✲✲✲

Dossiê - Investigação Criminal e Novas Tecnologias para Obtenção de Prova

✲✲✲

Hacking e Infiltração Policiais em Resposta ao Uso de Criptografia por Organizações Criminosas

Caio Porto Ferreira
Polícia Federal - SP
University of East London (UEL)

RESUMO

O crime organizado atualmente navega por águas tranquilas quando o assunto é segurança em suas comunicações. Amparados pela recalcitrância das Big Techs, os envolvidos em atividades criminosas usufruem de aplicativos de comunicação com tecnologia de criptografia, para organizar e expandir suas atividades no Brasil e no mundo. Neste ínterim, órgãos responsáveis pela investigação criminal se esforçam para desenvolver e aplicar novas tecnologias para obtenção de prova, que comumente são consideradas invasivas ou ilegais, não por afrontar direitos e garantias fundamentais, mas sobretudo pela falta de conhecimento de certos segmentos da sociedade acerca da importância da atividade de inteligência para proteção e promoção de Estados democráticos e livres.

Palavras-chave: Investigação criminal. Obtenção de prova. Interceptação das comunicações. Criptografia. Privacidade.

Introdução

Em 28/05/2020 foi realizada sessão virtual do Supremo Tribunal Federal – STF em que o ministro Edson Fachin, relator da Arguição de Descumprimento de Preceito Fundamental 403, proferiu voto no sentido de julgar procedente a ação, para declarar a inconstitucionalidade parcial sem redução de texto, de dispositivos da Lei 12.965/2014, "de modo a afastar qualquer interpretação do dispositivo que autorize ordem judicial que exija acesso excepcional a conteúdo de mensagem criptografada ponta-a-ponta ou que, por qualquer outro

Recebido em 16 de fevereiro de 2021.
Aceito em 07 de maio de 2021.
Brasília, v. 12, n. 5, p. 19-48 , mai/ago. 2021
ISSN 2178-0013
ISSN Eletrônico 2318-6917

meio, enfraqueça a proteção criptográfica de aplicações de internet." Na mesma sessão, a ministra Rosa Weber também inaugurou o julgamento da Ação Declaratória de Inconstitucionalidade 5527, que guarda similaridade com o tema e visa a declarar a inconstitucionalidade de dispositivos do chamado Marco Civil da Internet.

As duas ações foram propostas no STF para desafiarem duas decisões judiciais, uma proferida pelo Juiz de Direito da Vara Criminal da Comarca de Lagarto / SE, que deu origem à ADPF 403 / SE, e a outra proferida pelo juízo da 2ª Vara Criminal da Comarca de Duque de Caxias / RJ, que por sua vez deu origem a ADI 5527. As ordens judiciais determinavam inicialmente a interceptação em tempo real das mensagens entre membros das organizações criminosas. Com o descumprimento, os magistrados arbitraram multa diária, que também não foi suficiente para compelir a empresa de tecnologia que administra o aplicativo de mensagens instantâneas a colaborar com as investigações. Assim, não restou uma alternativa a não ser determinar a suspensão temporária do aplicativo com base no art. 12, inciso III, da Lei 12.965/2014.

A metodologia empregada pelo ministro Edson Fachin e pela ministra Rosa Weber foi a da dialética entre o STF e a sociedade, ao convocarem audiências públicas que foram realizadas nos dias 02/06/2017 e 05/06/2017. Órgãos públicos e entidades da sociedade civil tiveram a oportunidade de expor suas ideias e argumentos em defesa da inviolabilidade da criptografia ou da necessidade de acesso pelos órgãos de investigação e persecução penal às mensagens em tempo real de investigados. Muito embora a Polícia Federal tenha sido bem representada e tenha apresentado ideias e argumentos técnicos que justificavam a necessidade de acesso excepcional às comunicações telemáticas dos suspeitos de crimes graves, o tempo conferido à instituição foi insuficiente para abordar questão tão complexa. Este artigo tem como objetivo colaborar com o debate e acrescentar argumentos técnicos, científicos e jurídicos que podem ajudar operadores do direito a compreender melhor a questão.

Do voto do relator da ADPF 403[1]

Inicialmente, o ministro Fachin assentou que as premissas de seu voto levavam em conta o impacto tecnológico na sociedade e a necessidade de atualizar o alcance dos direitos e garantias fundamentais. Nesse sentido, estabeleceu que direitos digitais são direitos fundamentais e que o direito à privacidade e à liberdade de expressão nas comunicações devem ser protegidos para o pleno exercício do direito de acesso à internet.

Compreende sua Excelência que a criptografia e o anonimato são especialmente úteis para o desenvolvimento e compartilhamento de opiniões e que aquela seria um meio de assegurar a proteção de direitos que, em uma sociedade democrática, são essenciais para a liberdade civil. Por fim, declarou que é contraditório, em sua opinião, que em nome da segurança pública se deixe de promover e buscar uma internet mais segura, afastando medidas que poderiam trazer insegurança para os usuários, que "somente se justificam se houver certeza comparável aos ganhos obtidos em outras áreas" (STF, 2020).

O relator ressaltou que temas do mundo virtual, exemplificando o tema 533 (dever da empresa hospedeira de fiscalizar e remover conteúdo ofensivo sem intervenção do judiciário) ou o tema 977 acerca da licitude do acesso a informações contidas em aparelho celular, entre outros, não seriam abrangidos pelo voto proferido. Mesmo sua Excelência fazendo essa ressalva, entende -se que a solução final proposta pelo relator poderá ter impactos desfavoráveis e limitativos no que tange às ferramentas investigativas.

Quanto ao mérito, o Ministro Edson Fachin assentou que o objeto da Arguição de Descumprimento de Preceito Fundamental 403 é (i) "saber se é constitucional a ordem judicial de acesso por órgãos do Estado ao conteúdo de comunicações protegidas por criptografia, conforme previsão constante do art. 7º, II, do Marco Civil da Internet; e, em sendo constitucional, (ii) "saber se a sanção prevista no inciso III do art. 12 do mesmo diploma legal pode ser aplicada pelo Poder Judiciário" (STF, 2020, p. 53).

1 Arguição de Descumprimento de Preceito Fundamental (ADPF) 403, Relator ministro Edson Fachin, requerente Cidadania, Intimado Juiz de Direito da Vara Criminal da Comarca de Lagarto / SE, processo único 4000331-63.2016.1.00.0000.

Para o ministro, o voto proferido teria duas vertentes: a primeira com um olhar voltado aos direitos envolvidos e a segunda preocupada com "a intensidade de interferência neles causada a partir de possíveis alterações no modelo de criptografia adotado pelo *WhatsApp*" (STF, 2020, p. 55). Ao abordar o direito de expressão, reconheceu que todos os ordenamentos constitucionais compreendem que não existem direitos absolutos, devendo estes direitos serem sopesados à luz da "necessidade e interesse público" (segurança nacional etc.) (STF, 2020, p. 64). Relatou que os órgãos de segurança pública e a Procuradoria-Geral da República apontam que o acesso excepcional garante aos agentes de investigação um mecanismo indispensável para a consecução de suas atividades de investigação em casos graves (STF, 2020, p. 53).

O ministro Fachin, acompanhando opinião defendida na audiência pública, sugere que eventual "acesso excepcional de um aplicativo faria com que os usuários migrassem em direção a outros, mais seguros" (STF, 2020, p. 70), acompanhando a tese que criminosos optariam por "sistemas ainda mais restritos, ainda mais difíceis de serem rastreados" (STF, 2020, p. 71), quando não sistemas ilegais. Contudo, tal hipótese comumente não ocorre na prática. O indivíduo envolvido com atividades típicas de organização criminosa, antes de criminoso, é um ser sociável como um cidadão comum. Ele se relaciona com familiares, amigos, redes de interação social de seu interesse, muitas vezes utiliza aplicativos de mobilidade urbana, comércio eletrônico, entre outros, e, principalmente, interage intensamente com os membros da organização criminosa. Por mais que paire algum risco de conhecimento sobre suas comunicações, o suspeito continuará utilizando o aplicativo de comunicação instantânea, que no momento é o *WhatsApp*, pela conveniência de ter em uma ferramenta acesso a todas as pessoas que interagem em seu círculo social.

Esse acesso excepcional é importante sim, e muito, para os órgãos de investigação. Ademais, caso identificada a migração para outros aplicativos, caberá à polícia e ao Ministério Público – MP diligenciar no sentido de representar e implementar as medidas necessárias para prosseguir no monitoramento. Se o aplicativo não cooperar, o marco civil prevê sanções, que se espera sejam julgadas constitucionais, ou se ilegal, buscar junto às lojas virtuais que não sejam comercializados e baixados.

Concluiu sua Excelência, que compete somente à Autoridade Nacional de Proteção de Dados – ANPD e não ao Poder Judiciário a aplicação de sanção ao aplicativo que descumprir decisão judicial, justificando esse entendimento com base no artigo 55-J, inciso IV, da Lei n.º 13.709 de 14/08/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD). O artigo 5º, inciso XIX, da LGPD define autoridade nacional como "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados em todo o território nacional". Portanto, careceria a ANPD de autorização legislativa para fiscalizar o cumprimento de outras leis.

As autoridades de proteção de dados ou *Data Protection Authorities* são, de acordo com a Comissão Europeia, "autoridades públicas independentes que supervisionam, por meio de poderes investigativos e corretivos, a aplicação das leis de proteção de dados e recebem as reclamações contra violações à LGPD" (BEZERRA, 2019). Contudo, o artigo 4º, inciso III, alínea "d", do mesmo diploma legal preceitua que "a LGPD não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de atividades de investigação e repressão de infrações penais". Compreende-se, então, que a Autoridade Nacional de Proteção de Dados não possui competência legal para sancionar o descumprimento de decisão judicial de natureza criminal, mas tão somente sobre as competências correlatas de outras entidades ou órgãos da administração pública no que se refere à proteção de dados pessoais, observando a estrita competência que lhe foi concedida pelo artigo 55-K da LGPD.

Da exploração excepcional de dispositivos

durante o debate na audiência pública, a Procuradoria Geral da República – PGR e o Laboratório de Pesquisa em Políticas Públicas e Internet – Lapin, bem como o Tribunal de Justiça de Sergipe – TJ/SE, no julgamento do mandado de segurança contra ato do Juiz de Lagarto, citaram técnicas para exploração excepcional de dispositivos informáticos, que são medidas paliativas para obtenção de prova.

A legislação britânica denomina essa técnica como *equipment interference* (interferência em equipamento) e está prevista no *The Investigatory Powers Act* 2016 (IPA 2016) (Lei de Poderes de Investiga-

ção). A esse respeito, Mckay (2017, p. 113), em seu guia sobre a legislação que autoriza o serviço de inteligência britânico e forças de segurança a contornar a criptografia, escreveu "*The state's engagement in equipment interference, also known as computer network exploitation (CNE) has only been publicly admitted since early 2015 when the government published a draft Code of Practice on the use of the technique*".

A parte 5 do IPA 2016 prevê na seção 99, subseção 9, do *Blackstone´s guide to The Investigatory Powers Act* 2016, reproduzido por Mckay (2017, p.323 e 352), a expedição de dois tipos de mandados, os *targeted equipment interference warrants* e os *targeted examination warrants*. O primeiro permite a autoridade a quem lhe é dirigido obter o conteúdo das comunicações, as informações armazenadas em determinado equipamento e qualquer outra informação. O segundo tem como objetivo autorizar o acesso e o exame de conteúdo de interceptação de sinais coletados a partir de mandados expedidos *"under a bulk equipment interference warrant for examination"*, que seria uma espécie de coleta em massa de comunicações *"of overseas-related communications"*, ou seja, comunicações mantidas por indivíduos ou organizações que estejam fora das Ilhas Britânicas.

O objeto de estudo deste artigo não pretende o aprofundamento na interceptação em massa de sinais, técnica de inteligência utilizada por grandes potências, a exemplo dos Estados Unidos da América, Austrália, Reino Unido, Israel, Rússia e China, para defesa contra ameaças externas, como terrorismo e crime organizado transnacional. Ademais, a legislação brasileira não prevê interceptação em massa de sinais. Se a interceptação pontual de sinais e o acesso autorizado judicialmente ao conteúdo de comunicações protegidas por criptografia já gera uma grande polêmica no Brasil, seria difícil imaginar um debate e avanço legislativo no que tange à interceptação em massa de sinais.

Da remoção de proteção eletrônica

O parlamento do Reino Unido entendeu razoável a inserção e aprovação das chamadas ***technical capability notices*** que em tradução livre significa "requisição de auxílio em matéria técnica", para que o provedor de comunicações auxilie o Estado a implementar uma inter-

ceptação de sinais. Nesse sentido, a seção 253 do guia de Mckay (2017, p. 430) autoriza ao Secretário de Estado, após aprovação do *Judicial Commissioner*, a requisitar colaboração do operador postal, operador de telecomunicações ou qualquer outra pessoa que pretenda executar operações postais ou de telecomunicações. As obrigações que podem ser impostas seriam no sentido de disponibilizar estrutura ou serviços de telecomunicações ou postais, ou relacionadas com o aparato pertencente a essas organizações, ou a obrigação relacionada com a remoção de proteção eletrônica oferecida ou utilizada pelo operador de telecomunicações ou de internet.

A requisição de auxílio em matéria técnica não é uma ordem de interceptação, nas palavras de Graham Smith (2017) "ela prepara o terreno com antecedência para assegurar que o provedor tenha os equipamentos configurados" para a posterior ordem de interceptação telefônica ou de sinais. Smith menciona que a principal mudança da nova lei britânica de interceptações (IPAct, 2016), em comparação ao regulamento da lei anterior, seria que a *technical capability notice* – TCN não estaria mais limitada à interceptação telefônica, e sim aplicadas aos três poderes concedidos pela nova lei: (i) interceptação, seja ela em um alvo determinado, seja ela temática ou em massa, (ii) coleta de fluxo de dados de informática (seja ela ordinária ou em massa) e aos (iii) acessos em dispositivos de informática (*equipment interference*), sejam estes acessos dirigidos a alvos pontuais, temáticos ou em massa (SMITH, 2017).

Descrito por Smith (2017) como o mais controvertido aspecto das *technical capability notices* durante a tramitação da lei, é a hipótese da utilização da requisição para remoção de criptografia visando evitar o uso de criptografia ponta-a-ponta. O autor cita em seu artigo transcrições de debate ocorrido na Casa dos Lordes em 19/10/2016, quando o Secretário de Estado respondia questões formuladas pelos membros do Parlamento. Na oportunidade, o ministro Earl Howe declarou:

> *These safeguards ensure that an obligation to remove encryption under Clause 229 of the Bill will be subject to very strict controls and may be imposed only where it is* **necessary** *and* **proportionate**, **technically feasible** *and* **reasonably practicable** *for the relevant operator to comply. (SMITH, 2017, grifo nosso)*

Smith (2017) entende que o ponto central para as requisições das *technical capability notices* reside na viabilidade técnica. No sistema britânico, o *Home Secretary* deve consultar previamente o *Technical Advisory Board* que é uma espécie de conselho consultivo para obter considerações de ordem técnica, acerca da viabilidade para implementação das requisições preparatórias para a interceptação de sinais ou exploração de dispositivos informáticos.

Do acesso remoto

Passa-se agora abordar uma importante técnica de obtenção de prova digital para os órgãos responsáveis pela investigação criminal, que é o acesso remoto a dispositivo eletrônico, sistema informático ou rede de dados. O acesso remoto oculto ou não, é uma técnica policial autorizada judicialmente, que visa o acesso excepcional a dispositivo eletrônico, aplicativo ou sistema informático, utilizado pelo investigado, com o objetivo de coletar prova digital e o seu armazenamento com integralidade, com vistas à sua utilização no processo penal. O acesso excepcional a dispositivo informático não possui uma legislação específica no Brasil, mas é compreendido analogicamente com base legal no artigo 240, § 1º, alínea "e", do Código de Processo Penal, que autoriza a busca e apreensão para descobrir objetos necessários à prova da infração.

Alguns autores denominam a técnica como *hacking* policial. A palavra *hacking* tem como origem o verbo *to hack* que significa "cortar em pedaços de forma violenta", segundo o *Dictionary Cambridge* online. O termo *hacker* foi cunhado na década de 1960 por estudantes do *Massachussetts Institute of Technology* – MIT para designar soluções criativas para um problema, como por exemplo, interligar sistemas informáticos e telefônicos para fazer chamadas grátis (VILELA, 2006). Conforme Vilela,(2006), *hacker* se refere a pessoas habilidosas em programação, administração e segurança, o que difere de *crackers* que praticam atividades criminosas usando técnicas de invasão de computadores, furto de informações, depredação de *sites*, etc., alertando que mídia, e posteriormente a opinião pública, emprega o termo equivocadamente.

Ivan Škorvánek, Bert-Jaap Koops, Bryce Clayton e Andrew Roberts publicaram o artigo intitulado "Meu computador é meu castelo": Novas estruturas de privacidade para regulação do hacking policial[2] onde compararam a legislação da Alemanha, Itália, Holanda, Reino Unido e Estados Unidos e como a referida técnica investigativa é recepcionada pelas diferentes jurisdições. Os autores mencionam que o *hacking* policial pode ocorrer de três diferentes maneiras: a primeira seria com o (i) acesso físico ao computador do investigado, como por exemplo instalando um malware, um *keylogger*. Ao reconhecer que o acesso físico não é muitas vezes possível, os autores citam o (ii) acesso remoto como o mais comum acesso ao dispositivo do investigado. A exemplo disso, ilustram como um envio de e-mail ao investigado contendo um anexo ou link que conduziria a instalação de um malware, que poderia eventualmente copiar arquivos, acionar a webcam, ativar o microfone e etc. A terceira forma e menos invasiva seria acessar o computador do suspeito utilizando o (iii) login e senha (ŠKORVÁNEK, 2019, p. 9).

O grupo de pesquisadores descreveu seis funcionalidades para o *hacking* policial. A primeira delas seria (i) capturar tipos específicos de dados, técnica autorizada pela legislação holandesa onde se busca identificar o usuário do computador ou a sua localização. A segunda funcionalidade apontada é a (ii) busca remota de dados armazenados que pode ter como alvo o computador do investigado ou dados armazenados em nuvem, podendo ocorrer o espelhamento desses dados. A diferença dessa segunda funcionalidade com relação a uma diligência de busca e apreensão na qual ocorre o espelhamento do *hard disk* do investigado ou do servidor é que na busca remota mantém-se o sigilo do procedimento quanto às pessoas afetadas pela medida. A terceira aplicabilidade é o (iii) monitoramento remoto do uso do computador que possibilitaria a captura de dados, seja por *screenshots* ou *screencasting*, armazenados após a inserção do *malware* com vistas a enviar à autoridade responsável pela vigilância (ŠKORVÁNEK, 2019, p. 10-11).

A quarta funcionalidade narrada e a mais importante para o objeto do nosso estudo é a (iv) interceptação das comunicações. Aqui o *hacking* policial tem como finalidade a interceptação do conteúdo das

2 Tradução do autor.

comunicações eletrônicas, por exemplo, e-mail, mensagens de texto e chats via *WhatsApp ou Telegram*. Os autores sintetizam que seria nesta modalidade a principal oportunidade de contornar a dificuldade em se acessar o conteúdo das comunicações criptografadas: "Since most of these services nowadays use end-to-end encryption, and interception through the service provider is often not possible, interception at the source before encryption (or at the destination after decryption) may be the only way to capture the contents of online communications" (ŠKORVÁNEK, 2019, p. 11).

A quinta serventia seria (v) observação visual que objetiva "sequestrar" a webcam do investigado para identificar o usuário, determinar sua localização ou observar o comportamento do suspeito ou de pessoas suspeitas naquele ambiente, como se fosse uma câmera espiã (ŠKORVÁNEK, 2019, p. 11). A sexta aplicabilidade consistiria em (vi) deletar remotamente dados ilegais, como pornografia infantil, ou remover vírus de computadores infectados como forma de prevenir ataques coordenados. Essa última funcionalidade somente está prevista na lei holandesa (ŠKORVÁNEK, 2019, p. 12).

Na Alemanha, a previsão legal para *hacking* policial foi inserida no Código de Processo Penal na seção 100a e na 100b, a primeira regula a *source interception of telecommunications* e a segunda a *online search*, sendo esta última sujeita a procedimentos mais restritivos em decorrência de garantias, em especial o direito à integralidade e confidencialidade de sistemas computacionais, consagrado pela Corte Federal Constitucional em decisão de 27/02/2008. A interceptação das comunicações consiste no monitoramento e gravação dos diálogos ou mensagens das conversas em andamento, bem como a obtenção dos dados pretéritos armazenados que possuam conexão com o tema, desde que autorizados pela ordem judicial. Os autores ressaltam que doutrina alemã dominante não permite a geração de dados pelos investigadores tampouco edição destes dados. Nesse sentido, não seria permitido ligar a câmera, acionar o microfone ou deletar dados ilegais (ŠKORVÁNEK, 2019, p. 14). A ordem judicial de interceptação tem validade de três meses e pode ser renovada enquanto presentes os motivos que ensejaram a quebra do sigilo do investigado. Já a busca online da seção 100b somente pode ser concedida por uma Corte Distrital Média (*mid-level district court*) pelo período máximo de um mês. Para

a quebra de sigilo por período superior a seis meses, a apreciação caberá a uma Corte Regional Superior.

Na Itália, sugerem os autores que o *hacking* policial seria massivamente empregado na prática, mas possuindo pouca regulamentação. A Suprema Corte considerou legal a instalação sigilosa de dispositivo em computador para coleta de dados com base em meios atípicos de coleta de prova, previsto no artigo 189 do Código de Processo Penal Italiano. Já a instalação de um Trojan para monitorar o tráfego de dados no denominado caso Ryanair foi interpretado pela Suprema Corte como baseado no poder tradicional de busca e apreensão. Apesar do contraste acerca do fundamento legal para legalidade da medida, concluem os pesquisadores que as cortes Italianas são bastante permissivas em autorizar as várias práticas de *hacking* policial com base na legislação geral. O uso de Trojan para interceptação de comunicações orais, por meio de acesso e acionamento remoto do microfone, gerou casos relevantes junto à Suprema Corte, tendo sido considerada prova lícita para fins de investigação de crime organizado (ŠKORVÁNEK, 2019, p. 16-17).

No dia 1º de março de 2019 entrou em vigor na Holanda o *Computer Crime Act III* concedendo novos poderes a polícia para acessar remota e sigilosamente computadores para prevenir e combater *serious crimes* como pornografia infantil, tráfico de drogas e atentados. Os poderes conferidos possibilitam determinar a identidade e localização do usuário, gravação das comunicações privadas de investigados, sejam elas telecomunicações ou interceptação ambiental, observação sistemática, acesso aos dados previamente armazenados bem como às informações futuras, transmitidas posteriormente ao acesso remoto e tornando os dados inacessíveis, a exemplo disso, deletando material de pornografia infantil do computador do alvo, obviamente após o espelhamento para fins de prova (ŠKORVÁNEK, 2019, p. 18).

Nos Estados Unidos da América, a denominada *network investigative technique* – NIT vem sendo utilizado pelo FBI pelo menos desde 2001, sendo que os Tribunais Federais enfrentaram a questão a partir de 2016 após julgamentos de duas grandes operações, as denominadas Operação Torpedo (2011-12) e Operação Pacificador (2014-15) que combateram pornografia infantil. Segundo Škorvánek *et al.*

(2019, p. 23-26), a grande maioria dos casos de *hacking* governamental se limitariam à funcionalidade de capturar tipos específicos de dados, como já explicado anteriormente, com foco em identificar o usuário e sua localização. Em algumas operações teria o FBI optado pela funcionalidade de interceptação das comunicações em tempo real.

Já nas operações *PedoBook* e *PedoBoard* os investigadores do FBI tomaram o controle de um site de pornografia infantil e inseriram um malware que infectou os usuários, fazendo com que o endereço de IP, dia, hora e o sistema operacional fossem reportados ao órgão de investigação. Posteriormente, representaram por autorização judicial para instalar um *keylogging* para autorizar a equipe de investigação a obter senhas do computador do criador do site de pornografia, acessar os arquivos ali armazenados e interceptar as comunicações em tempo real mantidas pelo principal investigado e outros usuários ainda desconhecidos (ŠKORVÁNEK, 2019, p. 29-30).

Um outro caso citado no artigo *My Computer is my Castle* é uma investigação de pornografia infantil desencadeada pelo FBI, denominada *Playpen,* contra um site hospedado na *dark web* que utilizava a rede Tor. Os investigadores obtiveram o controle do site e realocaram o conteúdo para servidores localizados na sede do FBI, como forma de manter a integridade dos dados ilegais antes que fossem deletados, mas ainda sim encontraram enorme dificuldade em identificar os suspeitos de produzir e compartilhar material pornográfico de crianças e adolescentes, pois eles permaneciam protegidos pela criptografia ("*still cloaked by the Tor encryption technology*") (ŠKORVÁNEK, 2019, p. 30).

Fazendo uma breve digressão para o voto do ministro Edson Fachin que entendeu que "o risco causado pelo uso da criptografia ainda não justifica a imposição de soluções que envolvam acesso excepcional ou ainda outras soluções que diminuam a proteção garantida por uma criptografia forte" e que elimina "do ordenamento a interpretação que autorize o acesso excepcional" (STF, 2020, p. 75), seria possível constatar que, caso prevaleça este entendimento, criminosos no Brasil estariam protegidos pela criptografia, uma vez que sua Excelência interpreta que o ordenamento jurídico pátrio não autoriza o acesso excepcional, tampouco ordem de bloqueio de aplicativos, pois "se o Poder Judiciário não pode determinar a interceptação do fluxo, tam-

pouco poderia sancionar eventual descumprimento da ordem" (STF, 2020, P. 75).

Retornando ao *Playpen cases*, a única saída encontrada pela equipe do FBI para contornar o obstáculo da criptografia, proteger as vítimas da pornografia infantil e identificar os responsáveis pelo crime, foi representar por uma autorização judicial para utilizar a técnica de *hacking* policial (NIT) com o objetivo de instalar um malware para infectar os computadores dos criminosos e transmitir ao FBI o endereço de IP, data e hora do acesso, um identificador único como forma de individualizar cada suspeito, sistema operacional, o nome do computador, endereço MAC e informação se a *network investigative technique* chegou a ser instalada em determinado computador.

Para conferir maior efetividade às técnicas de investigação no Brasil, o dever de atender a pedidos de quebra de sigilo não deve ser extraído apenas do Marco Civil da Internet mas também da análise de um sistema de normas (Constituição Federal/88, Lei n.º 9296/1996, CPP e outras) que, quando interpretadas em forma sistêmica, permitem concluir que as empresas, provedores e aplicativos devem sim ser capazes de fornecer o conteúdo das comunicações nos casos de crimes graves. Nesse sentido, discorda-se de Jacqueline de Souza Abreu, citada pelo ministro Edson Fachin em seu voto (STF, 2020, p. 74), quando afirma que o "dever jurídico, extraído do direito brasileiro vigente, de que aplicações de internet sejam capazes de quebrar sigilo de conteúdo de comunicações não é evidente; carece de fundamentação". Na verdade, a capacidade para decretar a quebra emana do Poder Judiciário e o dever jurídico das aplicações de internet é de auxiliar a implementação destas excepcionais medidas, tal qual o dever dos *relevant operators* no Reino Unido, quando requisitados a colaborar por intermédio das *technical capability notices*.

Hipóteses de acesso de comunicações criptografadas

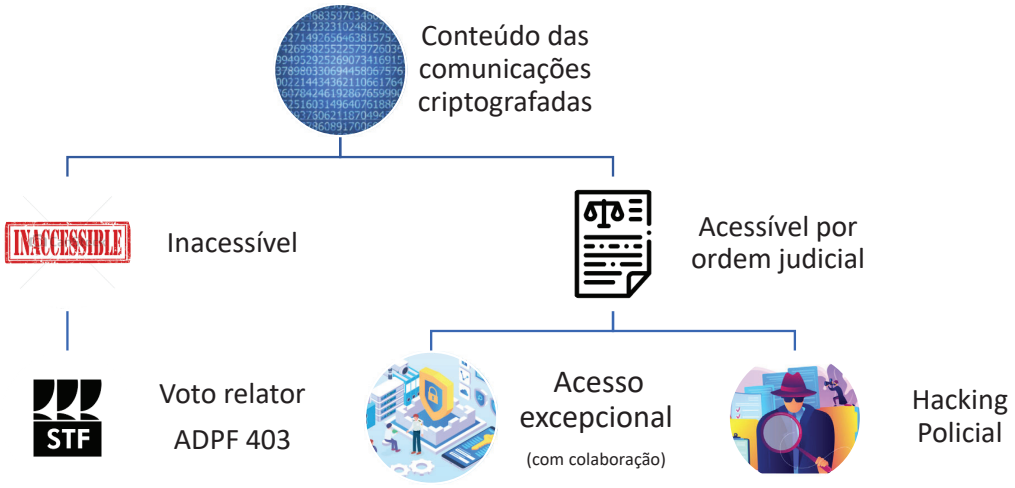
Apesar do voto do relator na ADPF 403 estar circunscrito à declaração de inconstitucionalidade do artigo 7º, inciso II, e artigo 12, inciso III, do Marco Civil da Internet para afastar qualquer acesso ex-

cepcional a conteúdo de mensagem criptografada ou que "por qualquer outro meio, enfraqueça a proteção criptográfica" (STF, 2020, p.74) de aplicativos, nos parece que o voto declara a inacessibilidade do conteúdo das comunicações criptografadas de indivíduos investigados por crimes graves[3], por temer um enfraquecimento da criptografia, o que poderia expor a privacidade da coletividade de usuários. Além disso, o voto sugere a inconstitucionalidade do acesso excepcional mesmo se porventura algum aplicativo decidisse colaborar com as investigações pois o voto "afasta qualquer acesso excepcional", bem como também macula de inconstitucionalidade o acesso ao conteúdo das comunicações por ordem judicial utilizando técnicas de *hacking* policial.

O quadro a seguir ilustra a situação da interceptação do conteúdo das comunicações criptografadas. A primeira hipótese seria da inacessibilidade legal defendida pelo ministro Edson Fachin. A segunda hipótese seria a da possibilidade legal do acesso às conversas criptografadas de suspeitos, podendo ocorrer, pelo menos, de duas formas: via acesso excepcional, quando um provedor de aplicações, ao reconhecer sua responsabilidade em colaborar com a segurança pública, auxilia na implementação técnica da medida. A segunda forma de se conhecer o conteúdo de diálogo criptografado seria o *hacking* policial, podendo este ser implementado com técnica desenvolvida para determinados casos ou soluções pontuais. A exemplo disso, software espião, infiltração policial virtual ou até mesmo ferramentas comerciais desenvolvidas especialmente para as forças de segurança.

3 Lembrando aqui dois pontos: (1) Não é possível a quebra de sigilo no Brasil de pessoas que não estejam incorrendo em crime punível com reclusão e (2) que a ADPF trata de interceptação de comunicações de membros de organização criminosa.

Quadro 01. Ilustra hipóteses de acesso ao conteúdo de comunicações criptografadas



Fonte: Autor

Infiltração policial

A infiltração policial consiste em um meio especial de obtenção da prova – verdadeira técnica de investigação criminal – por meio do qual o agente de polícia, judicialmente autorizado, ingressa, ainda que virtualmente, em determinada organização criminosa, forjando a condição de integrante, com o escopo de alcançar informações a respeito de seu funcionamento e de seus membros (MASSON; MARÇAL, 2017, p. 299). A doutrina já admitia a infiltração virtual antes mesmo do advento da Lei n.º 13.441 de 08 de maio de 2017[4], que previu a infiltração de agentes de polícia na internet. Por isso, pode-se afirmar que a infiltração policial é gênero do qual são espécies a presencial (física) e a virtual (cibernética ou eletrônica). Entende-se que bastava o legislador autorizar a infiltração de agentes policiais, sendo tarefa do juiz autorizar se ocorreria na espécie virtual e/ou presencial.

Parte da doutrina expressava dúvida quanto ao cabimento da técnica de infiltração policial virtual em investigações diversas das que

4 A definição de infiltração de agentes policiais de Masson e Marçal, incluindo a infiltração virtual, foi publicada no livro Crime Organizado, sendo a 3ª edição fechada em dezembro de 2016, portanto, anteriormente à Lei nº 13.441/2017.

apuravam crimes contra a dignidade sexual de criança e adolescente. Com a aprovação da Lei n.º 13.964 de 24 de dezembro de 2019 o legislador expressou seu consentimento para o uso da técnica também nos crimes de lavagem de dinheiro (art. 1º, § 6º, da Lei n.º 9.613/1998) e organização criminosa (art. 10-A da Lei n.º 12.850/2013). Bem como entendeu o ministro Edson Fachin, ao estabelecer a premissa de que o impacto tecnológico das mudanças porque passa a sociedade reclamam um permanente atualizar do alcance dos direitos e garantias fundamentais (STF, 2020, p.1) , estende-se o mesmo entendimento para atualizar permanentemente como se interpreta os meios de obtenção de prova previstos na legislação.

Não se trata aqui de criar meios de obtenção de prova, mas sim de um olhar sistêmico e atual para o instituto. Observa-se as três características básicas que marcam a infiltração de agentes policiais, a *dissimulação*, ou seja, a ocultação da condição de agente oficial e de suas verdadeiras intenções; o *engano*, posto que toda a operação de infiltração se apoia numa encenação que permite ao agente obter confiança do suspeito; e por fim, a *interação*, isto é, uma relação direta e pessoal entre agente e autor potencial (SILVA, 2014, p.92 apud MASSON; MARÇAL, 2017, p.299-300). As características mencionadas servem para nortear a ação do Estado, por exemplo, a necessidade de dissimulação do agente policial justifica a representação por expedição de documento de identidade ostentando o nome fictício que se deseja infiltrar, nos casos de aproximação presencial, ou a criação de um *nickname* e ocultação de sua identidade quando a infiltração for virtual, hipótese prevista no art. 10 da Lei n.º 12.850/2013.

É possível afirmar então que para implementação dos meios especiais de obtenção de prova, como a infiltração policial e a captação ambiental, será necessária a utilização de técnicas policiais de suporte, como a entrada imperceptível em locais de acesso restrito, estória-cobertura, disfarce, *hacking* policial e outras (GARAY, 2021). Assim, entende-se razoável o uso de técnicas de suporte para, por exemplo, a infiltração virtual de agente de polícia em grupo de *WhatsApp* utilizado por organização criminosa. A técnica-fim seria a infiltração, a técnica-meio pode ser o acesso físico ou acesso remoto excepcional ao aparelho do administrador do grupo, visando adicionar o agente disfarçado. Uma terceira hipótese de técnica de suporte é a obtenção de autorização ju-

dicial para determinar à operadora de telefonia celular que "clone" por alguns momentos a linha do investigado-administrador do grupo, para receber mensagem de texto (SMS) e posterior autenticação no aplicativo instalado em aparelho controlado pelos investigadores[5].

Gemaque (2017) no artigo "É possível a infiltração virtual de agentes em organizações criminosas" entende ser viável tecnicamente a obtenção de autorização judicial para habilitação de Sincards em substituição aos reais números das linhas investigadas a fim de que a autoridade policial se infiltre na linha. Acrescenta o autor que será tecnicamente infiltração de agente quando houver comunicação do agente infiltrado com algum delinquente, diferentemente da interceptação de comunicações que se classifica como interceptação telefônica.

A questão foi submetida à 13ª Turma do Tribunal Regional Federal da 3ª Região que entendeu que a infiltração policial virtual em grupo de *WhatsApp* da Organização Criminosa não encontraria respaldo na Constituição Federal/88 e Lei de interceptação telefônica e de dados. Seguinte ementa do mandado de segurança criminal:

> *MANDADO DE SEGURANÇA. INTERCEPTAÇÃO TELEFÔNICA. SUSPENSÃO DA COMUNICAÇÃO. PROCEDIMENTO ILEGAL. SEGURANÇA CONCEDIDA.*
>
> *1. Preliminar de ilegitimidade ativa rejeitada. A operacionalização da medida cabe à empresa de telefonia, que, por isso, é parte legítima para discutir a legalidade da ordem que lhe foi imposta. Em outras palavras, como não se pode exigir que alguém faça ou deixe de fazer alguma coisa senão em virtude de lei, aquele do qual é exigido determinado comportamento tem o direito de levar ao Poder Judiciário a discussão acerca da legalidade do comando.*
>
> *2. A medida impugnada não encontra respaldo no art. 5º, XII, da Constituição Federal ou na Lei n.º 9.296/1996, pois não se trata, propriamente, de interceptação telefônica, mas de procedimento por meio do qual se transferem, ainda que momentaneamente, os terminais dos investigados para simcards da autoridade policial.*
>
> *3. Mais do que a interceptação da comunicação telefônica, a*

5 Com a autenticação em dois fatores dos aplicativos de mensagem instantânea, a técnica de clonar o Sincard ficou mais a difícil de implementação.

> *medida autorizada implica a suspensão dessa comunicação, uma vez que os investigados deixariam de comunicar-se com seus interlocutores e, durante certo período, a critério da autoridade policial, seriam substituídos por esta ou seus agentes.*
>
> *4. Tratando-se de medida invasiva e que interfere em garantias e direitos fundamentais de investigado, sua interpretação deve ser restritiva e não poderá admitir aplicação analógica.*
>
> *5. Tratando-se de providência que excepciona a garantia à inviolabilidade das comunicações, a interceptação telefônica e telemática deve se dar nos estritos limites da lei, não sendo possível o alargamento das hipóteses previstas ou a criação de procedimento diverso.*
>
> *6. Preliminar rejeitada. Segurança concedida.*

O Ministério Público Federal interpôs Recurso Especial contra o acórdão sustentando que a

> *medida pretendida pela autoridade policial diz respeito ao fluxo das comunicações (a mensagem ou a ligação que será recebida no celular da polícia, instantaneamente) e, ao mesmo tempo, aos dados contidos nos celulares dos investigados (histórico das conversas e ligações), trata-se portanto de um misto de interceptação telefônica e acesso à base, ainda que virtual, no qual se encontram os dados, amoldando-se perfeitamente à Lei de Interceptação Telefônica.*

Em despacho datado de 31 de outubro de 20186, o Vice-Presidente do Tribunal Regional Federal da 3ª Região consignou que nenhum precedente foi encontrado no repertório de jurisprudência do Superior Tribunal de Justiça e admitiu o Recurso Especial, que poderá uniformizar a possibilidade e legalidade da utilização de técnicas especializadas de inteligência para implementação de infiltração virtual, captação ambiental ou outros meios especiais de obtenção de prova.

Discorda-se do entendimento da 13ª Turma do TRF3, pois como mencionado anteriormente, não se trata de interceptação telefônica e sim meio especial de obtenção de prova por intermédio de infiltração policial virtual, utilizando como técnica de suporte para sua implementação, a dissimulação de agente infiltrado momentaneamen-

6 O despacho que admite o Recurso Especial foi publicado juntamente com o acórdão da 13ª Turma do TRF3.

te como administrador do grupo. Os julgadores interpretaram a substituição momentânea de Sincards, que na prática ocorreria de madrugada quando o alvo está dormindo e não se comunicaria com nenhum interlocutor, como medida invasiva que não comportaria "alargamento das hipóteses previstas ou a criação de procedimento diverso"[7]. Pensa-se diametralmente oposto e em consonância como bem apontado por Gemaque, "em matéria processual penal, como previsto no artigo 3º do Código de Processo Penal, admite-se o emprego da interpretação extensiva e aplicação analógica" (GEMAQUE, 2017).

A compreensão equivocada dos desembargadores neste julgamento ocorre pela dificuldade de se compreender a diferença entre investigação criminal e inteligência de segurança pública, e que no entender de Garay, ocorre o fenômeno do empréstimo da metodologia de inteligência aos meios extraordinários de obtenção de prova. O autor exemplifica citando a captação ambiental, que por força do art. 8º-A, § 1º, da Lei n.º 9296/1996, exige que a representação da autoridade policial descreva circunstanciadamente o local e a forma de instalação do dispositivo de captação ambiental, o que caracteriza uma "abertura legal para a metodologia de inteligência, já que será indispensável a utilização de técnicas especializadas, especialmente a entrada, a qual será delimitada pelo juiz" (GARAY, 2021).

Assim, a utilização de técnicas especializadas para implementação da captação ambiental ou infiltração virtual é submetida ao juiz no caso concreto, momento em que a autoridade policial justifica quais os meios necessários para a implementação da medida pleiteada. Essa **abertura legal** é justamente a previsão no ordenamento jurídico que permite ao magistrado autorizar ou não, caso a caso, norteado pelos princípios de razoabilidade e proporcionalidade, a adoção de operação policial disfarçada ou *hacking* policial.

A operação policial disfarçada foi proposta como técnica especial de inteligência (técnica-meio) para a implementação da captação ambiental (técnica-fim), no projeto de Lei n.º 6341/2019 (n.º 10.372/2018 na Câmara dos Deputados), mas foi vetado pelo Presidente da República por excetuar a realização da diligência na Casa do investigado (BRASIL, 2019). Entendeu o Presidente da Repúbli-

7 Trecho do Acórdão mencionado anteriormente.

ca que a propositura legislativa geraria insegurança jurídica ao retirar do alcance da operação policial disfarçada a "casa"[8], o que poderia ser interpretado de forma ampla e inviabilizar a diligência em hotéis ou escritórios. Por consequência, apesar de não possuir dispositivo legal expresso, continua a valer a orientação da jurisprudência que permite a incursão policial noturna em escritório de advocacia, como restou decidido no INQ 2424, da denominada Operação Furacão, quando o STF considerou lícita a prova obtida a partir da entrada noturna no escritório de advogado, que culminou no único caso de afastamento de ministro de tribunal superior (BRASIL, 2008).

Como evidência da viabilidade, razoabilidade e proporcionalidade do uso de técnicas avançadas de investigação criminal, notadamente o *hacking* policial, cita-se a Operação *Sky* deflagrada em 09 março de 2021 pelas polícias federais e órgãos de persecução da Bélgica, França e Holanda, países historicamente comprometidos com a privacidade e proteção de dados, que consistiu na quebra de criptografia e interceptação de mensagens do aplicativo Sky ECC utilizado por 170 mil usuários, que trocavam cerca de três milhões de mensagens diariamente. Segundo a Europol, cerca de 20% dos usuários do aplicativo estavam baseados na Bélgica e na Holanda, sendo que a infraestrutura do Sky ECC está baseada nos Estados Unidos da América e no Canadá (EUROPOL, 2021). Noticiou-se que as autoridades apreenderam 27 toneladas de cocaína avaliadas em € 1,4 bilhão, que corresponde a cerca de R$ 9 bilhões (BOFFEY , 2021). Comprova-se, portanto, que somente a partir de meios especiais de obtenção de prova, o Poder Público conseguiu conhecer a estrutura da organização e, consequentemente, desmantela-la, bem como rastrear os bens, recursos e criptoativos branqueados pela criminalidade organizada.

Do projeto de lei sobre as provas digitais

Em 15 de outubro de 2020, o Deputado Federal Hugo Leal

8 O chefe do executivo ao fazer referência ao HC 82788, Rel. Min. Celso de Mello, que assentou "o conceito normativo de "casa" revela-se abrangente e, por estender-se a qualquer compartimento privado não aberto ao público, onde alguém exerce profissão ou atividade (CP, art. 150, § 4º, III), compreende, observada essa específica limitação espacial (área interna não acessível ao público), os escritórios profissionais".

(PSD/RJ) apresentou o projeto de lei n.º 4939/2020 que dispõe sobre a obtenção e admissibilidade de provas digitais na investigação e no processo. O projeto possui como fundamento, dentre outros, o da garantia de autenticidade e da integridade da informação, como tal consagrado pela Corte Constitucional Alemã em 27/02/2008. O texto propõe algumas definições, como a de prova digital como sendo toda a informação armazenada ou transmitida em meio eletrônico que tenha valor probatório (LEAL, 2020). A proposta prevê os crimes de falsidade informática, dano informático, sabotagem informática, acesso ilícito a dispositivo, sistema ou rede, e de interceptação ilícita.

O art. 9º da proposta dispõe sobre os meios de obtenção de prova digital, elencando os seguintes:

> *I – a busca e apreensão de dispositivos eletrônicos, sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica, e o tratamento de seu conteúdo.*
>
> *II – a coleta remota, oculta ou não, de dados em repouso acessados à distância.*
>
> *III – a interceptação telemática de dados em transmissão.*
>
> *IV – a coleta por acesso forçado de sistema informático ou de redes de dados.*
>
> *V – o tratamento de dados disponibilizados em fontes abertas, independentemente de autorização judicial.*

O projeto define que a coleta por acesso forçado a dispositivo eletrônico, sistema informático ou redes de dados ocorrerá somente após prévia desobediência de ordem judicial determinando a entrega da prova pretendida ou quando impossível identificar o computador ou provedor em território nacional, e compreenderá os métodos de segurança ofensiva ou qualquer outra forma de possibilite a exploração, isolamento e tomada de controle (LEAL, 2020).

O PL n.º 4939/2020 propõe prazo de até 60 (sessenta) dias para o monitoramento do fluxo de dados, permitindo prorrogações pelo mesmo período, até no máximo de 360 (trezentos e sessenta) dias, ou em caso de crime permanente, enquanto não cessar a permanência. A ordem de obtenção de prova digital pode ser dirigida a terceira pessoa, quando houver indícios de utilização de dispositivo eletrônico pelo investigado,

com ou sem consentimento do proprietário (LEAL, 2020).

Apesar de muito bem redigida e de boa concepção técnica, o projeto não andou bem e esboçou que os meios de obtenção de prova digital serão implementados por "perito oficial ou assistente técnico da área de informática" (LEAL, 2020). A nosso ver o texto, na forma que foi proposto, pode trazer questionamentos desnecessários à investigação, uma vez que as unidades de análise e inteligência policial são compostas por equipe multidisciplinar, contando com agentes de polícia com as mais diversas formações. É como se a interceptação telefônica ou uma diligência de busca e apreensão só pudessem ser implementadas e executadas por perito oficial. A coleta pode ser procedida por qualquer servidor de natureza policial, investido e qualificado para a tarefa, seja ele delegado, escrivão, agente, perito ou papiloscopista.

Corriqueiramente, os órgãos desenvolvem ou adotam ferramentas que auxiliam a obtenção de prova, com a cautela devida para garantir a sua integralidade, podendo estas soluções serem executadas por agentes de polícia especializados para ganhar escala. Contudo, manter-se-ia a exclusividade do perito oficial para confecção de laudos a partir de perícias criminais. Ademais, a legislação processual penal preceitua que a coleta de vestígios deverá ser realizada preferencialmente por perito oficial e não exclusivamente[9].

O projeto também contemplou a **infiltração virtual** de agentes de investigação em redes de dados, nos casos de crimes puníveis com pena máxima privativa de liberdade igual ou superior a 4 (quatro) anos (LEAL, 2020). A iniciativa é salutar uma vez que a infiltração era possível apenas nas investigações relativas aos crimes de organização criminosa, lavagem de dinheiro e dignidade sexual de menores e adolescentes. Caso convertido em lei, os órgãos de investigação poderão infiltrar agentes de polícia em, por exemplo, casos de furto de FGTS e auxílio emergencial executado por *crackers* a partir de dados pessoais comercializados na *deep web*, moeda falsa vendida pela internet e entregue pelos Correios, e outras infrações em que por não serem cometidas por organização criminosa, não era cabível a infiltração.

9 Vide Art. 158-C do CPP: "*A coleta dos vestígios deverá ser realizada* ***preferencialmente*** *por perito oficial, que dará o encaminhamento necessário para a central de custódia, mesmo quando for necessária a realização de exames complementares*" (grifo nosso).

Um ponto polêmico do projeto é a previsão legal da **ação disfarçada**, que consiste na atuação de agentes de investigação ou, excepcionalmente de particular no curso da investigação relativa aos crimes cometidos por meio eletrônico, a fim de coletar material probatório não protegido por reserva de jurisdição, já que o texto prevê a admissibilidade independentemente de autorização judicial (LEAL, 2020). Seria o caso, por exemplo, do policial que navega disfarçado na *deep web* para prevenir e reprimir crimes, como o de comércio ilegal de arma de fogo. Nesse caso, a lei pune o infrator que vende arma de fogo a agente policial disfarçado, quando presentes elementos probatórios razoáveis de conduta criminal preexistente, afastando assim a hipótese se flagrante preparado (BRASIL, 2003).

Conclusão

Com o avanço da sociedade rumo ao mundo digital, experimenta-se profundas mudanças nas relações sociais, principalmente pelas interações em redes, o acesso a cada vez mais serviços on-line, como os bancários, novas formas de consumo, como comércio eletrônico e *delivery*, mas, principalmente, na forma como se comunica. É legítima, portanto, a preocupação de organizações da sociedade civil, Poder Judiciário e imprensa, com a segurança dos dados pessoais e confidencialidade do conteúdo das comunicações privadas. Logo, a criptografia é ferramenta fundamental para proteção ao direito à privacidade, anonimato e liberdade de expressão.

Todavia, as organizações criminosas também vivenciam estes avanços e se aproveitam dos benefícios da revolução digital, sobretudo nas comunicações seguras entre seus membros. Em contrapartida, os órgãos de prevenção e de investigação buscam alternativas para minimizar este desequilíbrio, seja propondo aperfeiçoamento legislativo que minimize esta defasagem, ou buscando técnicas ou ferramentas que atenuem a disparidade entre a estrutura do crime organizado e a obsolescência das técnicas tradicionais de investigação. Essas técnicas policiais triviais, entre elas a interceptação telefônica clássica, já não possuem mais serventia para conhecer detalhes relevantes de uma or-

ganização criminosa[10]. A experiência empírica mostra que diálogos relevantes e provas digitais trafegam pelos aplicativos de mensagens em tempo real, que oferecem chamadas de voz e de vídeo, praticamente imunes à ação repressiva estatal.

Enquanto países como a Holanda, Reino Unido e a Austrália aprovam leis que conferem poderes arrojados à polícia para conhecer ofensivamente o âmago de uma organização criminosa, como requisitar auxílio às empresas de tecnologia, remoção de proteção eletrônica e técnicas avançadas de interferência em equipamentos, no Brasil, avança-se lentamente no campo legislativo e na esfera jurisprudencial, notadamente, quando o assunto se afasta dos canais tradicionais de metodologia investigativa (depoimentos, busca e apreensão e interceptação telefônica clássica). A magistratura de primeira instância, seja na esfera estadual ou na federal, mais acostumada a lidar com o *periculum in mora* nas representações criminais exerce uma vanguarda quando aprecia representações de meio especial de produção de prova (captação ambiental, infiltração policial e *hacking* policial), contudo, comumente os tribunais reformam estas decisões por interpretar equivocadamente que as técnicas mencionadas seriam invasivas.

Na esfera legislativa, é preciso aprimorar o debate sobre a metodologia de inteligência e o seu suporte às ações excepcionais de obtenção de prova. O Projeto de Lei n.º 4939/2020, que propõe um marco legislativo para obtenção de provas digitais na investigação criminal, muito embora precise de alguns ajustes, como a tomada oculta de controle do dispositivo, rede ou aplicativo administrado pelo investigado[11], é uma excelente propositura legislativa por avançar na coleta remota, coleta por acesso forçado e infiltração virtual.

Conclui-se, pois, que a criptografia, apesar de ser importante elemento de proteção da privacidade, não deve ser interpretada como direito fundamental absoluto. Havendo colisão de direitos igualmente relevantes, pode o operador sujeitar a criptografia às exceções consti-

10 Uma utilidade de remanesce é a geolocalização do investigado por meio da Estação-Rádio Base (ERB) a qual o suspeito está conectado.

11 Similar a tomada de controle executada pelo FBI na operação Playpen utilizando a network investigative technique (NIT)., ou Protocolo SS7, que consiste na clonagem de linha telefônica para tomar o controle de aplicativo.

tucionais do direito à inviolabilidade das comunicações, sob pena de alijar o poder geral de cautela conferido pelo ordenamento jurídico ao Poder Judiciário. Conferir apenas à Autoridade Nacional de Proteção de Dados (BRASIL, 2018) a aplicação de sanção de suspensão temporária de atividades, como proposto pelo ministro Edson Fachin e Ministra Rosa Weber (STF, 2020, p. 75), somente quando os aplicativos violarem o direito de privacidade de seus usuários, é esvaziar o poder conferido pelo legislador ao juiz nas legislações de interceptação telefônica e sistemas de informática (BRASIL, 1996), organização criminosa e marco civil da internet, que devem ser interpretadas sistemicamente. O desarranjo jurídico proposto no voto, à luz da premissa estabelecida por Rudolf Von Ihering, que "a justiça tem numa das mãos a balança em que pesa o direito, e na outra espada de que se serve para o defender. A espada sem a balança é a força brutal, a balança sem a espada é a impotência do direito" (IHERING, 2021) deixará a persecução penal como um fogo que não queima, uma luz que não ilumina.

Destarte, enquanto houver descumprimento de ordens judiciais de interceptação de conteúdo criptografado de comunicações e, caso o voto do relator da ADPF 403, que julgou procedente a arguição de descumprimento de preceito fundamental, de modo a afastar qualquer interpretação que autorize ordem judicial que exija acesso excepcional a conteúdo de mensagem criptografada, seja acompanhado pelos demais ministros do Supremo Tribunal Federal, é possível afirmar que os órgãos de investigação estarão cerceados de implementar técnicas especiais de obtenção de prova, imprescindíveis para apuração de crimes graves como o terrorismo, por exemplo, bem como o desmantelamento de organizações criminosas, razão pela qual é de se reconhecer que a criptografia permanecerá sendo uma ferramenta de comunicação segura para os agentes criminosos no Brasil, contrariando assim a tendência internacional que é de permitir *hacking* e infiltração virtual, conforme observa-se recentemente na Europa, reconhecida por sua legislação protetiva da privacidade, mas não para a criminalidade organizada.

Caio Porto Ferreira

Mestrado em terrorismo e estudos contra o terrorismo pela University of East London

Delegado de Polícia Federal

Police Hacking and Infiltration in Response to the Use of Cryptography by Criminal Organizations

ABSTRACT

Organized crime currently navigates calm waters when it comes to security in its communications. Supported by the recalcitrance of Big Techs, those involved in criminal activities take advantage of communication applications with encryption technology, to organize and expand their activities in Brazil and in the world. In the meantime, institutions responsible for criminal investigation strive to develop and apply new technologies to obtain evidence, which are commonly considered invasive or illegal, not because they face fundamental rights and guarantees, but above all because of the lack of knowledge of certain segments of society about the importance of intelligence activity for the protection and promotion of democratic and free states.

Keywords: Investigation. Evidence-gathering methods. Intercepting communications. Encryption. Privacy.

Hackeo e Infiltración Policial en Respuesta al Uso de Criptografía por Organizaciones Criminales

RESUMEN

El crimen organizado navega actualmente en aguas tranquilas en lo que respecta a la seguridad en sus comunicaciones. Apoyados por la obstinación de las Big Tech, los involucrados en actividades delictivas aprovechan las aplicaciones de comunicación con tecnología de encriptación, para organizar y expandir sus actividades en Brasil y en el mundo. Mientras tanto, los órganos encargados de la investigación penal se esfuerzan por desarrollar y aplicar nuevas tecnologías para la obtención de pruebas, comúnmente consideradas invasivas o ilegales, no porque se enfrenten a derechos y garantías fundamentales, sino sobre todo por el desconocimiento de ciertos segmentos de la sociedad sobre la importancia de la actividad de inteligencia para la protección y promoción de estados democráticos y libres.

Palabras-clave: Investigación. Métodos de recopilación de pruebas. Interceptar comunicaciones. Cifrado. Intimidad.

Referências

BEZERRA, Maria Ruth Borges. *Autoridade Nacional de Proteção de Dados Pessoais:* a importância do modelo institucional independente para a efetividade da Lei. 2019. p. 17. Disponível em: https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3828/1660 Acesso em: 04 mai. 2021.

BOFFEY, Daniel. *Colombia's cartels target Europe with cocaine, corruption and torture*. 2021. The Guardian. 11 abr. 2021. Disponível em: https://www.theguardian.com/world/2021/apr/11/colombias-cartels-target-europe-with-cocaine-corruption-and-torture Acesso em 07 mai. 2021.

BRASIL. *Lei Geral de Proteção de Dados Pessoais* – LGPD. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em 04 mai. 2021.

BRASIL. *STF recebe denúncia contra Paulo Medina e afasta magistrados do cargo.* 2008. Ministério Público Federal. Disponível em: https://mpf.jusbrasil.com.br/noticias/255992/stf-recebe-denuncia-contra-paulo-medina-e-afasta-magistrados-do-cargo. Acesso em: 12 fev. 2021.

BRASIL. *Lei no 10.826,* de 22 de dezembro de 2003. Presidência da República. Casa Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/l10.826.htm. Acesso em: 13 mai. 2021.

BRASIL. *Lei nº 9.296,* de 24 de julho de 1996. Presidência da República. Casa Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 13 mai. 2021.

BRASIL. *Mensagem nº 726 de 24 de dezembro de 2019.* Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Msg/VEP/VEP-726.htm. Acesso em: 12 fev. 2021.

CASTRO, Henrique Hoffman Monteiro. *Lei 13.441/2017 instituiu a infiltração policial virtual.* Disponível em: https://www.conjur.com.br/2017-mai-16/academia-policia-lei-1344117-instituiu-infiltracao-policial-virtual. Acesso em: 11 fev. 2021.

Computer Crime Act III. New law to help fight computer

crime. Disponível em: https://www.government.nl/latest/news/2019/02/28/new-law-to-help-fight-computer-crime. Acesso em: 31 jan. 2021.

CORN, Geoffrey S; BRENNER-BECK, Dru. *"Going Dark":* Encryption, Privacy, Liberty, and Security in the "Golden Age of Surveillance". The Cambridge Handbook of Surveillance Law, páginas 330-371, Cambridge University Press. Disponível em: https://doi.org/10.1017/9781316481127.015 Acesso em: 06 mai. 2021.

EUROPOL. *New major interventions to block encrypted communications of criminal networks.* 2021. Disponível em: https://www.europol.europa.eu/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks Acesso em 07 mai. 2021.

GARAY, Humberto de Sá. *Impactos do pacote anticrime na inteligência de segurança pública.* Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/impactos-do-pacote-anticrime-na-inteligencia-de-seguranca-publica/. Acesso em: 11 fev. 2021.

GEMAQUE, Silvio. **É possível a infiltração virtual de agentes em organizações criminosas**. Disponível em: https://www.conjur.com.br/2017-dez-29/silvio-gemaque-possivel-infiltracao-virtual-agentes2. Acesso em: 11 fev. 2021.

HACK. In: *Cambridge Dictionary.* Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles/hack. Acesso em: 15 fev. 2021.

IHERING, von Rudolf. **Site Pensador**. Frases e pensamentos. Disponível em: https://www.pensador.com/autor/rudolf_von_ihering/. Acesso em: 13 mai. 2021.

KOOPS, Bert-Jaap; KOSTA, Eleni. *Looking for some light through the Lens of "Cryptowar" History:* Policy options for Law enforcement authorities against "going dark". Disponível em: https://doi.org/10.1016/j.clsr.2018.06.003 Acesso em: 06 mai. 2021.

Laboratório de Pesquisa em Políticas Públicas e Internet. Lapin.org.br, 2020. *Lapin é citado no julgamento histórico do STF sobre*

o bloqueio ao WhatsApp. Disponível em: https://lapin.org.br/2020/05/28/lapin-e-citado-no-julgamento-historico-do-stf-sobre-o-bloqueio-ao-whatsapp/ Acesso em: 12 mai. 2021.

MASSON, Cleber; MARÇAL, Vinicius. *Crime Organizado.* 3. ed. Método, 2017. p. 299.

MCKAY, Simon. *Blackstone´s guide to The Investigatory Powers Act 2016*. Oxford University Press. 2017.

Mandado de segurança criminal nº 0003102-15.2017.4.03.0000/SP (2017.03.00.003102-0/SP), relator Desembargador Federal Nino Toldo, publicado no Diário Eletrônico da Justiça Federal da 3ª Região, edição nº 230/2018, de 13/12/2018, página 184, disponível em http://web.trf3.jus.br/diario/Consulta/BaixarPdf/21014 Acesso em 03 mai. 2021.

LEAL, Hugo. *Projeto de lei nº 4939/2020.* Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2264367. Acesso em: 15 fev. 2021.

SILVA, Eduardo Araújo da. *Organizações criminosas:* aspectos penais e processuais da Lei n.º 12.850/13. São Paulo: Atlas, 2014. p. 92.

ŠKORVÁNEK, Ivan; KOOPS, Bert-Jaap; NEWEL, Bryce Clayton; ROBERTS, Andrew. *My computer is my castle:* new privacy frameworks to regulate police hacking. Tilburg University. TILT Law & Technology, 2019.

SMITH, Graham. *Back doors, black boxes and #IPAct technical capability regulations.* Disponível em: https://www.cyberleagle.com/2017/05/back-doors-black-boxes-and-ipact.html. Acesso em: 27 jan. 2021.

STF. *Arguição de Descumprimento de Preceito Fundamental:* ADPF 403. Relator: Ministro Edson Fachin. STF, 2020. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf. Acesso disponível em: 12 mai. 2021.

Supremo Tribunal Federal. Ação Declaratória de Inconstitucionalidade 5527. Relatora Ministra Rosa Weber.

VILELA, G. M. *O uso do termo hacker nas notícias veiculadas pela internet brasileira.* 2006. 66 p. Monografia (Especialização em

Administração de Redes Linux) – Universidade Federal de Lavras, Lavras, 2006. p. 23. Disponível emhttp://repositorio.ufla.br/bitstream/1/9331/1/MONOGRAFIA_O%20uso%20do%20termo%20hacker%20nas%20not%C3%ADcias%20veiculadas%20pela%20internet%20brasileira.pdf. Acesso em: 15 fev. 2021.

WALDEN, Ian. *"The Sky Is Falling!"* – Responses to the "Going Dark" Problem. Computer Law & Security Review Volume 34. Assunto 4. Agosto 2018. Páginas 901-907. Disponível em: https://doi.org/10.1016/j.clsr.2018.05.013 Acesso em: 06 mai. 2021.