Investigação Criminal Tecnológica: perspectivas e limites para infiltração virtual por *malware*

Technological criminal investigation: prospects and limits for virtual infiltration by malware

Investigación criminal tecnológica: perspectivas y límites para la infiltración virtual por malware

Pedro Paulo Pereira Fonseca

Ronaldo De Souza Caldas Bontempo

RESUMO

A presente pesquisa colima analisar, na perspectiva da incidência da tecnologia da informação no processo penal, a possibilidade de utilização, pelo Estado, de *softwares* maliciosos na recolha de dados informáticos, para fins investigativos e probatórios. Nessa visada, será apresentado um panorama histórico da teoria cibernética, até se vulgarizar com a figura do computador e relacionar-se com a era da informação. Vislumbrada a extensão de possibilidade de emprego da tecnologia no âmbito da investigação criminal, focar-se-á, especificamente, no método de infiltração eletrônica através de *software*, estabelecendo suas características, modus de operação, natureza jurídico-processual e a possibilidade de sua admissão no Direito pátrio. Empós, com base na teoria da ponderação ou sopesamento de princípios, o que se propõe é o exame da colisão, gerada pela intrusão virtual, entre, de um lado, a segurança pública e, de outro, os direitos e garantias fundamentais relacionados à privacidade, integralidade de dados e sigilo das comunicações das pessoas investigadas. Para tanto, o trabalho, que se justifica pela atualidade e interdisciplinaridade, vale-se da documentação indireta, marcada pela revisão teórico-bibliográfica. Seguirão, em arremate, considerações críticas, admitindo, de forma excepcional, o método em discussão na investigação criminal brasileira.

PALAVRAS-CHAVE: Investigação criminal. Tecnologia. *Malware*. Proteção de dados.

ABSTRACT

This research seeks to analyze, from the perspective of the incidence from information technology in criminal proceedings, the possibility of use, by the state, of malicious software in the collection of computer data, for investigative and evidentiary purposes. In this view, will be presented a historical overview of cybernetic theory, until it became vulgarized with the figure of the computer and related to the information age. It having envisioned the extent of the possibility of using technology in the context of criminal investigation, it will focus specifically

on, in the method of electronic infiltration through software, establishing its characteristics, modus of operation, juridical-procedural nature and the possibility of its admission in the national law. After, based on the theory of weighting or balancing of principles, it is proposed the examination of the collision, generated by virtual intrusion, between, on one side, public safety and, on the other, the fundamental rights and guarantees related to privacy, completeness of data and secrecy of the communications of the people investigated. Therefore, the work, it is justified by its relevance and interdisciplinarity, makes use of indirect documentation, marked by the theoretical-bibliographic review. They will follow, in conclusion, critical considerations, exceptionally admitting the method under discussion in Brazilian criminal investigation.

KEYWORDS: Criminal investigation. Technology. Malware. Data protection.

1 INTRODUÇÃO

Hodiernamente, a sociedade é marcada pela utilização massiva de recursos tecnológicos, sobretudo conectados à rede mundial de internet. Já na década de 1980, o escritor de ficção William Gibson, na obra *Neuromancer*, apresentava uma visão futurista sobre a interatividade entre pessoas, por meio de máquinas, num novo ambiente: "O ciberespaço (...). Linhas de luz alinhadas que abrangem o universo não-espaço da mente; nebulosas e constelações infindáveis de dados. Como luzes de cidade, retrocedendo..." (1984, p. 25). Se, no início, esse mundo on-line era imaginado apenas para pessoas com apurado conhecimento de programação informática, o tempo mostrou o quanto a sociedade da informação fora influenciada pela cibercultura, a ponto de a internet afigurar-se, hoje, como o mais importante meio de comunicação, acesso à informação e difusão de dados.

Desenvolvida inicialmente em pesquisas militares, a uniformização da linguagem informática, em 1969, possibilitou o surgimento da rede, um meio de trocas de informações escritas, arquivos e programas simples. Em 1989, foi desenvolvida, por Tim Berners-Lee, um sistema de documentos interligados, através da Internet, que mesclava, além de texto e imagem, som e mídia, formando-se um ambiente no qual o usuário conectado poderia navegar através do acionamento de ligações (*links*). Referida tecnologia, denominado de *world wide web*, foi disponibilizada em 1992 e tal foi sua popularização que a rede mundial de computadores atingiu nível global, não sendo possível, atualmente, vislumbrar a sociedade sem a presença da informática e da virtualidade (SYDOW, 2021).

Daí dizer-se em Quarta Revolução Industrial, ou 4.0, representada, a título de exemplo, pela evolução dos aplicativos (de alimentos, turismo, transporte, busca, relacionamento, etc), objetos conectados à rede (IoT), veículos autônomos, quinta geração de comunicações móveis, computação em nuvem e a inteligência artificial (FIGUEIREDO JUNIOR, 2021).

Nesse contexto, percebe-se a aptidão do emprego, na atividade policial, dessas tecnologias, em razão da quantidade de dados que armazenam, para potencializar as investigações criminais, seja na apuração da materialidade de fatos possivelmente delituosos, seja na identificação dos respectivos agentes. Assim, urge a revisão dos métodos tradicionais de elucidação de infrações penais, a fim de que os inquéritos policiais e demais instrumentos investigativos se valham de informações obtidas pelas novas técnicas e recursos, especialmente os relacionados à virtualidade.

Dessarte, em face dos diversos métodos ocultos de investigação no ambiente virtual, o presente trabalho buscou analisar, especificamente, a possibilidade de utilização, pelo Estado, de *softwares* maliciosos para colheita de elementos informativos e provas no âmbito dos procedimentos investigatórios criminais, em cotejo com os impactos que tais instrumentos representam para os direitos fundamentais e garantias processuais, notadamente aqueles voltados à proteção da intimidade e privacidade das pessoas.

Nessa visada, será passado em revista, inicialmente, o desenvolvimento histórico da teoria cibernética, desde seu nascedouro, no primeiro quartel do século XX, até se vulgarizar com a figura do computador e relacionar-se com a era da informação. Empós, dar-se-á realce à nova perspectiva de utilização de técnicas e recursos tecnológicos na investigação criminal, nomeadamente à possibilidade de utilização, pelo Estado, de *softwares* maliciosos (*malware*) para infiltração informática com vistas à obtenção de dados de pessoas investigadas. Posto o problema, seguirão digressões sobre a dificuldade de se considerar tais métodos como medidas cautelares probatórias e, na sequência, o que se propôs foi explorar a ponderação do confronto entre os meios invasivos de investigação e os direitos fundamentais das pessoas, com o intuito de se estabelecer limites à persecução penal tecnológica.

Para tanto, a presente pesquisa, no que toca ao método de abordagem, é de cariz hipotético-dedutivo (MARCONI; LAKATOS, 2003), partindo-se do problema atinente aos requisitos para a utilização de métodos ocultos tecnológicos na investigação, especificamente a infiltração por *softwares* para obtenção de dados da pessoa investigada, estabelecendo-se, como hipótese geral, os preceitos do fundamento existencial do processo penal, qual seja, a instrumentalidade constitucional, para, assim, fixar, provisoriamente, hipóteses relacionadas à natureza jurídico-processual, à admissibilidade probatória e à ponderação com os direitos fundamentais à privacidade e ao sigilo das comunicações.

Já em relação ao método de procedimento e técnica de pesquisa, o trabalho se insere no campo da documentação indireta, marcado pela revisão teórico-bibliográfica, pela qual se

promoverá a colheita de opiniões doutrinárias, com viés interdisciplinar, visando à elaboração de argumentos capazes de comprovar a veracidade ou não das hipóteses (NUNES, 2021).

Como se vê, a perquirição toca em temas relevantes do processo penal, particularmente da investigação criminal. De um prisma, discute-se a eficiência estatal possibilitada pelo emprego de métodos adaptados às novas tecnologias, especialmente da comunicação, e, noutro, as limitações impostas pelos direitos e garantias da pessoa investigada. Resta o estudo, pois, justificado pela atualidade e interdisciplinaridade da matéria versada.

2 INFILTRAÇÃO VIRTUAL POR *MALWARE* COMO MEIO DE OBTENÇÃO DE PROVA NAS INVESTIGAÇÕES CRIMINAIS

2.1 A investigação criminal e o novo panorama do ciberespaço e da sociedade da informação

Falar em investigação criminal é tratar da "reconstrução de fatos passados que pretende responder a quatro perguntas básicas: onde, quando e como ocorreu o fato, e quem o praticou" (GARRIDO; STANGELAND Y REDONDO, 2006, apud PEREIRA, 2010, p. 59), atividade essa que, no sistema processual pátrio, é atribuída, em regra, aos órgãos de polícia judiciária. Cuida-se, assim, de procedimento administrativo, de natureza preparatória, imbuído da função de apurar a autoria e as circunstâncias de um fato, em tese, criminoso, com vistas a lastrear eventual ação penal, cujo principal instrumento é o inquérito policial (GLOECKNER; LOPES JR, 2014).

A legislação processual penal brasileira não imprimiu à investigação preliminar um rigor procedimental, diferentemente de como tratara a fase judicial, de sorte que cabe à autoridade policial, incumbida de sua presidência, proceder às diligências conforme as vicissitudes do caso concreto (LIMA, 2019).

Dada essa discricionariedade, por muitos anos, os depoimentos testemunhais afiguraram-se como os principais elementos informativos colhidos pelas autoridades para alicerçar os inquéritos policiais, o que também se explica pelo fato de que "a pobreza dos meios de investigação e a falta de cientificidade da cultura investigatória fazem com que no Brasil a prova seja essencialmente testemunhal" (LOPES JR, 2021, p. 249).

Denota-se, assim, que os meios investigatórios tradicionais tornam a apuração dos supostos delitos uma tarefa árdua, quando não, falha. Isso porque, na velha lição de Mittermayer (1871), uma vez praticado o crime, o infrator, usualmente, vale-se de todas as precauções para

impossibilitar a produção da prova, fulminar os vestígios e afastar as testemunhas comprometedoras. Daí ser de fulcral importância para o êxito da investigação criminal o aprimoramento dos métodos e o emprego de técnicas adaptadas às novas tecnologias.

Nesse passo, a obsolescência dos meios habituas de investigação revela-se ainda mais gritante em face da evolução tecnológica, máxime relacionada à rede de internet. Por isso, mostra-se indeclinável a análise do desenvolvimento da teoria da cibernética e sua influência na Sociedade da Informação, para que se possa compreender o novo espaço da virtualidade e as perspectivas nele visadas para subsidiar a atividade de apuração de infrações penais.

Os aspectos principais da teoria cibernética foram traçados muito antes do surgimento da própria internet e remontam aos estudos do matemático estadunidense Norbert Wiener. A partir das pesquisas realizadas no *Massachusetts Institute of Technology*, nas quais se buscava o emprego de programação de cálculos em dispositivos de monitoramento de artilharia antiaérea, Wiener formulou a cibernética como a possibilidade de manipular a interatividade de homens e máquinas, através de mecanismos de retroalimentação de informações (*feedback system*). Com isso, os sistemas, dotados de órgãos sensoriais, poderiam aferir e, no caso de desvios, proceder à compensação em relação a um padrão previamente programado e desejado (WIENER, 1954).

Como explica Colli (2021), coube, entretanto, a Gregory Bateson e Margaret Mead a aplicação da cibernética nos sistemas sociais de comunicação. Tais sistemas podem ser compreendidos

> [...] a partir de um procedimento interativo em busca de estabilidade, no qual processos de adaptação se desenvolvem com base na retroalimentação. Esses sistemas respondem aos efeitos do seu próprio feedback, bem como às alterações do ambiente ao qual estão submetidos. Através dos processos de adaptação, por meio de trocas de energia, matéria e informações passam a ser capazes de se auto-organizarem, autorrestringirem e autogovernarem. A cibernética influenciou e possibilitou o desenvolvimento de uma cultura ligada aos meios de comunicação em massa, uma cultura contemporânea que, alavancada pelo avanço da tecnologia da informação e dos recursos informáticos, aproximou, ainda mais, homens e máquinas (COLLI, 2021, p. 27).

É inegável, conforme ressalta Kim (2004), a influência dos princípios regentes da teoria cibernética na cultura moderna, que, mesclados com outros resíduos fornecidos pela tecnologia, traduzem o que pode hoje ser chamado de "cibercultura". A principal característica legada

> [...] foi a visão de que os seres vivos e as máquinas não são essencialmente diferentes. Essa noção se manifesta, em especial, nas tecnologias especializadas em mimetizar a vida (tecnologia da informação, robótica, biônica e nanotecnologia) e nas tecnologias especializadas em manipular a vida (as biotecnologias), onde a relação entre

> organismos e máquina depende intrinsecamente do texto, não só na forma de narrativa cientifica, mas também na forma dos códigos que determinam o funcionamento tanto das máquinas (softwares) como dos seres vivos (o código genético). Os produtos – reais e imaginários – de tais tecnologias podem contradizer certas noções de classificação fundamentais, tais como a oposição entre natureza e cultura, entre orgânico e inorgânico, entre o homem e a máquina, dentre outras (KIM, 2004, p. 2006).

Como produto dessa "cibercultura", e influenciado pelo movimento literário de ficção científica *ciberpunk*, a concepção de cibernética, que outrora fundara suas bases nos estudos de Wiener, restou vulgarizada a partir da década de 1980, dando enfoque para um novo ambiente, o ciberespaço, onde a realidade é virtual e tem no computador seu mediador por excelência (KIM, 2004).

Nessa esteira, Pierre Lévy (1999, p. 17) define o ciberespaço, também chamado de rede, como um novo meio de comunicação, oriundo da interconexão mundial de computadores, que representa não apenas a "infra-estrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo".

Verifica-se, assim, que a concepção desse espaço de virtualidade, marcado pelo fluxo de informações, está intimamente relacionada ao surgimento e desenvolvimento da internet. A rede mundial de computadores foi disponibilizada em 1992 e tamanha sua disseminação que, atualmente, não se pode imaginar a sociedade sem sua presença, trazendo, essa revolução digital, um novo conceito de normalidade (SYDOW, 2021).

Tão massiva é a utilização, não só na comunicação como em qualquer atividade da vida cotidiana, de equipamentos tecnológicos conectados à internet que, hoje, fala-se em Quarta Revolução Industrial, ou 4.0, representada, a título de exemplo, pela evolução dos aplicativos (de alimentos, turismo, transporte, busca, relacionamento, etc.), pelo surgimento de objetos conectados à rede (IoT), de veículos autônomos, da quinta geração de comunicações móveis, computação em nuvem e a inteligência artificial (FIGUEIREDO JUNIOR, 2021).

Essa era da informação globalizada, potencializada pelo espaço da virtualidade, formou um novo "panóptico digital". Aqui, as pessoas se imaginam livres, quando, na verdade, encontram-se interligadas por uma vasta rede, a hipercomunicação, e é este aspecto que, diferentemente do vigia incessante de Bentham, garante o controle da nova sociedade. Nessa lógica, a exposição de dados dos usuários é espontânea e alimenta o sistema (HAN, 2017), como se fosse uma moeda de troca para se ter acesso à rede (CASTELLS, 2003).

Como consequências da virtualidade, operam-se, por assim dizer, os fenômenos da "desterritorialização" e da transformação do tempo, possibilitando às pessoas o estado de quase

ubiquidade. Na percepção de Castells (2002), essa perspectiva é visualizada, por um lado, pela simultaneidade, porquanto propiciada a comunicação e a difusão de informações instantâneas em todo o Globo, e, noutro prisma, pela "intemporalidade", já que as informações da rede são acessíveis independentemente do contexto cultural em que originadas ou da periodização dos acontecimentos históricos. Nessa ordem de ideias, conclui-se que qualquer pessoa que interaja na rede pode ser localizada e alcançada, pouco importando o lugar e o tempo.

Justamente por constatar o vasto horizonte de possibilidades que representa a aplicação dos conhecimentos tecnológicos na apuração de crimes, sobretudo no que se refere à virtualidade e ao acesso a dados, parcela vanguardista da doutrina passou a ver na investigação criminal tecnológica uma nova disciplina, compreendida como

> [...] o conjunto de recursos e procedimentos, baseados na utilização da tecnologia, que possui o intuito de proporcionar uma maior eficácia na investigação criminal, principalmente por intermédio da inteligência cibernética, dos equipamentos e softwares específicos que permitem a análise de grande volume de dados, a identificação de vínculos entre alvos e a obtenção de informações impossíveis de serem agregadas de outra forma, da extração de dados de dispositivos eletrônicos, das novas modalidades de afastamento de sigilo e da utilização de fontes abertas (JORGE, 2021, p. 17).

Dentre as vertentes dessa nova modalidade de investigação, limitar-se-á o presente trabalho à análise, sob o crivo dos direitos fundamentais e garantias processuais, da possibilidade de infiltração informática por *software* para recolha de dados como instrumento de apuração de crimes.

2.2 Infiltração em ambiente digital por *malicious software* (*malware*) e sua admissibilidade na investigação criminal brasileira

A criminalidade revela-se cada vez mais complexa e, via de consequência, mais difícil de ser investigada. Para além dos *cibercrimes* e dos delitos informáticos impróprios – comuns, perpetrados através de meios informáticos (COLLI, 2021) – a comunicação telemática, através, por exemplo, de aplicativos mensageiros acobertados por criptografia ou computação em nuvem, tornou-se palco de interações relacionadas à prática de infrações penais, sem olvidar dos casos em que o acesso a tais meios pode resultar na obtenção de dados relevantes para apuração de crimes, ainda que estes não tenham sido executados por meios tecnológicos. É neste cenário que o emprego de *softwares* "espiões" pelo Estado exsurge-se como uma opção eficiente de método investigativo.

De antemão, cabe esclarecer que, não obstante ser-lhes comum a metodologia de intrusão à distância, o uso de *malware* não se identifica com o "Hacking". Neste, não necessariamente se procede mediante a instalação de *software* em dispositivo informático, já que o acesso remoto é possibilitado pelo emprego da internet e, por conseguinte, o controle sobre o sistema visado se limita ao período em que este estiver conectado à rede. A infiltração por *software*, por seu turno, revela-se mais ampla, prescindindo, inclusive, de conexão à internet (RAMALHO, 2017).

Na ciência da computação, o *software* é compreendido, basicamente, como um ou mais programas que manipula(m) e processa(m) estruturas de dados escritos, para, através de uma sequência de instruções descritas por um algoritmo, ensejar, quando executadas, a realização de uma tarefa pelo computador, com vistas à solução de um problema ou facilitação e segurança das atividades das pessoas (CARVALHO; LORENA, 2017). Tão relevante é o seu papel "que o mundo moderno não poderia existir sem o software. Infraestruturas e serviços nacionais são controlados por sistemas computacionais, e a maioria dos produtos elétricos inclui um computador e um software que o controla" (SOMMERVILLE, 2011, p. 3).

A problemática reside quando o *software* é empregado para fins escusos. O *malware* (aglutinação das palavras *software* malicioso) trata-se, a rigor, de um programa instalado sub-repticiamente em um sistema de processamento de dispositivo informático (*v.g.* smartphone, tablete, notebook), com o fim de quebrar a confidencialidade dos dados nele armazenados, permitindo-se, assim, o portal de acesso remoto (LEITÃO JÚNIOR, 2021).

Basicamente, o controle remoto por *malware* é executado por meio de dois módulos principais. O investigador vale-se de dois programas, um *servidor* e outro *cliente*. O primeiro destina-se a infectar o dispositivo, e, uma vez infiltrado, utiliza-se o segundo programa, cliente, para controlá-lo (TESTAGUZZA, 2018, apud MENDES, 2020).

Como assinalado, a infiltração pode se dar tanto pela internet quanto por acesso físico direto ao *hardware*. Ramalho (2013) arrola três principais modelos de instalação: por suporte físico removível, via *web browser* e por *download* voluntário. Naquele, o *malware* é propagado através de conexão física (*pendrive*, CDs, etc.), geralmente usado para atingir sistemas locais sem acesso à internet, permitindo, assim, a atividade em relação a sistemas específicos e determinados. No segundo modelo, o usuário abre uma página Web que, embora se aparente normal e inofensiva, está composta pelo programa maliciosos, havendo outras vertentes, a exemplo de *download* automático ao tentar clicar em algum *link*, não rara vezes de natureza publicitária. Possível, também, a instalação do *malware* por *download* voluntário, seja por meio

de abertura de anexos de mensagens de correio eletrônico, seja por programas executáveis corrompidos, seja por falsas atualizações de *software* (RAMALHO, 2013).

Existem diversos *softwares* maliciosos desenvolvidos especificamente para infectar dispositivos informáticos. Leitão Júnior (2021, p. 218) lista nove categorias, quais sejam, "(1) cavalos de Tróia; (2) logic bombs; (3) spyware; (4) keylogger e screenlogger; (5) rootkits; (6) vírus; (7) worms; (8) blended threats; e (9) bots entre outros possíveis existentes". Por isso, o meio investigativo de infiltração informática por *malware* é, para fins desse trabalho, compreendido em sentido amplo, não se atendo à determinada espécie ou tipo.

Esses mecanismos podem produzir danos dos mais diversos, como acesso e modificação de dados, obtenção de senhas, criptografia de informações pessoais para fins de extorsão, apenas para ilustrar. Porém, o *malware*, quando utilizado pelo Estado na atividade investigativa "não se propõe a destruir ou danificar dados, mas interceptar e capturar informações importantes à obtenção de provas digitais essenciais ao esclarecimento de crimes graves" (PINHO FILHO, 2022, p. 123).

A eficiência do sobredito método oculto de investigação reside na possibilidade de controle pleno do dispositivo infiltrado. Isso porque permite o acesso remoto, sub-repticiamente e em tempo real, a dados neles armazenados, ademais de poder acessar as várias funcionalidades, como câmera, microfone, memória e geolocalização, ainda que desligadas ou quando não estejam sendo utilizadas pelo usuário. Não bastasse, o *malware* serve para contornar mecanismos de segurança dos dispositivos visados, a exemplo de antivírus e criptografia de comunicações (MENDES, 2020).

Observa-se, dessa maneira, que o método investigativo tecnológico consiste, diferentemente da tradicional colheita de elementos informativos, na captação de dados informáticos do sujeito investigado, sejam armazenados ou transmitidos por dispositivos, sejam em circulação na rede de *internet*.

Na prática, é extensa a amplitude dos atos investigativos com infiltração virtual. O *malware* permite a interceptação e captação de dados telemáticos, monitoramento on-line, captação ambiental com gravação de vídeo e áudio do usuário investigado, assim como acesso à geolocalização dos dispositivos visados (MENDES, 2020).

Em virtude dessa atuação multifacetada, o programa malicioso pode servir como meio de interceptação telemática. No conceito formulado por Sidi (2014, p. 46), considera-se telemática "a comunicação que se realize de forma digital, ou seja, que se utilize da conversão em séries binárias, seja qual fora a infraestrutura de que se utilize, desde que não se enquadre nas modalidades específicas *telefônica* e *telegráfica*". Nessa ótica, a intercepção telemática é

tida como a captação de comunicações contemporâneas, isto é, que ocorrem no exato momento do ato investigativo (SIDI, 2014), medida que já possui previsão no art. 1º, parágrafo único, da Lei nº 9.296, de 24 de julho de 1996 (BRASIL, 1996).

Verifica-se, portanto, que a intrusão por *malware* se assemelha à tradicional interceptação telemática (passiva), na medida em que apreende em tempo real as comunicações, porém, a distinção é visível no *modus*, já que a captação das informações receptadas, geralmente criptografadas, ocorre internamente no dispositivo visado, após a decodificação (MENDES, 2020).

Outra linha investigativa possibilitada é a interceptação entre presentes. O acionamento, remota e insidiosamente, do microfone e câmera do dispositivo informático visado, possibilitando ao investigador a recolha de comunicação e sinais ópticos da pessoa investigada, técnica conhecida como *Roving Bug* (SIDI, 2014), é uma realidade e pode ser operada por meio de *malware* específico, como demonstram Farley e Wang (2010). Assim empregado, o *software* possibilitaria o que Arantes Filho (2011) conceituou de *interceptação de comunicação entre pessoas presentes*, medida investigativa relacionada à captação ambiental prevista na Lei nº 12.850/2013 (Lei de Organizações Criminosas), embora dela se distinga, no particular da infiltração virtual, por não se tratar, a depender do dispositivo alvo, de um ponto fixo de captação, mas de verdadeira monitoração itinerante (MENDES, 2020).

De igual modo, o "vírus" espião do Estado é capaz permitir ao investigador, de forma remota, a recolha de dados informáticos do agente alvo. Interessante destacar que a captação pode se dar em relação tanto aos dados armazenados no dispositivo quanto àqueles dispostos em "nuvem" (PINHO FILHO, 2022). Trata-se, por assim dizer, de uma busca e apreensão virtual, que dispensa a apoderação do suporte físico.

Noutro giro, a intrusão é capaz de facilitar as investigações através de acesso à geolocalização do dispositivo informático alvo. Com a disseminação da tecnologia móvel, a obtenção do posicionamento espaço temporal do dispositivo infiltrado acaba por representar a monitoração, a todo momento, do lugar onde se encontra o usuário (MENDES, 2020).

São essas as principais linhas investigativas contempladas pela tecnoinvestigação por *malware*. Reprise-se o fato de se tratar de recurso multiforme que, na prática, pode assumir várias outras funcionalidades, que são aperfeiçoadas à medida que se avança e desenvolve-se a tecnologia de *software*. Os métodos acima descritos foram invocados porque, em maior ou menor medida, assemelham-se a institutos e meios investigativos já disciplinados pelo ordenamento brasileiro (interceptação telemática, captação ambiental, etc.).

Com efeito, o uso de *malware* a serviço do Estado confere eficiência à atividade investigativa, mas, em razão de seu alto grau de ingerência na privacidade das pessoas, a adoção de tal inovação técnica no processo penal não escapa de uma principal indagação: se é admissível sua utilização no ordenamento jurídico-penal brasileiro.

No ponto, é patente a carência de regras legais específicas. Atualmente, revela-se necessário, como pontua Leitão Júnior (2021), o emprego da analogia, confluindo dispositivos como, por exemplo, da Lei de Intercepção Telefônica e da Lei do Marco Civil da Internet, muito embora inexistam critérios concretos para nortear a intrusão por *malware*. Para o autor, seja qual for o paradigma adotado, a prévia autorização judicial é exigência inderrogável, submetendo-se, pois, sua utilização à cláusula de reserva da jurisdição.

A ausência de previsão legal expressa e específica não impede, contudo, inovações técnicas na investigação criminal, a exemplo da intrusão virtual. De fato, o art. 3º do Código de Processo Penal admite tanto a interpretação extensiva como a aplicação analógica das normas. Assim, poderia o questionamento parecer de fácil resolução, pois o *malware* como instrumento persecutório do Estado, a depender do modo empregado, aproxima-se de métodos ocultos de investigação já disciplinados no ordenamento brasileiro, a exemplo da intercepção telefônica, que possui lei própria, e da captação ambiental, tratada na Lei de Organização Criminosa.

Todavia, pela acentuada intromissão na esfera privada das pessoas, a analogia, no âmbito da investigação criminal, não pode ser empregada indiscriminadamente. Impositivo, assim, o estabelecimento, em matéria de métodos ocultos de investigação, de um modelo teórico de harmonização entre a admissão de inovações tecnológicas e os direitos fundamentais, "que não lhes tire a necessária dinamicidade, mas que tampouco abra espaço para o descontrole do Estado-Persecutor" (SOARES, 2014, p. 254).

Nesse caminho, Soares (2014) propõe uma limitação material e temporal para as inovações técnicas e tecnológicas – no que se insere a infiltração virtual -, tomando como centro de sua tese que:

> [...] é tolerável a adoção de inovação investigativa sem satisfatória regulamentação jurídica, ainda que cause significativo impacto em direitos fundamentais, desde que, obedecido o mandamento da proporcionalidade, seja compensado seu déficit de regulamentação por método judicial que a trate como *praeter legem*, expecional, temporária, decorrente de interpretação extensiva ou aplicação analógica e inserida em contexto de evolução legislativa progressiva (SOARES, 2014, p. 270).

O referido autor parte da constatação de que, em se tratando de medidas investigativas, as inovações enfrentam, primeiro, uma experimentação prática e, quando producentes, tornam-

se recorrentes na atividade persecutória, passando a ser objeto de decisões judiciais, geralmente sem disciplina legal específica, e da doutrina. Disso, surgem os primeiros problemas jurídicos, fazendo com que o Legislativo verse sobre a matéria, inicialmente de forma tímida, para, só depois da maturação dos institutos, receberem densidade normativa. Foi o que aconteceu, por exemplo, com o acesso a dados telefônicos e financeiros, ação controlada e infiltração de agentes, meios extraordinários de investigação que são, hoje, disciplinados legalmente, mas que se originaram na prática (SOARES, 2014).

Esse processo dinâmico de incremento deve ser, porém, limitado material e temporalmente. As inovações tecnológicas na investigação criminal, dada a compressão de direitos fundamentais, podem ser apenas *praeter legem*, isto é, como forma de integrar lacunas legislativas, jamais para violar dispositivos legais, restringindo-se, assim, à aplicação analógica e à interpretação extensiva. Ademais, a utilização de tais medidas, que são total ou parcialmente atípicas, é tida como excepcional, devendo passar por rígido controle judicial (a ponderação entre direitos fundamentais, relevante para a decisão judicial em casos tais, será examinada no subitem 2.4, infra), de modo a serem admitidas tão somente quando outros meios se mostrarem, no caso concreto, insuficientes, impondo, igualmente, a modulação temporal, numa perspectiva de tipificação processual progressiva. Portanto, a abertura para inovação dos meios investigativos é marcada pela excepcionalidade e provisoriedade, a fim de que o atraso legislativo não obstaculize a atividade persecutória estatal (SOARES, 2014).

Nessa ordem de ideais, pode-se afirmar que, a despeito da ausência de previsão expressa, será cabível o emprego da medida de infiltração virtual, por controle judicial casuístico, quando, concretamente, não houver outros meios capazes de permitir a apuração de crimes, desde que respeitadas, como regulamentação paradigma, as normas constitucionais e legais disciplinadoras dos institutos semelhantes, sobretudo quanto à reserva de jurisdição, como da interceptação telemática, captação ambiental, infiltração virtual de agentes, busca e apreensão, o que dependerá do *modus* de operação do *malware* (PINHO FILHO, 2022).

2.3 Natureza jurídico-processual e eficácia probatória da infiltração virtual

Para entender a natureza jurídica da infiltração virtual por *malware*, assim como as consequências, no processo penal, do material por ela obtido, revela-se premente distinguir os conceitos de fonte de prova, meios de prova e métodos de investigação/obtenção de prova.

De antemão, oportuno consignar que o termo prova, no vocabulário jurídico brasileiro, é plurívoco. Tecnicamente, pode ser conceituada como: a) a atividade realizada pelos sujeitos

processais, em regra, pelas partes, com o objetivo de demonstrar suas alegações; b) os meios ou instrumentos empregados para a comprovação de uma asserção ou de um fato; c) o resultado final da atividade probatória, isto é, a formação da convicção do órgão julgador, seu destinatário. Logo, distinta será a acepção de prova conforme o sentido empregado (BONFIM, 2019).

Nessa senda, cabe diferenciar o meio de prova do meio de obtenção (ou investigação) de prova. Por aquele, na dicção de Tourinho Filho (2010, p. 555), entende-se "tudo quanto possa servir, direta ou indiretamente, à comprovação da verdade que se procura no processo: testemunha, documento, perícia, informação da vítima, reconhecimento, tudo são meios de prova". Trata-se, pois, de atividade realizada, em regra, no bojo do processo criminal e, excepcionalmente, na fase investigatória, com a participação dialética das partes.

Por outro vértice, os meios de obtenção de prova ou de investigação da prova, na lição de Lima (2019, p. 612), "referem-se a certos procedimentos (em regra, extraprocessuais) regulados por lei, com o objetivo de conseguir provas materiais, e que podem ser realizados por outros funcionários que não o juiz (v.g., policiais)". Aqui, diferentemente da categoria anterior, o objeto é a descoberta de fontes materiais de prova, de modo que seus resultados que poderão funcionar como meios de prova.

Passados em revista tais conceitos, e para melhor compreender a posição epistêmica de cada qual no âmbito do processo penal, impõe-se o exame de um outro, *fonte de prova*. Este diz respeito a tudo que, derivado do fato supostamente delituoso, possa servir para esclarecê-lo, independentemente de processo, como, a título de exemplo, as pessoas que presenciaram a prática de determinada infração (LIMA, 2019). Cuida-se, na síntese de Tourinho Filho (2010, p. 555), de "tudo quanto possa ministrar indicações úteis, cujas comprovações sejam necessárias". Denota-se, assim, que os meios de prova servem para introduzir no processo judicial penal as fontes de prova, ao passo que os métodos de obtenção de prova visam à descoberta destas.

A doutrina classifica os meios de obtenção de prova em ordinários e extraordinários, conforme a grau de compressão de direitos e garantias do investigado. Os ordinários seriam aqueles aplicáveis para infrações de qualquer gravidade, como a busca domiciliar (ARANTES FILHO, 2011). Já os meios extraordinários, também denominados de técnicas especiais de investigação:

> [...] são as ferramentas sigilosas postas à disposição da Polícia, dos órgãos de inteligência e do Ministério Pública para a apuração e a persecução de crimes graves, que exigem o emprego de estratégias investigativas distintas das tradicionais, que se baseiam normalmente em prova documental ou testemunhal. [...] São identificados, em regra, pela presença de dois elementos: o sigilo e a dissimulação. Por meio deles,

> são coletadas informações, indícios ou prova de um crime sem o conhecimento do investigado, de modo a proporcionar aos órgãos estatais o fator surpresa. Nesse caso, o contraditório será exercido apenas de maneira diferida. Nesse grupo de técnicas sigilosas estão incluídas a interceptação das comunicações telefônicas, a ação controlada, etc. (LIMA, 2019, p. 613).

Há, ainda, a classificação dos citados métodos em abertos e ocultos. Os segundos "consistem na obtenção dos elementos comprovativos da existência da prática de um ilícito penal por parte do arguido, sem que este tenha conhecimento de que é alvo dessas diligências probatórias" (FURTADO, 2020, p. 9).

No caso específico da infiltração por *malware*, em razão do seu potencial multiforme, como discorrido acima, surge a dificuldade de estabelecer sua natureza jurídica. Foi visto que tal instrumento possibilita a interceptação, o monitoramento e a captação da atividade do usuário visado, tudo de forma insidiosa. Com isso, resta claro, à luz das classificações supramencionadas, que tal instituto se enquadra na categoria de meios ocultos extraordinários de obtenção/investigação de prova.

Necessário ponderar, outrossim, que, na atual conjuntura tecnológica, não há recursos para admitir, com segurança, a invasão por *software* como uma medida cautelar probatória. Isso porque, consoante advertência de Mendes (2020), é quase inacessível a comprovação da confiabilidade e integralidade dos dados coletados remotamente pelo *malware*, notadamente pelo risco que tal método gera de alteração das configurações do sistema invadido, além de ainda não haver mecanismos consolidados de preservação da cadeia de custódia da prova digital. Nessa ótica, o material recolhido não pode ser tido como elemento de prova em si, mas, antes, o caminho para se chegar a este, enquadrando-se, assim, como meio extraordinário de obtenção de prova ou meio oculto de investigação.

Um exemplo da dificuldade de aferir a integralidade dos dados colhidos é o caso de acesso a aplicativos de mensagens. No particular da observação de conversas pelo *WhatsApp Web*, que nem exige *malware*, mas pode ser feito por mero espelhamento conferido pela própria plataforma, há a possibilidade de o terceiro interagir diretamente na comunicação e excluir, sem deixar vestígios, mensagens, inclusive passadas, o que fulminaria a possibilidade de contraprova pelo investigado, como comenta Lima:

> Por mais que os atos praticados por servidores públicos gozem de presunção de legitimidade, doutrina e jurisprudência reconhecem que se trata de presunção relativa, que pode ser ilidida por contraprova apresentada pelo particular. Não é o caso, todavia, do espelhamento: o fato de eventual exclusão de mensagens enviadas (na modalidade "Apagar para mim") ou recebidas (em qualquer caso) não deixar absolutamente nenhum vestígio nem para o usuário nem para o destinatário, e o fato de tais mensagens excluídas, em razão da criptografia *end-to-end*, não ficarem armazenadas

> em nenhum servidor, constituem fundamentos suficientes para a conclusão de que a admissão de tal meio de obtenção de prova implicaria indevida presunção absoluta de legitimidade dos atos dos investigadores, dado que exigir contraposição idônea por parte do investigado seria equivalente a demandar-lhe produção de prova diabólica (o que não ocorre em caso de intercepção telefônica, não qual se oportuna a realização de perícia) (LIMA, 2020, p. 552).

Destarte, constata-se que o material colhido através do método oculto de investigação não possui valor probatório. Ainda que admitido, excepcionalmente, como já visto, é de rigor a cautela de se restringir sua função à identificação das fontes de prova, cingindo-se à fase de investigação preliminar. Por decorrência, seus resultados não têm os atributos da prova e, destarte, o condão de serem transferidos ao processo judicial com validade para, por si sós, lastrear a procedência de uma pretensão punitiva.

2.4 Ponderação de Direitos Fundamentais – Segurança Pública *versus* Privacidade

Se, de um lado, é notória a eficiência do meio de investigação debatido, noutro, não se pode olvidar da sua incidência nos direitos fundamentais do investigado. São eles a proteção da privacidade, do sigilo das comunicações e da integridade dos dados informáticos.

Positivado expressamente no art. 5º, X, da Constituição Federal, "o direito à privacidade, em sentido mais estrito, conduz a pretensão do indivíduo de não ser foco da observação por terceiros, de não ter os seus assuntos, informações pessoais e características particulares expostas a terceiros ou ao público em geral" (MENDES; BRANCO, 2019, p. 288). Corolário desse direito e também de envergadura constitucional, conforme lição de Mendes e Branco (2019), tem-se o sigilo das comunicações telegráficas, de dados e telefônicas, que traduz o direito à confidencialidade, do emissor, de escolher o destinatário do conteúdo da sua comunicação.

Na mesma ótica, a proteção da integridade dos dados relaciona-se com a autonomia informativa dos respectivos titulares e com o necessário controle que estes precisam manter sobre os seus próprios dados. Ademais, trata-se de proteção a acessos indevidos, à modificação de dados por terceiros, bem como sua utilização não autorizada (SYDOW, 2021).

É certo que não existem direitos absolutos e, por essa razão, não se mostra razoável que dispositivos informáticos sirvam de manta para acobertar a prática de crimes ou obstar sua elucidação (LEITÃO JÚNIOR, 2021). Nessa perspectiva, restaria legitimada a infiltração por *software*, como método de investigação criminal, quando, no caso concreto, o interesse público

na apuração e repressão da criminalidade se revelar preponderante em face do direito individual à privacidade e à proteção de dados.

Não se pode, porém, perder de vista o fundamento de existência do processo penal, a saber, a "instrumentalidade constitucional". No escólio de Lopes Jr. (2021), referida instrumentalidade se presta a possibilitar o maior grau de eficácia dos direitos e garantias fundamentais insculpidos na Constituição Federal, tomando-se por norte o princípio da dignidade da pessoa humana, com vistas a sofrear o poder punitivo do Estado. Em harmonização com tal leitura, torna-se evidente que a autorização para o emprego do *malware*, a despeito de se tratar de medida atípica, exige o estabelecimento de critérios rígidos para pautar a decisão judicial, a fim de não traduzir discricionária compressão de direitos do investigado.

Destaque-se, de logo, que muitos dos direitos fundamentais se apresentam, quanto à estrutura normativa, na forma de princípios jurídicos. Embora ambos sejam espécies de normas, os princípios, diferentemente das regras - que se aplicam de forma disjuntiva (ou é realizada ou não é) -, são tidos como *mandamentos de otimização*, posto que "ordenam que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes" (ALEXY, 2008, p. 90). Tal distinção é relevante, principalmente, para análise de conflito de normas, cujas formas de solução também são diversas.

Disso, vislumbra-se, de modo geral, o caráter relativo dos direitos fundamentais (alguns, evidentemente, não cabem relativização, como direito à vida, vedação da tortura, entre outros). É que estes, enquanto princípios (e que, abstratamente, estão no mesmo nível hierárquico), podem, no caso concreto, colocarem-se em rota de colisão com outros, de sorte que, a depender do contexto fático e jurídico, poderão ser realizados em maior ou menor medida (pesos diferentes), sem, contudo, esvaziar-se o núcleo essencial de cada um. Nessa linha que Canotilho (2003, p. 1273) afirma que "os direitos consideram-se **direitos prima facie** e não direitos definitivos, dependendo a sua radicação subjetiva definitiva da ponderação e da concordância feita em face de determinadas circunstâncias concretas". Não se pode, destarte, dizer, a priori, qual direito prevalecerá no caso de conflito.

Veja-se que, na discussão vertente, é justamente a colisão de princípios de direitos fundamentais que se põem em relevo: a segurança pública de encontro à privacidade, ao sigilo das comunicações e à integridade dos dados informáticos. Como já foi dito, ainda que o método oculto seja admitido com base em regulamentação paradigma, revela-se imprescindível o rígido controle judicial de sua autorização, o que perpassa, obviamente, pela resolução do choque entre os princípios subjacentes.

Para resolver sobreditos conflitos, é recorrente, tanto na doutrina quanto na jurisprudência, a utilização da técnica da ponderação ou sopesamento desenvolvida por Robert Alexy, conquanto esta mesma seja circundada por críticas e abordagens teóricas que escapam dos limites desta pesquisa. Para o renomado jurista alemão, em razão da estrutura de *mandados de otimização* dos princípios, haverá, no caso concreto, pesos diferentes de cada um, de modo que um(ns) prevelerá(ão) sobre outro(s), o que foi sintetizado na sua "Lei de colisão": "as condições sob as quais um princípio tem precedência em face de outro constituem o suporte fático de uma regra que expressa a consequência jurídica do princípio que tem precedência" (ALEXY, 2008, p. 99).

Com vistas à definição da relação de precedência, a ponderação a ser exercida relaciona-se estritamente com a máxima da proporcionalidade, consolidada na jurisprudência do Tribunal Constitucional Federal Alemão. Dela decorre três postulados parciais, examinados nesta ordem: a adequação, necessidade (utilização da medida menos gravosa) e proporcionalidade em sentido estrito (cotejamento entre os ônus impostos e os benefícios almejados; sopesamento propriamente dito) (ALEXY, 2008). Enaltece-se, com tal mecanismo, "o princípio da concordância prática, que se liga ao postulado da unidade da Constituição, incompatível com situações de colisão irredutível de dois direitos por ela consagrados" (MENDES; BRANCO, 2019, p. 184).

O primeiro vetor, a adequação, não traduz dificuldade no exame do *malware*. Isso porque, como já ressaltado, o emprego de programas "espiões" pelos órgãos da persecução penal representa elevado grau de eficiência na apuração de materialidade e autoria de delitos, dada sua metodologia de acessar, remota e insidiosamente, os dados da pessoa visada. Não se enxerga, pois, hipótese em que a medida oculta não seria apta a atingir os fins investigativos.

Atenção especial deve ser, todavia, dispensada ao critério da necessidade. Em virtude da acentuada intromissão na esfera de direitos fundamentais do visado, forçoso concluir que a infiltração por *software* terá cabimento tão somente quando a autoridade postulante (Delegado ou membro do Ministério Público) comprovar que, na hipótese fática, todos os demais meios investigativos, tradicionais e menos invasivos, são insuficientes para garantir o êxito da investigação. Mas, como adverte Silveira (2016, p. 40), a necessidade deve ser aferida tomando-se por referência "um concreto catálogo de infracções criminais que o pretendem legitimar, nomeadamente um catálogo de crimes que se apresentem como suficientemente gravosos, pois como referimos a verdade material não pode ser obtida a qualquer custo".

Num terceiro momento, o que se exige é verificar se a medida é proporcional em sentido estrito, significa dizer, se "o ônus imposto ao sacrificado não sobreleve o benefício que se

pretende obter com a solução" (MENDES; BRACO, 2019, p. 184). Não basta a adequação e a necessidade; demanda, também, o cotejamento entre o bônus atingido (com a prevalência de um direito) e os prejuízos causados (pelo direito preterido), residindo, aqui, o juízo de ponderação propriamente dito.

Nesse estágio, Alexy (2008, p. 167) sintetiza o que chama de "lei do sopesamento", segundo a qual "quanto maior for o grau de não-satisfação ou de afetação de um princípio, tanto maior terá que ser a importância da satisfação do outro". Essa avaliação se desenvolve, num primeiro momento, com o estabelecimento do grau de não realização do princípio tendente a ser relegado no caso; depois, examina-se a importância de se privilegiar o princípio que tende a prevalecer; disso, verifica-se se a importância de satisfazer um princípio justifica a preterição em relação ao outro (ALEXY, 2008).

Como adverte Fonteles (2018, p. 105), é comum que o princípio da proporcionalidade ora tratado seja aplicado, pelos Tribunais, no Direito Processual Penal, inclusive em matéria de restrição de direitos em face de medidas investigativas, porquanto, "com a constitucionalização do Direito, é natural que todos os ramos se sujeitem a uma *hermenêutica constitucional*".

Pois bem, aplicando-se tal raciocínio, chegar-se-á à constatação de que, sob o crivo da proporcionalidade estrita, a utilização de *software* "espião" pelo Estado não pode ocorrer na investigação de qualquer infração penal, senão apenas daquelas com elevadíssimo potencial ofensivo, a exemplo da criminalidade organizada (crime organizado, tráfico, lavagem de capitais, etc.).

Partindo dessas premissas, Barbiero (2021) traz interessante exemplo de aplicação da "lei do sopesamento" para admissão do *malware* como meio investigativo. O autor toma dois tipos de infrações, uma perpetrada por organização criminosa e outra de receptação culposa. De forma escalonada, analisa, respectivamente, o peso abstrato dos princípios no ordenamento (G), o grau de intensidade da intervenção de um direito em outro (I) e, por fim, o grau de importância do direito fundamental justificador da intervenção no caso concreto (S). Em cada etapa, utiliza os conceitos de leve (1), médio (2) e grave (3), para aferição do peso. A ilustração (faz menção, também, ao direito a não incriminação) restou assim esquematizada:

> 1º momento (peso abstrato que têm no ordenamento – G): privacidade (G3), sigilo das comunicações (G3), direto a não incriminação (G3) *versus* tutela da segurança pública (G3);
> 2º momento (grau de intensidade da intervenção de um direito fundamental em outro na hipótese em estudo – implementação de *malwares* – I): privacidade sobre segurança pública (I1), sigilo das comunicações sobre segurança pública (I1), direito a não incriminação sobre segurança pública (I2); segurança pública sobre privacidade

> (I3), segurança pública sobre sigilo das comunicações (I3) e segurança pública sobre direito a não incriminação (I3);
> 3º momento (graduação da importância do direito fundamental justificador da intervenção com base no caso concretamente analisado – S). **Hipótese 1** (receptação culposa): segurança pública sobre privacidade (S1), segurança pública sobre sigilo das comunicações (S1) e segurança pública sobre direito a não incriminação (S1); **hipótese 2** (infrações penais praticadas por organizações criminosas): segurança pública [sobre infrações] complexas e de acentuada gravidade, [assim] como sobre privacidade (S3), segurança pública sobre sigilo das comunicações (S3) e segurança pública sobre direito a não incriminação (S3) (BARBIERO, 2021, p. 146).

Em seguida, o autor conclui sobre o referido quadro:

> Disso resultaria que, na hipótese 1, os direitos individuais (privacidade, sigilo das comunicações, direito a não incriminação) prevalecem sobre a tutela coletiva da segurança pública, cabendo, portanto, ao investigador, valer-se de meios probatórios ordinários e pouco invasivos para alcançar êxito no objetivo investigativo. Já na hipótese 2, a tutela coletiva da segurança pública prevalece sobre dois dos direitos individuais em análise (privacidade e sigilo das comunicações), mas permanece em choque de idêntica intensidade com o direito a não incriminação (BARBIERO, 2021, p. 146).

Na confluência desse referencial teórico, tem-se que a colisão gerada, pela intrusão virtual, entre a tutela da segurança pública e os direitos relacionados à privacidade, todos de cariz fundamental, pode ser resolvida, a partir de um controle judicial casuístico, pela aplicação da máxima da proporcionalidade, em seus três desdobramentos (adequação, necessidade e proporcionalidade em sentido estrito), associada à "lei do sopesamento", de Robert Alexy. Nessa sistemática, patenteia-se que o método oculto em debate poderá ter vez unicamente em casos de criminalidade complexa e de acentuada gravidade, desde que respeitados, igualmente, os parâmetros delineados no subitem 2.2, máxime o balizamento por regulamentação paradigma (hipóteses de admissão, prazos, procedimentos, etc.), a provisoriedade e a excepcionalidade. A não ser assim, só se poderia concluir que o núcleo dos direitos e garantias do investigado estariam a sofrer ilegítima violação, fulminando a dita "instrumentalidade constitucional" do processo penal.

3 À GUISA DE CONCLUSÃO

Ao teor do exposto, vislumbra-se que, na atual conjuntura do desenvolvimento da tecnologia da comunicação, a investigação criminal está a reclamar por novos métodos. Com o aperfeiçoamento e disseminação da telemática, a exemplo dos aplicativos mensageiros acobertados por criptografia ou computação em nuvem, o ciberespaço (ou virtualidade) tornou-se uma vasta fonte de dados pessoais, além figurar como palco de atividades criminosas várias,

estas cada vez mais complexas. Constatou-se, assim, a dificuldade de as medidas investigatórias tradicionais, diante desse cenário, executarem a contento seu mister.

Dentre as inovações técnicas no âmbito da persecução penal, desponta-se, pelo seu elevado grau de eficiência, a utilização, pelo Estado, de infiltração por *malware*. Assim denominado pela aglutinação dos termos *software* malicioso, pode-se entendê-lo como um programa instalado sub-repticiamente em um sistema de processamento de dispositivo informático (*v.g.* smartphone, tablete, notebook), com o escopo de quebrar a confidencialidade dos dados nele armazenados e permitir que estes sejam acessados remotamente.

Cuida-se, por sinal, de método oculto de obtenção de prova em ambiente digital, que se revela extremamente sofisticado e multiforme. Na prática, o programa malicioso permite a interceptação e captação de dados telemáticos, monitoramento on-line, captação ambiental com gravação de vídeo e áudio do usuário investigado, assim como acesso à geolocalização dos dispositivos visados. Poderá se assemelhar, pois, a outros meios investigativos previstos legalmente, como, por exemplo, a captação ambiental e a interceptação telefônica.

No curso da pesquisa, verificou-se que, a despeito da carência de regulamentação legal expressa, o emprego da intrusão virtual poderá ser admitido em situações excepcionais. Para tanto, mostrou-se necessário o rígido controle judicial, a fim de limitar temporal e materialmente a inovação tecnológica, restrita à aplicação analógica e interpretação extensiva dos métodos extraordinários investigatórios já previstos, que servirão como paradigma. Fala-se, desse modo, em tipificação processual progressiva, como forma de admitir ao Estado valer-se de instrumentos eficientes *praeter legem* para tutelar a segurança pública em casos de extrema necessidade, enquanto não haja consolidação legislativa a respeito.

As hipóteses iniciais, quanto à natureza jurídica e à limitação probatória, restaram confirmadas. Ainda que admitida, excepcionalmente, a invasão virtual, forçoso concluir que o material recolhido teria limitada eficácia probatória. É que, na atual conjuntura, a carência de recursos seguros de preservação da integralidade dos dados e da cadeia de custódia da prova digital dificulta a configuração do presente método oculto como meio de prova. Sua natureza jurídica, a rigor, é de meio de investigação de prova, devendo cingir-se, em regra, à fase pré-processual. Por conseguinte, os resultados obtidos não seriam provas propriamente ditas, mas, antes, fontes de prova.

Noutro prisma, dada a compressão de direitos fundamentais gerada pelo *malware*, afigura-se imprescindível a ponderação entre a tutela da segurança pública e a privacidade do investigado, adotando-se, como premissa, a técnica de sopesamento desenvolvida por Robert Alexy. Nessa ótica, o método oculto poderá ser autorizado pelo Poder Judiciário quando, à luz

do caso concreto, revelar-se adequado, necessário e estritamente proporcional, desde que respeitada a regulamentação paradigma e limitada temporalmente. Fora desses parâmetros, a invasão na esfera privada deve ser reputada indevida.

Deflui-se, em arremate, que tanto maior será a possibilidade de restrição de direitos fundamentais quanto mais complexas e graves forem as infrações criminais objeto da investigação, razão pela qual se admite, nos moldes supramencionados, medidas ocultas de investigação sensivelmente invasivas, como a infiltração por *software*, disso não se podendo dizer que estaria a desrespeitar a "instrumentalidade constitucional" da processo penal. Afinal, o ilegítimo é permitir que dispositivos informáticos sirvam de manta para acobertar a prática de crimes ou obstar sua elucidação pelo Estado.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2008.

ARANTES FILHO, Marcio Geraldo Britto. **A interceptação de comunicação entre pessoas presentes como meio de investigação de prova no direito processual penal brasileiro**. 2011. 326 f. Dissertação (Mestrado em Direito Processual) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2011. Disponível em:10.11606/D.2.2011.tde-03092012-090127. Acesso em: 22 nov. 2022.

BABIERO, Diego Roberto. **Implantação de *malwares* em investigações complexas.** Curitiba: Juruá, 2021.

BONFIM, Edilson Mougenot. **Curso de direito processual penal**. 13. ed. São Paulo: Saraiva, 2019.

BRASIL. Presidência da República. **Lei 9.226, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm. Acesso em 10 out. 2022.

CANOTILHO, J.J. Gomes. **Direito Constitucional e Teoria da Constituição**. 7. ed. Coimbra: Almedina, 2003.

CARVALHO, Andre Carlos Ponce de Leon Ferreira de; LORENA, Ana Carolina. **Introdução à computação:** hardware, software e dados. Rio de Janeiro: GEN/LTC, 2017.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Tradução de Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2003.

COLLI, Maciel. **Cibercrimes**: Limites e Perspectivas para a Investigação de Crimes Cibernéticos. 2. ed. Curitiba: Juruá, 2021.

FARLEY, Ryan; WANG, Xinyuan. **Roving Bugnet:** Distributed surveillance threat and mitigation. Comput. Securit, vol. 29, n. 5, p. 592-602, 2010. Disponível em: https://typeset.io/pdf/roving-bugnet-distributed-surveillance-threat-and-mitigation-5e93b9ekhe.pdf. Acesso em: 10 ago. 2022.

FIGUEIREDO JUNIOR, Jorge. Tecnologia Disruptiva e a Investigação Criminal. In: JORGE, Higor Vinicius Nogueira (Coord.). **Tratado de Investigação Criminal Tecnológica**. 2. ed. Salvador: JusPodivm, 2021. p. 123-138.

FONTELES, Samuel Sales. **Hermenêutica Constitucional**. Salvador: JusPodivm, 2018.

FURTADO, Rafael João Barreto. **Os Limites de Utilização do Malware**. 2021. Tese (Doutorado). Universidade de Lisboa, Portugal, 2021. Disponível em: https://repositorio.ul.pt/bitstream/10451/50624/1/ulfd0149686_tese.pdf. Acesso em: 20 ago. 2022.

GIBSON, William. **Neuromancer**. São Paulo: Aleph, 1984.

HAN, Byung-Chul. **A sociedade da transparência.** Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017.

HO KIM, Joon. Cibernética, Ciborgues e Ciberespaço: Notas sobre as origens da cibernética e sua reinvenção cultural. **Horizontes Antropológicos.** Porto Alegre, n. 21, 2004.

JORGE, Higor Vinicius Nogueira (Coord.). **Tratado de Investigação Criminal Tecnológica**. 2. ed. Salvador: JusPodivm, 2021.

LEITÃO JÚNIOR, Joaquim. Bioterrorismo, agroterrorismo, geração e dimensão dos elementos informativos. In: JORGE, Higor Vinicius Nogueira (Coord.). **Tratado de Investigação Criminal Tecnológica**. 2. ed. Salvador: JusPodivm, 2021. p. 211-272.

LEVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu da Costa. São Paulo: Ed. 34, 1999.

LIMA, Renato Brasileiro de. **Legislação Criminal Especial Comentada:** volume único. 8. ed. Salvador: JusPodivm, 2020.

_____. **Manual de Processo Penal**: volume único. 7. ed. Salvador: JusPodivm, 2019.

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

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos da Metodologia Científica**. 5. ed. São Paulo: Atlas, 2003.

MENDES, Carlos Hélder Carvalho Furtado. **Tecnoinvestigação criminal:** entre a proteção de dados e a infiltração por *software*. Salvador: JusPodivm, 2020.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet Branco. **Curso de Direito Constitucional**. 14. ed. São Paulo: Saraiva, 2019.

MITTERMAYER, C. J. A. **Tratado da Prova em Matéria Criminal.** Tradução de Alberto Antônio Soares. Rio de Janeiro: Editor A. A. da Cruz Coutinho, 1871.

NUNES, Rizzatto. **Manual da Monografia Jurídica**. 14. ed. Salvador: JusPodivm, 2021.
PINHO FILHO, Ossian Bezerra. **Investigação criminal tecnológica**: infiltração por *Malware* nas investigações informáticas. Curitiba: Juruá, 2022.

PEREIRA, Eliomar da Silva. **Teoria da Investigação Criminal**: Uma introdução jurídico-científica. São Paulo: Almedina, 2010.

RAMALHO, D. S. O uso de *malware* como meio de obtenção de prova em processo penal. **Revista de Concorrência e Regulação**, n. 16, p. 195-244, 2013.

_____. **Métodos Ocultos de Investigação Criminal em Ambiente Digital.** Coimbra: Almedina, 2017.

SILVA, R. S. M. **A interceptação das comunicações telemáticas no processo penal.** Orientador: Marcus Alexandre Coelho Zilli. 2014. 266 f. Dissertação (Mestrado) - – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2014. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2137/tde-04032015-082717/publico/Ricardo_Sidi_Dissertacao_Mestrado_Integral.pdf. Acesso em: 10 nov. 2022.

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. 2017. 52 f. Tese de Doutorado. Universidade Católica Portuguesa, Faculdade de Direito, Escola de Lisboa, Lisboa, Portugal, 2017. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/21854/1/Tese%20final%2028%20Mar%C3%A7o.pdf. Acesso em: 10 ago. 2022.

SOARES. Gustavo Torres. **Investigação criminal e inovações técnicas e tecnológicas**: perspectivas e limites. Orientador: Antônio Scarance Fernandes. 2014. 307 f. Tese (Doutorado) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2014. Disponível em:https://www.teses.usp.br/teses/disponiveis/2/2137/tde30112015165420/publico/Versao_integral_Gustavo_Torres_Soares.pdf. Acesso em: 10 nov. 2022.

SOMMERVILLE, Ian. **Engenharia de Software**. Tradução de Ivan Bosnic e Kalinka G. de O. Gonçalves; revisão de técnica Kechi Hirama. 9. ed. São Paulo: Pearson Prentice Hall, 2011.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático:** Partes Geral e Especial. 2. ed. Salvador: JusPodivm, 2021.

TOURINHO FILHO, Fernando da Costa. **Manual de processo penal**. 13. ed. São Paulo: Saraiva, 2010.

WIENER, Norbert. **Cibernética e Sociedade**: O Uso Humano de Seres Humanos. Tradução de José Paulo Paes. 2. ed. São Paulo: Cultrix, 1954.