OS OBSTÁCULOS DA INVESTIGAÇÃO DOS CRIMES DIGITAIS

Edilson Carlos Lima Correa Junior[61]

RESUMO: A partir da pandemia do Covid-19, as pessoas passaram a realizar suas atividades através de dispositivos eletrônicos a fim de evitar a aglomeração social. Os crimes praticados nas ruas sofreram relevante diminuição, contudo os crimes informáticos ou cibernéticos aumentaram vertiginosamente. Os recursos e as técnicas utilizados, atualmente, pelas polícias judiciárias não estão sendo suficientes para conter os criminosos virtuais, sobretudo em razão de uma série de peculiaridades exigidas na investigação dos crimes digitais. As facilidades encontradas para abertura de contas bancárias e habilitações de linhas telefônicas, a necessidade de decisões judiciais para quebras de sigilo, a falta de colaboração de quem detém as informações necessárias, a distância geográfica entre os envolvidos no crime, a criptografia de aplicativos de conversas, entre outros obstáculos, tornam a investigação de crimes cibernéticos especialmente complexa. Mediante uma análise qualitativa do problema, propõe-se a criação de uma agência central, de âmbito nacional, como forma de conter o avanço da criminalidade virtual.

Palavras-chave: Crime Cibernético. Pandemia. Investigação Policial. Obstáculos. Solução.

OBSTACLES IN THE INVESTIGATION OF DIGITAL CRIMES

ABSTRACT: From the Covid-19 pandemic, people started to carry out their activities through electronic devices in order to avoid social agglomeration. Crimes committed on the streets suffered a significant decrease, however, computer or cybernetic crimes increased dramatically. The resources and techniques currently used by the judicial police are not being enough to contain cyber criminals, mainly due to a series of peculiarities required in the investigation of digital crimes. The facilities found for opening bank accounts and enabling telephone lines, the need for judicial decisions to breach secrecy, the lack of collaboration on the part of those who hold the necessary information, the geographic distance between those involved in the crime, the encryption of conversation applications, among other obstacles, make the investigation of cybercrime especially complex. Through a qualitative analysis of the problem, it is proposed the creation of a central agency, nationwide, as a way to contain the advance of cybercrime.

Keywords: Cybercrime. Pandemic. Police investigation. Obstacles. Solution.

INTRODUÇÃO

Os chamados crimes digitais, informáticos, cibernéticos ou simplesmente *e-crimes* são aquelas infrações penais praticadas contra ou com a utilização de um dispositivo eletrônico. Os mais comuns são aqueles que se valem da rede mundial de computadores, a internet, como meio de transmissão

61 Delegado de Polícia em Minas Gerais. Especialista em *Cybercrime* e *Cybersecurity* pelo Centro Universitário Internacional Signorelli.

dos dados maliciosos, causando uma ofensa a um bem jurídico tutelado.

Como exemplos dessa espécie de crime, temos o furto eletrônico (art. 155, § 4º-B, CP), a fraude eletrônica (Art. 171 § 2º-A, CP), a extorsão, quando praticada mediante uso de dispositivos eletrônicos, como no caso da "sextorsion"[62] ou do "ramsonware"[63] (Art. 158, CP), os crimes contra a honra, também quando praticados com a utilização de tais dispositivos (Arts. 138, 139 e 140, CP), a divulgação de cena de estupro (Art. 218-C, do CP), a invasão de dispositivo informático (Art. 154-A, do CP), entre outros.

A prática de delitos cibernéticos costumava ser esporádica, sobretudo antes da popularização dos *smartphones*. Ocorre que, em 11 de março de 2020, a Organização Mundial da Saúde (OMS) classificou o surto do Coronavírus como pandemia e, como forma de conter o avanço da doença, as autoridades públicas determinaram medidas sanitárias, como o distanciamento social, a quarentena e o *lockdown*, o que fez com que as pessoas "informatizassem" suas atividades. Aulas, reuniões de negócios, audiências judiciais, etc., passaram a ser virtuais ou transmitidas por videoconferência.

Dentro do possível, as pessoas deixaram de circular nas ruas e passaram a realizar suas tarefas em casa, através do computador ou celular. Nesse diapasão, o crime, como fato social que é, teve que se adaptar à nova realidade, gerando, por um lado, a diminuição dos crimes de furtos e roubos a transeuntes, mas, por outro, um aumento de mais 200% dos crimes virtuais, somente no ano de 2020, conforme dados do CEACrim-SP (FERREIRA, 2022). Em consulta ao Sistema REDS[64] de Minas Gerais, verificou-se um aumento de 21% (vinte e um porcento) em relação aos crimes de estelionato, sendo a maior parte deles praticada com uso da internet.

Dessarte, considerando o aumento no índice de crimes praticados, atualmente, com uso de dispositivos informáticos, não há como negar a necessidade de implementação de estratégias para aprimorar a investigação e repressão desses delitos.

DOS OBSTÁCULOS À INVESTIGAÇÃO DE CRIMES DIGITAIS

1 – Peculiaridades da investigação cibernética

Praticada uma infração penal, as instituições constituídas precisam tomar medidas para reprimi-la. Cabe à Polícia Civil apurar a autoria e a materialidade delas por meio de um procedimento investigatório, normalmente, o Inquérito Policial. A investigação dos crimes cibernéticos, por sua vez, possui certas peculiaridades que a tornam especialmente desafiadora. Uma das causas dessa especificidade é que a proteção constitucionalmente conferida ao direito à intimidade e à privacidade, bem como o trato com os dados pessoais, exige certos requisitos e formalidades que dificultam ou, no mínimo, atrasam a investigação policial. E a mera demora no fornecimento das informações necessárias à apuração da autoria delitiva, em alguns casos, pode acarretar o fracasso da investigação.

Imaginemos um caso em que um estelionatário, utilizando um aparelho celular habilitado com dados de terceira pessoa, se desfaça do aparelho algum tempo depois do crime e não mais volte a usá-lo. A demora na obtenção de uma decisão judicial concedendo a interceptação telefônica ou relação de chamadas do IMEI (do inglês *International Mobile Equipment Identity*) do aparelho do investigado, por exemplo, pode tornar a ordem judicial sem proveito. O mesmo ocorre quando há lentidão na autorização para bloqueio de valores em uma conta bancária aberta, também em nome de um "laranja", para o único fim de praticar delitos e, depois de sacar os valores, não mais a utiliza. Muitas vezes, também, uma empresa

62 Sextorsion, ou sextorsão, é a modalidade criminosa em que se coage alguém a fazer algo sob ameaça de divulgação de imagens íntimas, normalmente, obtidas de forma ilícita. O objetivo pode ser vingança, humilhação ou uma vantagem financeira.

63 Ramsoware é o sequestro de dados telemáticos mediante criptografia em que se exige, como resgate, o pagamento de determinado valor, normalmente na forma de criptoativos.

64 Sistema de Registros de Defesa Social do Estado de Minas Gerais. Consulta realizada em 10/01/2023.

detentora de uma informação, ou mesmo uma imagem de câmera de segurança, exige que os requerimentos policiais sejam analisados pelo setor jurídico, resultando em morosidade no atendimento do pedido.

2 – Facilidade de abertura de contas bancárias e habilitação de linhas telefônicas

Outro fator a ser destacado é que, hoje em dia, instituições bancárias e operadoras de telefonia, na ânsia de angariar novos clientes, simplesmente não exigem sequer a cópia de um documento de identidade ou um comprovante de residência para abertura de contas bancárias e linhas telefônicas, e, quando o fazem, muitas vezes, não exigem que as fotografias sejam tiradas "ao vivo", admitindo fotos guardadas na galeria do celular, o que permite que os criminosos consigam abrir diversas contas bancárias digitais utilizando, até mesmo, fotos de documentos de terceiros.

Essa facilidade na abertura de contas bancárias cria também a necessidade de diversas autorizações judiciais para se chegar ao último beneficiário de eventuais valores angariados com o crime, já que um criminoso pode abrir várias contas e transferir valores de uma para outra, fazendo com que sejam necessários consecutivos pedidos de quebra de sigilo a fim de se tentar chegar ao verdadeiro responsável pela infração penal.

Quase todos os crimes informáticos patrimoniais com que nos deparamos nos últimos meses foram praticados utilizando linhas telefônicas e contas bancárias fraudulentas[65], o que demonstra a falta de cuidado das empresas que operam nessas áreas.

3 – Necessidade de autorização judicial

O artigo 5º, inciso XII, da Constituição Federal preconiza que *"é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal"*. Garantiu-se, assim, o sigilo das comunicações entre as pessoas, bem com a troca de dados telemáticos, limitando sua quebra às causas criminais e mediante ordem judicial.

A imprescindibilidade de autorizações judiciais, nesses casos, visa a proteger a privacidade e intimidade das pessoas. Ocorre que essa garantia constitucional tem sido usada como escudo em favor dos criminosos virtuais. É que o grande número de casos em detrimento de um pequeno contingente de servidores policiais, sobretudo especializados na matéria, torna prejudicada uma atuação mais eficiente dos órgãos de investigação.

A fim de ilustrar, imaginemos que um estelionatário utilize uma linha telefônica, uma rede social e uma conta bancária para aplicar um golpe (e normalmente são utilizados esses três recursos conjuntamente). Nesse caso, serão necessárias três quebras de sigilo específicas. Claro que elas podem ser reunidas em um único pedido, mas é comum ocorrer, por exemplo, que um determinado endereço IP seja obtido após a quebra de sigilo de uma conta do *Facebook*, exigindo nova representação ao judiciário para que um provedor informe a quem pertence aquele IP. Assim, entre a representação da vítima na delegacia e a obtenção de todos os dados necessários à identificação do agente, há um período que pode chegar a semanas.

Ainda assim, mesmo de posse dos dados cadastrais de determinado endereço IP, é possível que se chegue à conclusão de que o criminoso utilizou um celular com dados móveis (e não um ponto de internet fixo) para a prática do delito e que a linha telefônica esteja habilitada em nome de uma terceira pessoa, a qual sequer tinha conhecimento que seus dados haviam sido utilizados para esse fim.

Nesse caso, seria possível, por exemplo, a interceptação telefônica do IMEI do celular, antes que o agente se desfaça do dispositivo, a fim de se tentar averiguar outras linhas telefônicas utilizadas

65 Observação verificada empiricamente, a partir dos casos ocorridos na circunscrição da Delegacia de Polícia Civil da Comarca de Morada Nova de Minas.

por ele no mesmo aparelho, o que pode levar à sua identificação. Daí a importância da celeridade na investigação.

Observe que, para essa interceptação, também é necessária uma autorização judicial. Assim, em um único caso, tivemos três pedidos de quebra de sigilo, os quais não podem ser feitos em um único momento. O primeiro para obter o IP da conta de Facebook, o segundo para obter os dados do provedor em relação àquele IP e o terceiro para a interceptação telefônica do IMEI do aparelho utilizado. Além disso, possivelmente será necessária outra decisão judicial autorizando, por exemplo, a busca e apreensão no imóvel de eventual suspeito para obtenção de provas e apreensão de dispositivos eletrônicos, os quais, para serem periciados, também requerem autorização da justiça.

No que tange ao endereço IP, há certa divergência quanto à necessidade de alvará judicial. É que a informação sobre o IP, para alguns, é considerada como um desdobramento dos dados cadastrais, tal como o endereço de uma pessoa e, portanto, passível de ser fornecida independentemente de intermediação do judiciário. O endereço IP, nos termos do marco civil da internet, é *"o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais"*. Assim, há quem sustente que tal informação estaria inserida entre os dados cadastrais de um usuário. Embora predomine o entendimento de que o fornecimento de tais registros esteja condicionado à autorização judicial, a maioria dos provedores de internet têm fornecido os dados cadastrais, com base no endereço IP, mas há aqueles que se esquivam alegando o disposto no artigo 10, §1º, da Lei n.º12.965/14 (marco civil da internet).

De qualquer forma, essa necessidade de consecutivas decisões judiciais cria sérios entraves à rápida apuração do delito. Sobretudo se considerarmos que nem todas as comarcas são providas de juiz titular, sendo que os magistrados que atuam em cooperação não estão sempre disponíveis, havendo casos em que a supressão da lacuna ocorre apenas uma vez por semana, o que torna o problema ainda mais grave.

4 – Falta de colaboração de quem detêm os dados

Mesmo de posse de uma ordem judicial, ou ainda, no caso de dados cadastrais não resguardados pela reserva de jurisdição, não é raro se deparar com a falta de cooperação das entidades que detêm as informações requeridas. Além das incontáveis horas despendidas com a busca pelos canais de atendimento de instituições bancárias ou provedores de internet menos conhecidos, diversas também foram as vezes em que já foi necessário reiterar os pedidos enviados a eles, mesmo existindo norma que prevê como crime o descumprimento das requisições feitas no curso de uma investigação criminal (art.21 da Lei n. º12.850/13).

Na maioria dos casos, como já aludido, as empresas recebem os pedidos e repassam aos respectivos departamentos jurídicos, os quais demoram dias ou até semanas para analisarem e responderem às demandas. Não há como culpá-las também. É certo que recebem requisições de todo o país, e o volume de pedidos, somado às demais atribuições que já detêm, torna a demora compreensível.

5 – Criptografia de ponta-a-ponta

Outro grave problema (e talvez o mais comum) enfrentado não apenas por quem investiga o crime informático, mas quase todos os tipos de delitos, é a impossibilidade de quebra da criptografia de ponta-a-ponta do aplicativo de mensagens *Whatsapp*. É difícil encontrar alguém que possua um telefone celular e que não utilize esse aplicativo. Assim, a interceptação das mensagens e ligações telefônicas do *Whatsapp* poderia ser extremamente útil na identificação e localização dos criminosos virtuais ou obtenção de provas. Ocorre que, segundo a empresa criadora do aplicativo, a criptografia utilizada na troca de dados entre os usuários não pode ser quebrada, fazendo com que não seja possível tal interceptação.

Sabendo disso, os malfeitores optam por realizar chamadas telefônicas e troca de mensagens por meio desse aplicativo, tornando, em muitos casos, inócua a investigação por interceptação telefônica convencional, a qual abrange apenas chamadas comuns das operadoras de telefonia.

6 – Falta de softwares especializados

Ainda que se tenha acesso ao telefone celular do investigado, na maioria dos casos, o dispositivo está bloqueado com senha, não sendo possível o acesso ao aparelho. Mesmo por meio de *softwares* avançados, como o *Cellebrite*, muitas vezes não se tem êxito no desbloqueio do aparelho. A própria empresa responsável pelo referido *software* informa que há limitações quanto ao desbloqueio, dependendo da versão do sistema operacional utilizado. Cumpre ressaltar também que, em razão do alto custo da licença e atualização deste tipo de *software*, os órgãos de investigação contam com apenas uma central de extração de dados, havendo uma enorme fila de espera, o que acarreta demora na obtenção dos dados. E, como já vimos, a demora na obtenção da informação pode levar ao fracasso da investigação. Não é raro ocorrer casos em que o resultado da extração de dados chega à unidade policial após a condenação ou absolvição do investigado.

7 – Distância geográfica entre as partes e necessidade de precatórias

Não se pode deixar de listar, entre as dificuldades da investigação de crimes digitais, a distância geográfica entre o local de residência da vítima e a real localização do autor do crime, ou entre o local de apuração do crime e o local onde vítima e autor se encontram. Como os crimes normalmente ocorrem por meio da internet, quase nunca os locais onde vítima e investigado residem ou se encontram são coincidentes. Com isso, temos não apenas o problema de identificar o juízo competente para apurar a infração penal (o que veremos mais à frente), mas também sérios entraves relacionados às oitivas dos envolvidos, as quais, quase sempre, dependem da expedição de cartas precatórias que levam meses (quando não anos!) para serem cumpridas e juntadas aos autos, isto quando retornam às comarcas deprecantes.

Além das dificuldades em relação às oitivas, tem-se ainda a dificuldade de representar e cumprir mandados de busca e apreensão para obtenção de provas. Imaginemos um caso de extorsão eletrônica em que o agente reside em Porto Alegre-RS e está coagindo uma vítima que reside em Uberlândia-MG, através de ligações telefônicas. O juízo mineiro será competente para a apuração, já que o crime de extorsão se consuma no momento em que a vítima é constrangida. O delegado responsável pela apuração, caso entenda necessário, terá que representar à justiça mineira pela busca e apreensão na residência de um suspeito, a fim de verificar se o IMEI de seu telefone celular é o mesmo do dispositivo utilizado no crime. Ocorre que o cumprimento do referido mandado terá de ser realizado na capital gaúcha, normalmente com o apoio do órgão policial de lá, após o aval da justiça competente em relação ao local da diligência. Desse modo, a investigação levada a efeito em um local dependerá da ação de outra agência policial, a qual não está familiarizada com os pormenores da investigação, podendo não se atentar para detalhes que apenas os policiais do caso conhecem.

8 – Dificuldade de cooperação internacional

É possível ainda que os agentes, valendo-se das facilidades da Internet, pratiquem delitos com efeitos no país, mas encontrando-se no exterior, o que torna o sucesso da investigação ainda mais improvável, já que, embora o Brasil seja signatário da Convenção de Budapeste, a qual prevê a cooperação internacional em matéria de crimes digitais, as ferramentas nela previstas não estão em operação por aqui, como a denominada "REDE 24/7", a qual seria um ponto de apoio em cada Estado signatário para aconselhamento técnico, preservação de dados e coleta de provas. Desse modo, ainda são necessárias cartas rogatórias ou intermediação do Ministério Público Federal para pedidos internacionais.

9 – Indefinições quanto à competência jurisdicional

Internamente, a questão do juízo competente já sofreu diversas mudanças legislativas e jurisprudenciais, sobretudo no crime de estelionato, tendo sido, recentemente, definido no artigo 70, §4º do CPP que, *"nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção"* (alterado pela Lei n.º14.155/21).

Fora desses casos específicos do estelionato, a regra, no entanto, é que a competência será definida pelo local da consumação do delito. Então, por exemplo, no caso de um furto eletrônico (art. 155, § 4º-B, CP), em que o agente viola o mecanismo de segurança da conta bancária da vítima e subtrai determinada quantia dela, o juízo competente é o local onde ocorre a inversão da posse dessa quantia, isto é, o local onde está sediada a conta bancária beneficiária, o qual pode ou não coincidir com a residência do autor. Como visto, a facilidade de abertura de contas bancárias permite que o dinheiro angariado com o crime seja recebido, transferido e repartido entre diversas contas bancárias sediadas em diferentes localidades.

Embora pareça claro que a inversão do ônus da posse ocorra apenas quando os valores subtraídos efetivamente sejam depositados na conta beneficiária (nesse sentido: STJ - CC181538/SP[66]), há diversos entendimentos no sentido de que o juízo competente para julgamento é o do local da conta fraudada (STJ - RHC 84622/PR[67]). Como visto, a questão não é pacífica nem internamente em um mesmo órgão jurisdicional. Cumpre ressaltar que, caso a conta fraudada pertença a uma empresa pública da União, como a Caixa Econômica Federal, a competência para julgamento é da Justiça Federal e, portanto, a investigação competirá à Polícia Federal.

É possível ainda, e até rotineiro, que a infração penal envolva mais de um autor, ou que sejam diversas as subtrações para contas diversas, as quais podem estar sediadas em locais distintos. Assim, além das diversas precatórias necessárias para ouvir os suspeitos e beneficiários, ainda será necessário certo esforço para se definir a competência territorial e, por sua vez, a unidade policial com atribuições para a investigação.

10 – Insuficiência do número de unidades especializadas

Por fim, tem-se ainda, como entrave na investigação dos crimes digitais, a ausência de equipes policiais especializadas nesta área para atender o volume de demandas que chega todos os dias. Como visto, a pandemia fez com que o número de casos de crimes virtuais disparasse. O mesmo não ocorreu, contudo, em relação às unidades policiais de combate aos crimes cibernéticos, pelo menos não na mesma proporção. De igual modo, não se viu a destinação de recursos específicos para o setor, como aquisição de computadores de ponta e *softwares* próprios de extração e análise de dados, sobretudo nas unidades do interior dos Estados.

POSSÍVEL SOLUÇÃO PARA O PROBLEMA

Como visto, são diversos os entraves à investigação de crimes digitais. Uma possível solução para alguns dos problemas listados acima é a criação de um órgão central de investigação cibernética, de âmbito nacional, com integrantes de todas as Polícias Civis, para o qual todas as ocorrências envolvendo infrações penais desta natureza seriam destinadas.

Um primeiro escopo deste órgão seria a unificação da investigação sobre determinados alvos coincidentes. Nas diversas investigações de crimes cibernéticos já realizadas, sobretudo nas que caracterizam fraudes com fins patrimoniais,

66 In https://www.portaljustica.com.br/acordao/2545218.
67 In https://www.jusbrasil.com.br/jurisprudencia/stj/339952309.

verificamos que os criminosos passam o dia aplicando golpes ou subtrações, fazendo diversas vítimas espalhadas por todos os Estados da Federação. A unificação pretendida poderia identificar tais alvos através das coincidências de linhas telefônicas, contas bancárias e endereços de IP utilizados por eles, permitindo, ainda, verificar o real prejuízo que eles causaram, a fim de realizar uma melhor dosimetria das penas.

A identificação de um alvo responsável por diversos delitos reduziria drasticamente o número de pedidos de autorizações judiciais necessárias, já que é provável que as diversas agências policiais representem pela quebra de sigilo de um mesmo alvo, separadamente, várias vezes. Indo mais longe, diante da concentração desses diversos pedidos em um só, poderia ser apresentado um projeto ao Judiciário, para que fosse criada uma vara exclusiva para apreciar pedidos de quebra de sigilo de investigações em andamento, de forma especializada e célere. Desse modo, teríamos um verdadeiro Juiz de Garantias, atendendo ao anseio da lei já existente, além de conferir mais efetividade ao sistema acusatório.

Até as requisições às entidades privadas como bancos, operadoras de telefonia e provedores de internet poderiam ser concentradas, de modo a manter um canal de contato direto entre elas e o órgão central. Seria mais fácil ainda se houvesse a criação e a constante atualização de um cadastro central com os contatos dessas entidades, o que economizaria várias horas de buscas pelos canais de atendimento.

Além disso, a centralização da investigação em um órgão especializado reuniria servidores mais capacitados, maquinário mais moderno e softwares mais atualizados, gerando economia para os cofres públicos. Por exemplo, em vez de cada unidade federativa ter que adquirir uma atualização do *Cellebrite*, isso poderia ser feito uma única vez, com o custo repartido entre os 26 (vinte e seis) Estados e o Distrito Federal, mantendo o sistema sempre atualizado.

Os conhecimentos técnicos específicos e as práticas de investigação que deram certo no combate aos crimes digitais, nos diversos órgãos policiais, seriam somados, passando a ser aplicados a todos os casos de forma uníssona. Poderia ainda ser elaborado um Procedimento Operacional Padrão-POP, de nível nacional, para a investigação dessa espécie de infração penal. E poderia também ser mantido um cadastro nacional de criminosos e hackers conhecidos e seus *modus operandi,* o que tornaria a investigação ainda mais eficaz.

Essa agência centralizada poderia estar sediada em qualquer parte do país. O limite geográfico de um Estado não pode ser barreira para a investigação já que, como visto, o crime cibernético não conhece esses limites. Mas também seria possível, com as tecnologias já existentes, a manutenção desse órgão central até mesmo de forma remota, permanecendo cada equipe em sua respectiva unidade, mas com atribuições específicas e com compartilhamento de dados e informações de forma ininterrupta com as demais através de videoconferências e outros recursos.

Seria até mais interessante que seus integrantes estivessem espalhados pelo maior número de locais possíveis, de modo a permitir que fossem feitas diligências de campo, oitivas e interrogatórios necessários, sem depender da expedição de precatórias, o que eliminaria, como visto, uma das maiores dificuldades enfrentadas na investigação dos *e-crimes*.

CONSIDERAÇÕES FINAIS

Enquanto não forem tomadas medidas contundentes contra a criminalidade cibernética, continuaremos assistindo ao aumento no número de casos, os quais trazem graves danos às vítimas. Além disso, a descrença da sociedade em relação às instituições de segurança, causada pela impunidade que ainda prevalece em relação a tais infrações penais, não pode ser desconsiderada. É preciso que se reverta não apenas a proporção de casos solucionados, a qual ainda é bem inferior aos arquivados sem indiciamento, mas também que se consiga uma resposta mais célere, a fim de se tentar minorar os danos sofridos pelas vítimas.

A rápida apuração da autoria delitiva permite uma maior probabilidade de sucesso quanto a bloqueios de ativos ilicitamente angariados, no caso de crimes patrimoniais, e se evita a propagação de eventuais crimes contra a honra, intimidade, privacidade, etc.

A solução proposta neste trabalho, relativa à criação de um órgão central, é economicamente viável e pode ser facilmente implementada, bastando ser apreciada e aprovada pelo Conselho Nacional dos Chefes de Polícia. Acreditamos que seja uma alternativa que poderia trazer enormes benefícios à investigação criminal.

Dos problemas apresentados, o único que não é solucionado pela implantação de um órgão central é a questão da criptografia do *Whatsapp*, para o que ainda não se descobriu uma solução que garantisse, ao mesmo tempo, o sucesso da investigação criminal e a preservação dos direitos fundamentais. Contudo, os principais objetivos de uma almejada interceptação de mensagens e ligações, feitas através desse aplicativo, são a obtenção de provas e a identificação do agente, o que, como visto, poderá ser concretizado por outros meios, a partir da criação desta agência de âmbito nacional, com mais eficiência do que vem sendo hoje realizado, de forma isolada, pelas Polícias Civis de cada ente federativo. ■

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Constituição da República Federativa do Brasil:** promulgada em 5 de outubro de1988.

BRASIL. **Decreto-Lei 2.848, de 07 de dezembro de 1940.** Código Penal. Diário Oficial da União, Rio de Janeiro, 31 de dezembro de 1940.

BRASIL. **Decreto-Lei nº 3.689, de 03 de outubro de 1941.** Código de Processo Penal. Diário Oficial da União, Rio de Janeiro, 13 de Outubro de 1941.

BRASIL. **Lei n. 12.850, de 02 de agosto de 2013.** Código Civil. Diário Oficial da União, Brasília, 05 de agosto de 2013.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014.** Código Civil. Diário Oficial da União, Brasília, 24 de abril de 2014.

BRASIL. **Lei n. 14.155, de 27 de maio de 2021.** Código Civil. Diário Oficial da União, Brasília, 28 de maio de 2021.

CASELLI, Guilherme. **Manual de Investigação Digital.** 2. ed. São Paulo: Editora JusPodivm, 2022.

COUNCIL OF EUROPE. ***Convention on Cybercrime***. Versão em português. Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa428>. Acesso em: 08 jan. 2023.

DUQUE, Nayara Caetano Borlina. **Fraudes bancárias praticadas por meios eletrônicos – Importância da análise de vínculo na cognição investigativa.** In: Relatos sobre a investigação de crimes cibernéticos. São Paulo: Editora JusPodivm, 2022.

FERREIRA, Rafaela. **Aumento do uso da internet faz crescer o número de crimes cibernéticos.** [S.l.] 2022. Disponível em: https://www.jornalopcao.com.br/ultimas-noticias/aumento-do-uso-da-internet-faz-crescer-o-numero-de-crimes-ciberneticos-374687/. Acesso em: 13 jan. 2023.

FREITAS JUNIOR, Dário Taciano; LYRA NETO, Luiz Pereira. Investigação tecnológica em crime de ***sextortion***: Estudo de caso. In: Relatos sobre a investigação de crimes cibernéticos. São Paulo: Editora JusPodivm, 2022.

FREITAS, Sabryna de Souza. **Cibercriminalidade:** Um vírus fortalecido pela Pandemia. In: Direito Policial – Temas Atuais. Salvador: Editora JusPodivm, 2021.