimento de sua personalidade, além de garantir o seu direito de serem deixadas em paz, de tal sorte que a proteção não diz respeito ao direito de posse ou propriedade, mas com a esfera espacial na qual se desenrola e desenvolve a vida privada. Por tal razão, o direito do domicílio, isto é, a garantia de sua inviolabilidade, não implica um direito ao domicílio.

Tal noção corresponde, em termos gerais, ao entendimento dominante na esfera tanto do direito internacional dos direitos humanos, quanto ao que se pratica no direito constitucional comparado, pelo menos, cuidando-se de autênticos Estados Democráticos de Direito. Assim, apenas em caráter ilustrativo, doutrina e jurisprudência constitucional espanhola afirmam a existência de um nexo indissolúvel entre a inviolabilidade do domicílio e o direito à intimidade, que implica, em princípio, um conceito constitucional mais ampliado de domicílio que o convencional conceito jurídico-privado ou mesmo jurídico-administrativo, o que também se constata no caso do direito português e alemão, sempre a privilegiar um conceito amplo de

domicílio e destacando sua conexão com a garantia da dignidade humana e de um espaço indevassável para a fruição da vida privada (SARLET; NETO, 2016, p. 547).

Neste caso, o domicílio seria violado na medida em que certas modalidades de *malware* permitem ativar a câmera ou o microfone do equipamento informático visado, isto é, haveria uma invasão do domicílio mediante meios tecnológicos e virtuais, que captariam conversas e imagens da vida privada, íntima e familiar dos moradores. A inviolabilidade do domicílio é seguramente incompatível com tais mecanismos de proteção da vida humana, no sentido de o investigador poderá monitorar, não só o investigado, em tempo real, mas toda a sua habitação, sem o conhecimento destes (SILVEIRA, 2016, p. 27-28).

Quanto à violação do sigilo das correspondências e dos dados, ocorre no sentido de que não se pode enquadrar o presente caso como uma mera interceptação telefônica, já que esta modalidade demanda que a interceptação ocorra sem a anuência de ambos os interlocutores, e que seja captado somente aquilo que está sendo momentaneamente produzido. Como já mencionado, o meio oculto de provas permite o acesso ao conteúdo já produzido e aquele que está sendo produzido em tempo real, isto é, uma somatória entre o acesso às correspondências e a interceptação telefônica, o que nos permite dizer que esta matéria não estaria abarcada pelas exceções ao inciso XII, do art. 5º da Constituição Federal, ou seja, ausente qualquer aplicabilidade da Lei nº 9296/96.

Posto isso, não obstante vigore no Direito Processual Penal pátrio a regra da não taxatividade dos meios de prova, e, por conseguinte, é admissível a utilização de meios de obtenção da prova não previstos em lei, não se pode admitir qualquer meio de obtenção da prova que ultrapasse os limites constitucionais e legais e corrompa as finalidades da estrutura do processo penal de um Estado democrático de direito (CAMPOS, 2016, p. 66). A título de exemplo CAMPOS (2016, p.67-74), demonstra que no direito comparado, a

exigência de lei específica para o uso do *malware* prevaleceu. Não somente, estas legislações internacionais adotaram como requisito elementar que a Lei traga um rol taxativo de delitos onde se faz possível o uso, aos moldes, no caso brasileiro, da Lei nº 9296/96, bem como, que seja utilizado para um delito já investigado e não para a descoberta de novos delitos. Isto é, com amparo no princípio da proporcionalidade e da subsidiariedade, nunca deve ser utilizado como o primeiro método de obtenção de prova.

Neste íterim, a busca da verdade, a persecução penal, o *ius puiendi* e a realização da justiça têm limites claros impostos pela Constituição, o que obriga especial apreço e respeito pelos direitos fundamentais, a fim de preservar o livre desenvolvimento da personalidade e da dignidade da pessoa humana (SILVEIRA, 2016, p. 33). Conforme será melhor explorado a seguir, não é suficiente que a Constituição chancele exceções e preveja restrições a direitos e garantias constitucionalmente protegidos, bem como, que a Lei regule tais exceções. É necessário, ainda, atender aos ditames do princípio da proporcionalidade e subsidiariedade.

4. O julgamento do RHC 99735/SC como paradigma da jurisprudência brasileira

O julgamento do RHC 99735/SC pode ser visto, na jurisprudência brasileira, como um divisor de águas em relação à matéria do uso do *malware* enquanto instrumento legítimo de prova no processo penal brasileiro. Inicialmente, contudo, é necessário estabelecer de maneira fidedigna, o que o STJ decidiu em relação ao espelhamento do aplicativo de conversas WhatsApp Web. Há uma relevante diferença entre a possibilidade do uso da Lei 9296/96, por meio de ordem judicial, do conteúdo existente no aparelho celular do investigado, com o efetivo acesso da autoridade policial e do espelhamento das conversas existentes por meio do WhatsApp Web, esta vedada pelo STJ.

As razões que levaram o Tribunal da Cidadania a vedar o espelhamento foram as seguintes: no aplicativo WhatsApp Web, o investigador pode alterar as conversas ali presentes, atuando como participante ativo das conversas, gerando dúvidas sobre a fidedignidade do presente no aparelho. Além disso, o investigador pode acessar informações anteriores à autorização judicial (*extunc*) e não apenas as futuras (*ex nunc*), contrariando o princípio da presunção de inocência e, bastando que o aparelho fique em posse do investigador por curto período de tempo, as informações policiais sobre o procedimento realizado seriam consideradas informações absolutas e, diante disso, não passariam pelo crivo do contraditório e da ampla defesa.

No RHC aqui analisado, ficou observado pelo STJ que além da presunção de inocência, esculpida no rol do artigo 5º da Constituição Federal, os delitos informáticos devem ser analisados sob a ótica de uma dupla proteção do ditame da não culpabilidade. Assim fica delimitado:

Primeiro porque a identificação de uma ação delitiva cometida através de um computador apenas identifica o IP (Internet Protocol) da máquina, ou seja, o número identificador daquele dispositivo e daquele acesso à rede. Quando praticada por smartphone, também é identificado pelo número utilizado. Contudo, assim como identificar a arma de fogo não resolve a questão de autoria por ainda ser necessário identificar o responsável pelo disparo do projétil fatal – e a não identificação impede aquela certeza de autoria –, identificar o computador/tecnologia de onde partiram os comandos geradores da violação do bem jurídico nada representa se não se identificar o usuário responsável por eles. Aqui há elevado grau de incertezas. Aparatos normalmente são manipulados por usuários que nele inserem comandos. Assim é a regra. (SYDOW, 2017, p. 303).

Assim o sendo, o uso de provas digitais no processo penal deve ser analisado com cautela, pois é difícil localizar, de maneira precisa e inequívoca, quem de fato estaria enviando determinada mensagem que poderia ser utilizada como evidência da autoria de determinado delito. Esse é o entendimento:

Mas é possível afirmar que a demonstração eficaz de autoria apenas a partir de um dado apenas é bastante frágil. Por isso, identificamos uma importante característica das condutas informáticas denominada Imprecisão de Autoria que pode se dar por defeito na

composição da identidade ou por manipulação da autoria (própria ou por terceiro) (SYDOW, 2017, p. 303).

Postas essas questões, o RHC 99.735 ganhou contornos relevantes para o processo penal informático e relacionam-se com a aplicação do *malware* como instrumento legítimo da produção de provas no processo penal. Nesse sentido, é necessário compreender, conforme o acórdão do STJ assim o fez, que a utilização de instrumentos que permitam à autoridade policial colheita de provas digitais, devem ser lastreadas com irrestrito respeito aos ditames constitucionais da privacidade, intimidade e presunção de inocência.

A legislação penal, por outro lado, não consegue acompanhar os avanços tecnológicos experimentados, em especial na última década. Justamente por isso, cabe ao exegeta uma tarefa hercúlea no sentido de salvaguardar os Direitos e Garantias Fundamentais penais e processuais penais, em uma tarefa hermenêutica que consagre esses avanços, porém não retire da Constituição o seu aspecto protetivo.

Ficou consagrado nesse julgado do Tribunal da Cidadania, o que a doutrina vem denominando de direito probatório de terceira geração, em uma evolução ocorrida na jurisprudência da Suprema Corte dos Estados Unidos (SCOTUS). Nessa geração probatória, a Corte assentou o entendimento de que a proteção constitucional à intimidade e à privacidade não pode ser limitada pelo Estado com o intuito de conseguir provas para o esclarecimento de determinados crimes, dentre os quais ficam destacados os cibernéticos.

O trecho seguinte sedimenta esse entendimento:

Logo, diante de tal conjuntura, concluiu a Suprema Corte que na eventualidade de a autoridade policial pretender utilizar-se de tecnologia até então não disseminada ao uso geral do público, mister se faz a obtenção de prévia autorização judicial, sem a qual tornar-se-á írrita as provas assim angariadas em diligência policial. Dessarte, insere-se nesse cenário as chamadas provas de terceira geração, também denominadas de direito probatório de terceira geração, que engloba as “provas invasivas, altamente tecnológicas, que permitem alcançar conhecimentos e resultados inatingíveis pelos sentidos e pelas técnicas tradicionais” (JACOB; FERREIRA, 2021, p.302).

Contudo, esse entendimento da Suprema Corte Norte-Americana foi construído de maneira gradativa, em um processo de constante evolução da sua jurisprudência. Inicialmente, em um processo da chamada primeira geração probatória, a SCOTUS assentou no caso *Olmstead* (1928) que não é necessária a autorização judicial quando autoridades policiais implementarem aparelhos tecnológicos em locais públicos e, a partir daquela situação, conseguirem elementos probatórios para a elucidação do crime. Nesse sentido, o processo penal ficou atrelado a uma noção de propriedade e não da pessoa humana, malgrado a devassa da propriedade individual por meio dessas tecnologias somente fosse possível através de uma decisão judicial.

Por outro lado, o chamado direito probatório de segunda geração representou um avanço importante na construção jurisprudencial concatenada com os ditames constitucionais. A partir do caso *Katz vs. United States* (1967), no qual foi plantado instrumento tecnológico que captou a conversa em cabine telefônica pública, houve o entendimento de que há no aparelho público em questão, uma legítima expectativa de que a sua intimidade será resguardada. Houve, portanto, invalidação das provas obtidas e uma mudança do paradigma da propriedade para o de proteção da pessoa humana.

Porém, conforme anteriormente mencionado, há a chamada terceira geração probatória, na qual a Suprema Corte entendeu, a partir do caso *Killo* (2001), que as autoridades policiais não podem utilizar, sem autorização judicial, aparelhos tecnológicos que não são acessíveis ao público em geral. O caso em tela é relacionado a *Danny Killo* e às autoridades policiais que desconfiaram de que ele plantava maconha no interior da sua residência. Contudo, os elementos presentes não eram o bastante para que um mandado judicial fosse possível de ser deferido. Nesse sentido, os policiais utilizaram equipamento que mede a radiação do calor das lâmpadas no interior da residência, pois o cultivo de maconha utiliza lâmpadas de alta intensidade.

Ao decidir o caso, a Suprema Corte dos Estados Unidos determinou que no uso da tecnologia para conseguir provas no processo penal, o Estado policial deve sempre agir no sentido de considerar as tecnologias necessárias e acessíveis ao público em geral. Por outro lado, quando o uso de sofisticados equipamentos é imprescindível para uma correta aplicação da lei penal, a autorização judicial é fundamental.

A partir dessas premissas é que o STJ consignou, no RHC 99.735, com alicerce no direito probatório de 3ª geração, que possui como premissa básica a proteção dos Direitos Fundamentais frente à opulência estatal, a impossibilidade, sem autorização judicial, do espelhamento do WhatsApp via QR code e similares.

A Lei das Interceptações Telefônicas (Lei nº 9296/96.), portanto, não guarda relação íntima com o WhatsApp Web, pois a digressão legal não aponta para a possibilidade de tal meio probatório. Logo, pelo princípio da legalidade, falta previsão legal para um uso indiscriminado de elementos tecnológicos de elevada complexidade e invasão dos Direitos e Garantias Fundamentais. O RHC 99.735/SC, portanto, adotou a terceira geração probatória na condução do uso das tecnologias no processo penal e impôs limites constitucionais ao uso desses novos instrumentos a partir de uma leitura constitucional.

5. O novo meio de obtenção de prova: uma breve análise filosófica e constitucional dos desafios do uso do *malware* no processo penal democrático

Uma análise democrática do Direito Penal Informático deve ser sempre construída e pensada na ótica dos Direitos Humanos Fundamentais, com lastro na dignidade da pessoa humana. Nesse sentido específico, ao considerarmos a utilização de programas nos aparelhos eletrônicos com o intuito de produção de provas contra o investigado, é necessário considerar se

houve efetivo respeito à legalidade, à proporcionalidade, à dignidade da pessoa humana e aos demais ditames constitucionais inerentes ao processo penal garantista e democrático.

O combate à impunidade deve ser pautado por elementos concretos e relevantes ao efetivo respeito das formalidades processuais e da efetiva aferição da responsabilidade criminal ao caso concreto. A questão do uso do *malware*, enquanto instrumento legítimo de produção de provas no processo penal, é fruto da pós-modernidade e dos desafios inerentes ao Direito Penal em um processo de adaptação para os desafios das novas tecnologias.

O trecho seguinte abrange o afirmado acima:

Processos e procedimentos existem para imprimir certos valores na confecção de leis e de outros condicionantes estatais da ação humana. Como o Ciberespaço é uma terra sem valores inerentes, capaz de se adequar a qualquer realidade prevista no seu Código, por que não o fazer, naquilo que for possível, conformar-se aos valores previstos na Constituição de 1988(notadamente os direitos fundamentais)? Aqui, por exemplo, a liberdade irrestrita de troca de informações poderia ser restringida na regulamentação das fake news para assegurar a proteção da dignidade humana. Da mesma forma, certas informações de utilidade pública poderiam estar mais facilmente disponíveis aos nossos cidadãos cibernéticos. (ABBOUD, 2019, p. 295).

Fundamental é, a partir dessa breve introdução, realizar uma leitura filosófica e sociológica sobre o atual estado do Direito na contemporaneidade. A leitura da sociedade, para a teoria funcionalista, não pode ser feita a partir de um único mecanismo, seja ele a religião, o Direito, o poder e a economia. Nesse sentido, a sociedade é uma constituição multicêntrica e policontextual, com sistemas que coexistem e concorrem entre si. O Direito, portanto, é apenas um subsistema dentre outros no contexto social. Sendo assim, o Direito irrita e é irritado por outros subsistemas, como o político e o econômico, além de interferir e se acoplar a eles. O Direito não é, portanto, o que determina a lógica e a reprodução de todos os subsistemas com os quais se comunica, com limites e alcances bem mais limitados.

Na modernidade, houve o desencantamento do mundo, afastando a metafísica e a religião como fatores determinantes da vida entre os homens. Já na pós-modernidade, houve um novo desencantamento, pois não é possível mais operar com a certeza, mas sim, somente com a contingência. A contingência pode ser assim qualificada:

Contingente es algo que es como es, pero podría haber sido de otra forma. La contingencia remite a las otras posibilidades y a la necesaria selección. Cada acción realizada por una persona, cada elección atribuible a un sistema, son, entonces, producto de una selección en que ha dejado de lado otras alternativas. Contingencia es – al mismo tiempo – libertad de elección, pero obligación de elegir (RODRIGUEZ, 2001, p. 31).

A seguinte citação esclarece esse ponto:

É a participação nestes procedimentos que determina a legitimidade das decisões e, portanto, a legitimidade dos subsistemas em geral: é tanto inconcebível como impossível que essas decisões sejam ancoradas em valores ou normas compartilhados pela sociedade como um todo. Mas isso significa que Luhmann se desvencilhou de todos os vestígios do normativismo, incluindo aquela característica da teoria do sistema parsoniana, e desferiu um golpe contra todas as análises socialmente críticas, que necessariamente trabalham com conceitos de verdade e justiça. É unicamente a lógica dos subsistemas e dos seus procedimentos específicos que, em última instância, determina a sua estabilidade e dinâmica. Enquanto esses subsistemas são, em princípio, dependentes de seu ambiente, eles apresentam uma dinâmica própria; eles não podem nem ser controlados de fora por objetivos ou valores, nem são dependentes de valores externos (OAS; KNOBL, 2009, p. 346).

O funcionalismo vislumbra uma composição social atomizada, pulverizada na igualdade formal. A sociedade é, diante desse contexto, um organismo onde os homens são as células e a coletividade é marcada por relações específicas, as quais destinam a estabilidade e padronização de condutas. Logo, o funcionamento da estrutura social é garantido por atividades institucionalizadas.

O Direito é um sistema que opera no código legal/ilegal e procura estabelecer expectativas normativas que são diferentes das expectativas cognitivas. As cognitivas são aquelas advindas do conhecimento, mas não admitem desilusão quando determinada lei da física, por exemplo, for desobedecida, obrigando a revisão do conhecimento. Por outro lado, as

expectativas normativas advêm da norma, inclusive as penais, e não admitem o seu descumprimento. A pena ou sanção aparece como um elemento de recuperação da confiança que foi abalada na prática ilegal do infrator.

A teoria da autopoiese, nesse contexto, relaciona-se com o fato do ser humano ou organismo vivo atuar como um sistema operativamente fechado, mas cognitivamente aberto, pois sente os influxos do meio envolvente, isto é, as suas irritações e perturbações, por meio do *input*, que são irritações do meio, cujas respostas são motivadas e medidas de maneira proporcional às irritações advindas do meio envolvente de outros sistemas sociais.

Logo, no sistema penal contemporâneo, os principais fatores de irritação são as transformações de ordem técnica e os novos modos de organização econômica e política que, no contexto de globalização econômica, permitem o surgimento de uma criminalidade transnacional, com efeitos potenciais de largas proporções. O uso do *malware* está incluído nesse processo de irritação do sistema jurídico e deve ser analisado sobre o prisma da Constituição e dos Direitos Fundamentais.

Por outro lado, ao analisarmos os desafios da modernidade, na Teoria da Ação Comunicativa, o Direito é visto como instrumento de poder que regula a economia e as relações sociais, nas quais as possibilidades de emancipação da pessoa humana são mínimas. Avançando em sua proposta, aqui destacado o Direito, o Direito não é apenas um sistema, conforme a teoria funcionalista desenhou, malgrado possa também ser elemento de exercício do poder. Além disso, o Direito conecta demandas sociais ao mundo da vida, tendo o poder de alterá-lo, alinhando propostas de facticidade, ou seja, de coerções existentes à validade que dá legitimidade a demandas sociais.

Nesse sentido, o Direito procedimentaliza processos de discordância e possibilita que no dissenso haja integração social. Hodiernamente, há a construção de um sistema garantidor de liberdades assegurado pela força do Direito objetivo, possuindo o Direito um papel transformador e emancipador da pessoa humana.

A dignidade da pessoa humana possui, nesse contexto, relevância normativa fundamental na construção de um Estado Democrático de Direito e é atualmente positivada em diversas Constituições, como a brasileira, em seus artigos 1º, III e 170, caput da Constituição de 1988. Nesse sentido, a construção da cidadania é dada por elementos norteadores da democracia, capaz de unir o mundo da vida com as demandas sociais legítimas dos grupos vulneráveis.

Nesse sentido:

Somente uma cidadania democrática, que não se fecha num sentido particularista, pode preparar o caminho para um status de cidadão do mundo, que já começa a assumir contornos em comunicações políticas de nível mundial. (...). O estado de cidadão do mundo deixou de ser uma simples quimera, mesmo que ainda estejamos muito longe de atingi-lo. A cidadania em nível nacional e a cidadania em nível mundial formam um *continuum* cujos contornos já podem ser vislumbrados no horizonte (HABERMAS, 1997, p. 304).

Habermas, portanto, defende como vetor democrático, um deslocamento de elementos de poder administrativo e dinheiro para processos públicos autônomos de deliberação e em procedimentos autônomos de formação democrática da opinião e, em especial das vontades políticas, que devem ser institucionalizadas em função do Estado de Direito. Assim o autor se manifesta:

Assim como no modelo liberal, também na teoria do discurso os limites entre o Estado e a sociedade são respeitados; mas aqui a sociedade civil, como a base social de espaços públicos autônomos, distingue-se tanto do sistema da ação econômica quanto da administração pública. E dessa visão da democracia segue-se normativamente a exigência de um deslocamento do centro de gravidade da relação entre os recursos representados pelo dinheiro, pelo poder administrativo e pela solidariedade, dos quais as sociedades modernas se valem para satisfazer sua necessidade de integração e de regulação. As implicações normativas saltam à vista: a força da integração social que tem a solidariedade social, não obstante não mais poder ser extraída somente das fontes da ação comunicativa, deve poder desenvolver-se com base em amplamente diversificados espaços públicos autônomos e em procedimentos de formação democrática da opinião e da vontade políticas, institucionalizadas em termos de Estado de Direito; e, com base no meio do Direito, deve ser capaz de afirmar-se também contra os outros dois poderes- o dinheiro e o poder administrativo (HABERMAS, 1995, p. 48).

A democracia, para Habermas, portanto, pressupõe uma democracia lastreada na participação e deliberação, em busca da razão comum com o intuito de fortalecimento das instituições democráticas. Há, portanto, na construção do sistema jurídico e nas novas formas de tutela da pessoa humana e, mais especificamente, nas garantias processuais penais, o dever de alinhar o combate aos novos desafios da modernidade penal e das suas tecnologias, por meio da legalidade e proporcionalidade a uma escorreita aplicação do sistema constitucional.

Logo, não é vedado, por completo, o uso do *malware* como instrumento apto a produzir provas no processo penal informático. Contudo, o seu uso deve ser lastreado pelas limitações constitucionais e legais, sob pena de desvirtuação do processo constitutivo do sistema jurídico enquanto instrumento de consenso é fundamental para a construção democrática no Brasil.

6. Conclusão

A partir do exposto, observamos que o uso do *malware* é questão ainda polêmica no estudo da prova no processo penal brasileiro. Assim o sendo, é fundamental considerar que a sua aplicação somente pode ser utilizada a partir de fortes balizas constitucionais e jurisprudenciais, pois haveria um desvirtuamento do processo, visando a propriedade em detrimento da dignidade da pessoa humana.

Há, portanto, a possibilidade de aplicação dessa nova tecnologia no ordenamento jurídico brasileiro, em observância da 3ª onda da geração probatória e em irrestrito respeito à legalidade, proporcionalidade e excepcionalidade do caso concreto. Logo, inviável o seu uso irrestrito por parte das autoridades policiais, ao utilizar uma interpretação extensiva da Lei das Interceptações Telefônicas (Lei 9296/36), ao permitir que novas tecnologias,

como o *malware*, sejam aplicadas indistintamente, sem observação escorreita da lei processual. Os desafios dos sistemas do Direito Penal e Processual Penal Moderno não podem ser superiores ao respeito da dignidade humana e da liberdade do homem, bens fundamentais do Estado Democrático de Direito.

Referências

- ABBOUD, Georges. Verdades inconvenientes sobre direito e ciberespaço: uma pequena introdução ao mundo digital. **Revista dos Tribunais**, v. 1000, p. 291-300, 2019.
- ALVES, Daniel Bento. Uso de "malware" em investigação criminal. **Actualidad Jurídica Uriá Menéndez**, España, v. 3, n. 47, p. 19-30, mar./2017.
- BADARÓ, Gustavo. Direito à prova e os limites lógicos de sua admissão: os conceitos de pertinência e relevância. In: BEDAQUE, José R. S.; CINTRA, Lia C. B.; EID, Elie P. (coord.). **Garantismo processual**: garantias constitucionais aplicadas ao processo. Brasília: Gazeta Jurídica, 2016. p. 219-260.
- BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus nº RHC 99.735/SC**. Relator: Laurita Vaz. Brasília, DF, 12 de dezembro de 2018. Diário de Justiça Eletrônico. Brasília.
- CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção da prova em processo penal**. 2019. 139 f. Dissertação (Mestrado) - Curso de Direito, Faculdade de Direito da Universidade de Coimbra, Coimbra, 2018.
- HABERMAS, Jürgen. **Direito e Democracia**: entre facticidade e validade. Rio de Janeiro: Tempo Brasileiro, 1997.
- HABERMAS, Jürgen. Três modelos normativos de democracia. **Lua Nova**: Revista de Cultura e Política, [S.L.], n. 36, 1995.
- JACOB, Muriel Amaral; FERREIRA, Sander Silva. O espelhamento via Qr Code como meio híbrido de obtenção de prova e a sua (i) licitude à luz da Constituição Federal. **Revista da Faculdade de Direito do Sul de Minas**, Pouso Alegre, v. 37, n. 1, p. 285-310, jun./2021.
- LORÊNCIO FILHO, Marco Aurélio Pinto; DENARDI, Eveline Gonçalves. A qualidade do ensino jurídico no Brasil: algumas transformações necessárias. **Revista do Direito**, Santa Cruz do Sul, v. 3, n. 56, p. 106-118, set./2018.
- MARTINEZ, Thiago Hartmann. **Os direitos fundamentais X segurança pública**: a admissibilidade de métodos ocultos de investigação criminal em ambiente digital. 2019. 138 f. Dissertação (Mestrado) - Curso de Direito, Universidade de Lisboa, Lisboa, 2019.
- MENDES, Carlos Hélder C. Furtado. Dado informático como fonte de prova penal confiável(?): apontamentos procedimentais sobre a cadeia de custódia digital. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 61, n. 1, p. 31-61, nov./2019.
- OAS, Hans; KNOBL, Wolfgang. **Teoria Social**: vinte lições introdutórias. Petrópolis: Editora Vozes, 2009.
- OLIVEIRA, Ana Teresa Seabra de. **Obtenção de prova digital**: utilização de malware pelos órgãos da polícia criminal. 2017. 81 f. Dissertação (Mestrado) - Curso de Direito, Universidade do Minho, Braga, 2017.
- RODRIGUEZ, Darío. **La teoría de la sociedad. Invitación a la sociología de Niklas Luhmann**. Santiago do Chile: Metapolítica, 2001.
- SAMPAIO, Tadeu Cincurá de A. S. A importância da metodologia da pesquisa para a produção de conhecimento científico nos cursos de pós-graduação: A singularidade textual dos trabalhos científicos jurídicos. **Revista do Programa de Pós-graduação em Direito da Universidade Federal da Bahia**, v. 23, n. 26, 2013.

SARLET, Ingo Wolfgang; NETO, Jayme Weingartner. A inviolabilidade do domicílio e seus limites: o caso do flagrante delito. **Revista de Direitos Fundamentais e Democracia**, Curitiba, v. 14, n. 14, p. 544-562, jul./dez. 2013.

SERRANO, Manuel Martín. A comunicação na existência da humanidade e de suas sociedades. **Matrizes**, São Paulo, v. 3, n. 1, p. 11-20, 15 dez. 2009.

SILVEIRA, Maria Ana Barroso de Moura da. **Da problemática da investigação criminal em ambiente digital**: em especial, sobre a possibilidade de utilização de *malware* como meio oculto de obtenção de prova. 2016. 49 f. Dissertação (Mestrado) - Curso de Direito, Universidade Católica Portuguesa - Faculdade de Direito - Escola de Lisboa, Lisboa, 2016.

STARR, Adriana Galvão. A dificuldade de acesso ao conteúdo das mensagens ilícitas trocadas via WhatsApp para uso em procedimento de investigação e ação penal. **TRF3 - Caderno de Estudos 1 - Investigação e Prova nos Crimes Cibernéticos**, São Paulo, v. 1, n. 1, p. 7-352, jan./2017.

Artigo recebido em: 22/11/2025.

Aceito para publicação em: 29/11/2025.