ANÁLISE SOBRE AS DIFICULDADES DE INVESTIGAÇÃO RELACIONADAS AOS CRIMES CIBERNÉTICOS DE ESTELIONATO NA REDE SOCIAL WHATSAPP

SILVA, Moacir Antunes [a] ; CARVALHO, Urssula Rodrigues [b]

[a] moacirantunnessilva@gmail.com
[b] ursulla.carvalho@unifagoc.edu.br

[a] *Graduando em Direito*
[b] *Especialista em Direito Público– Analista Judiciária – Professora – UNIFAGOC*

RESUMO

Este estudo objetivou analisar as dificuldades de investigação do crime de estelionato no âmbito do WhatsApp. Por meio de revisão bibliográfica e pesquisa em fontes secundárias, pode-se perceber como aumentou paralelamente o uso do WhatsApp com a prática de crimes de estelionato através desse aplicativo, considerando a utilização da função PIX. Constatou-se que é necessário que policiais tenham uma qualificação considerável, dasda a dificuldade de encontrar os criminosos. Assim, há, inclusive, delegacias especializadas só nese âmbito. Percebeu-se o quanto é difícil identificar o patrimônio da vítima do crime, considerando a forma que utilizam para blindarem sua localização, sendo praticamente impossível sua restituição. Com base em tudo que foi pesquisado, insta salientar a gravidade da ação por parte dos criminosos quanto à invasão de informações e ao acesso a todos os dados da rede social da vítima, facilitando crimes posteriores.

Palavras-chave: *Crimes Cibernéticos. Inviolabilidade. Investigação. Combate.*

INTRODUÇÃO

Na sociedade brasileira, percebe-se um aumento significativo do uso de celulares e computadores, principalmente com o advento da COVID-19. Paralelamente, foi significativo o aumento de fraudes nesse âmbito, atrelado a uma crise financeira, bem como à facilidade de burlar os meios tecnológicos para se fazer passar por determinadas pessoas, fazendo com que criminosos se utilizem dessa falha para o cometimento de crimes.

Segundo Marin (2022), ao menos 43% dos usuários do WhatsApp sofreram com fraudes através dessa plataforma, em que a prática mais comum é a utilização de um perfil falso, em que o criminoso usa fotos de uma pessoa conhecida da vítima em uma rede social e faz-se passar por ela, solicitando transferências de dinheiro ou ajuda financeira.

Inevitavelmente, o aplicativo revolucionou a vida das pessoas, bem como de empresários e empresas que utilizam essa plataforma como marketing e na compra e venda de produtos. Segundo DG Solutions 2022, o WhatsApp possui quase 11 (onze) anos de existência. Já o WhatsApp Business, que foi lançado em meados de 2018, permite a criação de um perfil empresarial, com descrição de produtos, mensagens automáticas, análise estatística sobre o envio, recebimento e leitura das conversas.

Assim, é possível perceber uma função voltada para o marketing e trabalho

empresarial, considerando a facilidade e as funções voltadas para um uso mais adequado das pessoas deste ramo.

O agente na prática do crime de estelionato tem como objetivo principal o patrimônio da vítima, cuja vantagem indevida se dá por meio enganoso ou fraudulento, conforme se depreende da leitura do artigo 171 do Código Penal (BRASIL, 1940).

Dessa forma, analisando a conceituação do crime de estelionato junto à sua prática via WhatsApp, é possível perceber a sagacidade do agente para aplicação nesse âmbito, coniderando a necessidade de conhecimento prévio entre a vítima da ação e a suposta pessoa pela qual o agente se faz passar. Paralelamente a isso, está a dificuldade na investigação e possibilidade de estorno do patrimônio adquirido de forma indevida, considerando que o agente que pratica o ato imediatamente já repassa valores para contas diversas. Ainda que quisesse, o banco não poderia informar tal caminho percorrido pelo dinheiro, considerando a violação de direitos constitucionais assegurados, ressalvada a possibilidade de decisão judicial autorizando.

O presente estudo tem como objetivos específicos apresentar a sistemática das investigações no âmbito da prática do crime de estelionato através da plataforma WhatsApp, como ela de fato acontece, quem investiga e qual é a competência policial nesses casos. Analisará, à luz da Constituição, a relação desse crime com o princípio da inviolabilidade do domicílio e da privacidade, abordando como de fato esses princípios são violados de forma velada com a prática deses crimes. Isso porque, dependendo da forma como é praticado, ocorre a invasão do domicílio da vítima, bem como de dados pessoais e íntimos, sem que ela perceba ou até mesmo saiba como isso ocorreu. Sendo assim, o intuito da presente pesquisa é apresentar formas de inibir/diminuir as dificuldades nas investigações desses crimes, considerando a gravidade e a quantidade dessa prática nos dias atuais.

Dessa forma, o presente estudo se justifica diante da necessidade de informações sobre a prática de crimes cibernéticos, mais especificamente, o estelionato. Nesta senda, o presente estudo abordará algumas nuances desta prática e as formas que se tem de investigar e seus resultados, diante da posterior inversão do patrimônio da vítima em favor do estelionatário.

O presente estudo tem como problema de pesquisa a seguinte questão: quais as dificuldades de investigação no crime de estelionato praticado através da plataforma WhatsApp?

Assim, o objetivo geral deste estudo consiste em analisar as dificuldades quanto à investigação do crime de estelionato e como ele de fato acontece, no âmbito do WhatsApp.

Trata-se de um ensaio teórico, no qual, para o alcance do objetivo proposto, a metodologia empregada foi a revisão bibliográfica e pesquisa em fontes secundárias, que consiste no levantamento de material já elaborado e publicado em documentos, tais como livros e revistas, com vista a explicar um problema com base em referências teóricas.

A PRÁTICA DO CRIME DE ESTELIONATO VIA WHATSAPP NO BRASIL

É possível perceber um aumento significativo na prática do delito de estelionato praticado via WhatsApp no Brasil, considerando a facilidade que os agentes possuem de efetuar tal ato.

Essa prática se realiza, reincidentemente, com o mesmo modus operandi, ou seja, ocorre com todas as vítimas da mesma forma. O agente obtém uma foto de um dos contatos da vítima – na maioria das vezes, são pessoas mais próximas, como familiares ou amigos íntimos – e a coloca como foto de perfil da rede social WhatsApp. Em seguida, ainda que com um número de telefone diverso do que essas pessoas usam, inicia uma conversa com a vítima e já solicita uma quatia em dinheiro, via PIX ou transferência bancária.

Devido ao trâmite dessa nova forma de transferência, qual seja, o PIX, implantada recentemente pelo Banco Central - BACEN, ficou ainda mais fácil, considerando que, logo após a vítima realizar tal transferência, o dinheiro vai imediatamente para a conta mencionada pelo agente realizador de tal conduta descrita, restando, em tese, impossível estorná-lo.

Segundo Branco (2021), as instituições bancárias, no fim do ano de 2021, comoveram-se com tal situação e criaram a possibilidade de estornar esse valor que foi transferido de forma fraudulenta. Porém, analisando de forma ampla a logística das instituições, é necessário haver dinheiro na conta para a qual o PIX foi endereçado. Fato comprometedor, considerando a malícia dos agentes, pois, imediatamente após a transferência, já transferem o valor recebido para outra conta, dificultando eventual bloqueio de valores recebidos. Branco (2021)

Ainda conforme Branco (2021), a maioria das instituições bancárias não estorna, tampouco investiga a situação quando o PIX é proveniente de erro, realizado incorretamente. Assim, em vez de ir diretamente ao fato da transferência fraudulenta, as instituições realizam uma investigação prévia, com o fim de buscar provas do golpe. Essa investigação é feita para vítimas que, eventualmente, erram a chave no momento da transferência via PIX e alegam ter sofrido fraudes, fato que, se constatado pela instituição, descarta totalmente a possibilidade do estorno. A Caixa Econômica Federal - CEF afirma que, se ficar comprovada a fraude, garante que o estorno será realizado em benefício do usuário. Quanto às possibilidades de estorno criadas por essas instituições, o procedimento varia de instituição para instituição (BRANCO, 2021).

Essa hipótese de estorno foi criada com o objetivo de diminuir o prejuízo das vítimas, considerando que, em um levantamento da PSafe, em 5 dias de dezembro de 2021, mais de 500 mil tentativas de golpes, via PIX, foram realizadas (BRANCO, 2021).

Cabe ainda salientar que o crime está descrito no artigo 171 do Código Penal (BRASIL, 1940): "Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento", prevendo, em seu preceito secundário, uma pena de reclusão de um

a cinco anos, e multa, de quinhentos mil réis a dez contos de réis. Todavia, considerando o fato de o assunto aqui tratado ser de uma maior reprovabilidade, bem como pela forma reincidente como vem acontecendo, a Lei nº 14.155 de 2021 trouxe uma inovação para o Código em questão, de modo que seja mais prejudicial ao agente que pratica o delito, Ex positis:

> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (BRASIL, 2021).

Sendo assim, como dito, percebe-se que a conduta praticada se amolda igualmente ao modus operandi dos agentes mencionados, que utilizam a foto de uma das pessoas listadas nos contatos da vítima como perfil do WhatsApp e, em nome dela, solicitam dinheiro ou qualquer outro benefício.

Não obstante, com a novatio legis in pejus, incluindo o §2º - A no artigo 171 do Código Penal (BRASIL, 2021), essa conduta se torna qualificada, ou seja, no caso da dosimetria da pena, o juiz já inicia a primeira fase, ainda que com todas as circunstâncias judiciais favoráveis do artigo 59 do Código Penal (BRASIL 1940), com uma pena mínima de 4 (quatro) anos, sendo que o agente que pratica o delito do caput do artigo 171 desse código (BRASIL 1940) inicia sua primeira fase (considerando as circunstâncias judiciais favoráveis) com uma pena mínima de 1 (um) ano.

COMO AS INVESTIGAÇÕES ACONTECEM NA PRÁTICA

As investigações dos crimes informáticos são desafiadoras, conforme Moura (2021) bem salienta. Todavia, não são impossíveis, considerando que as investigações já ocorrem com bastante força e dedicação e que há casos que encontram os autores do crime. Assim, a internet não pode ser considerada como uma plataforma de impunidade.

Os crimes cibernéticos, por si sós, exigem uma atenção e um cuidado ainda maior nas investigações, devido à gama de formas de praticá-los. Segundo Moura (2021), em 1988 houve uma primeira forma de invasão cibernética, quando Mathias Spéer invadiu 450 computadores militares nos EUA, Japão e Europa. Moura (2021) afirma ainda que houve mais duas invasões promissoras, quais sejam, uma em 1995, em que Vladmir Levin invadiu o Citibank e desviou 2,8 milhões de dólares e outra em 18/06/1999, quando houve uma invasão das páginas do Supremo Tribunal Federal (STF) e do Planalto. Até os dias atuais, percebe-se um aprimoramento no modo de praticar crimes cibernéticos.

Um marco com o fim de sanar invasões cibernéticas no Brasil, bem como de reprimí-las, foi a publicação da Lei Carolina Dieckemann – Lei 12.737/2012 (BRASIL, 2012). A Lei se deu em virtude de a atriz ter fotos íntimas divulgadas na rede mundial de

computadores. Ademais, ainda que com a aprovação precoce, segundo Moura (2021), não houve qualquer diminuição no número de crimes informáticos; muito pelo contrário, o aumento da criminalidade nesse âmbito ainda é um problema, visto que não há uma mudança no comportamento dos usuários.

Diante da clara necessidade de atualização e conhecimento no âmbito da tecnologia da informação, a legislação deu mais um passo nesse sentido, considerando a publicação do Pacote Anticrime – Lei 13.964/2019 (BRASIL, 2019), em que se acrescentou o artigo 10 – A na Lei 12.850/2013 – Lei de Organização Criminosa (BRASIL, 2013), prevendo a possibilidade da investigação undercover, também conhecida como infiltração policial. Nesse ínterim, a publicação de tal Lei, conforme Moura (2021), acrescentou à Lei de Organização Criminosa, a possibilidade da infiltração virtual, conforme se transcreve a seguir:

> Art. 10-A. Será admitida a ação de agentes de polícia infiltrados virtuais, obedecidos os requisitos do caput do art. 10, na internet, com o fim de investigar os crimes previstos nesta Lei e a eles conexos, praticados por organizações criminosas, desde que demonstrada sua necessidade e indicados o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas. (BRASIL, 2013).

Posto isso, a partir de uma análise detida do artigo 10-A e correlatos da Lei mencionada, é possível perceber que a investigação é cautelosa e exige o preenchimento de requisitos específicos, quais sejam: solicitação do Delegado de Polícia ou requerida pelo Minisério Público; autorização judicial; indícios da prática de crimes por organização criminosa ou conexos, conjugada com a prática de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos ou de caráter transnacional; indicação dos policiais envolvidos, subsidiariedade da ação; prazo do deferimento por 6 (seis) meses; com renovação por autoridade judicial, com limite de 720 (setecentos e vinte) dias. (BRASIL, 2013.)

Sendo assim, cabe à competência de cada polícia prevista no artigo 144 da Constituição da República Federativa do Brasil investigar os crimes nesse âmbito, cada uma dentro de suas possibilidades. (BRASIL, 1988)

Quanto ao avanço das investigações, Moura (2021) assevera o progresso do Estado de Minas Gerais, considerando a criação de delegacias especializadas e a coordenação do Ministério Público de Minas Gerais. As delegacias especializadas são chamadas de DEICC – Delegacias Especializadas de Investigação de Crimes Cibernéticos e regulamentadas pela Resolução 8004 de 14/03/2018 da Polícia Civil de Minas Gerais. (MINAS GERAIS, 2018)

Assim, essas delegacias especializadas são destinadas à investigação de crimes específicos, considerando a necessidade de maior dedicação e estudos. Dessa forma, a mencionada Resolução, em seu artigo 27, discriminou a função dessa delegacia e de

certo modo a competência, ex positis:

> Art. 27 – Compete à Delegacia Especializada em Investigação de Crime Cibernético proceder ao exercício das funções de polícia judiciária e a investigação criminal relativamente às seguintes infrações penais:
> I – divulgação de segredo, disposto no art. 153 do CP, na hipótese de a ação delituosa caracterizar divulgação, via "internet", de correspondência que possa provocar dano a outrem;
> II – invasão de dispositivo informático alheio, disposto no art. 154-A do CP, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita;
> III – furto qualificado mediante fraude, disposto no § 4º do art. 155 do CP, na hipótese de a fraude ou o desvio de valor ser praticado, via "internet", por meio de "saques eletrônicos" em contas bancárias de terceiros, quando o valor do dano patrimonial for igual ou superior a 100 (cem) salários mínimos;
> IV – estelionato, disposto no art. 171 do CP, na hipótese de as fraudes serem praticadas com a utilização, "via internet", de cartões de crédito de terceiros, realizando saques ou transferências, ressalvados, em qualquer caso, os delitos relacionados a fonograma e videograma quando o valor do dano patrimonial for igual ou superior a 100 (cem) salários mínimos;
> V – crimes contra a dignidade sexual, quando a sua execução tiver ocorrido via "internet", inclusive quando a vítima for criança ou adolescente;
> VI – crimes relacionados à pedofilia quando praticados pela internet, os quais estão previstos na Lei Federal nº 8.069, de 1990, Estatuto da Criança e do Adolescente – ECA. Parágrafo único: Será ainda de competência da Delegacia Especializada em Investigação de Crime Cibernético proceder ao exercício das funções de polícia judiciária e a investigação criminal de outras infrações não elencadas nos incisos, desde que praticados via "internet", quando pelo grau de complexidade, clamor ou repercussão social, ou ainda pelo nível de organização se justificar a atuação desta Delegacia Especializada, podendo essa atuar mediante solicitação fundamentada do Titular de Delegacia de Polícia Civil, ou de ofício, desde que não iniciada por outra unidade policial, ocasião em que o Chefe do DEF deverá comunicar imediatamente ao Superintendente de Investigação e Polícia Judiciária, para conhecimento e deliberação. Subseção III Do Laboratório de Investigação de Crimes Cibernéticos.(BRASIL, 2018)

Não obstante, o artigo 28 Resolução 8004 de 14/03/2018 destina-se ao laboratório de investigação de crimes cibernéticos, que tem a finalidade de desenvolver conhecimentos, metodologias e criar estratégias de investigação eficientes.

A coordenação do Ministério Público, também chamada de COECIBER - Coordenadoria Estadual de Combate aos Crimes Cibernéticos, atua junto aos Promotores de Justiça no intuito de combater os crimes cibernéticos. Atua também em escolas, no sentido de orientar crianças, adolescentes e seus pais sobre os riscos da internet, informando as formas seguras de utilização.

Já no âmbito federal, afirma que a Polícia Federal conta com uma Coordenção-Geral de Cooperação Internacional, que possui três divisões: cooperação policial internaional, cooperação jurídica internacional e relações internacionais, as quais colaboram no combate aos crimes informáticos (MOURA, 2021).

AS DIFICULDADES NA INVESTIGAÇÃO E NA PROCURA DO PATRIMÔNIO DA VÍTIMA

Moura (2021) considera três fases de investigação em que determina os índices de dificuldades, diante da clara evolução dos crimes: surface web, deep web e redes sociais. A primeira é a plataforma comumente é utilizada através da internet, por meio da navegação em que as páginas de acesso estão indexadas. Na segunda não há indexadores, o acesso é realizado através de softwares específicos ou Virtual Private Network – Rede Privada Virtual (VPN). Já a terceira é a plataforma de interação mais comum, por exemplo, o WhatsApp, o Instagran, entre outros.

A surface web permite uma investigação aberta, descobrindo-se dados deixados por registros de conexão e acesso, fazendo com que seja um processo mais fácil, considerando que está disponível para todos os usuários, pois, na maioria das vezes, são as páginas indexadas pelo Google e que podem ser acessadas por qualquer navegador. Assim, ao acessar o conteúdo, o computador ou dispositivo, ao conectar-se ao servidor, indentifica-se o Internet protocol - IP do usuário (MOURA, 2021).

Na deep web, o VPN ou os softawares específicos deixam rastros mínimos, considerando o uso constante de técnicas para ocultar IPs, criptografias ponta a ponta (consiste na prática de codificar e descodificar dados, fazendo com que se perca o formato original e não possam ser lidos), dificultando o processo de descobrimento da autoria e materialidade, pois nessa camada garante o anonimato do usuário navegante (MOURA, 2021).

Ainda nessa camada da web, há a dark web, em que a criminalidade é obscura e organizada, considerando a ocorrência de tráfico de drogas, pedofilia e outras atividades ilegais. Geralmente, nessa forma de navegação, exigem-se softwares ou configurações específicas para o devido acesso, usando como forma de pagamento a criptomoeda bitcoin (MOURA, 2021).

Nas redes sociais também há a possilidade de investigação aberta, permitindo assim maior facilidade das autoridades policiais investigarem, ainda que haja a possibilidade de perfis falsos e anonimatos.

Dito isso, Moura (2021) assevera que a investigação através da surface web se dê apenas com informações de registro de acesso e de conexões, tendo em vista os rastros deixados pelos criminosos.

Outra agravante quanto à possibilidade de encontrar suposta autoria, bem como rastros do patrimônio da vítima, é quanto há uma possível falha na legislação, mais especificamente, na possibilidade de quebra de sigilo, prevista no artigo 5º, inciso XII da Constituição Federal (BRASIL, 1999) e Lei 9296/96 (BRASIL, 1996). Essa Lei, em seu artigo 2º, inciso III, exige que a pena seja cominada com no mínimo pena de reclusão. Nesse sentido, Moura (2021), seguindo o posicionamento Alessandro Gonçalves Barreto (2016), argumenta que a autoridade policial deve fundamentar seu pedido de quebra de sigilo

telemático com o parágrafo único do artigo 22 do Marco Civil da Internet, ex positis:

> Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
> I - fundados indícios da ocorrência do ilícito;
> II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
> III - período ao qual se referem os registros. (MOURA, 2021).

Isso se deve considerando a possibilidade de encontrar a autoria e consequente bem da vítima alvo de crimes e uma punição do autor.

Outra forma que dificulta ainda mais desvendar a autoria do fato é quando o delito é praticado através do conhecido "golpe do WhatsApp", tecnicamente chamado de phishing. Na prática desse golpe, o agente encontra o seu contato telefônico de algum modo e tenta acessar o aplicativo através dele. A partir disso, é gerado um código de verifcação para o acesso; o agente então se faz passar pelo próprio aplicativo e pede o código de verificação. Automaticamente, ao enviar o código, via mensagem, para o agente que se fez passar pelo aplicativo, este acessa o WhatsApp e toda a sua rede social, fazendo com que a vítima perca a sua conta.

Uma forma de impedir essa fraude seria através da verificação em duas etapas, que consiste em mais uma camada de proteção, considerando que, após a utilização da senha de seis dígitos que o próprio WhatsApp envia, a vítima possui a senha de seis dígitos que ela mesmo criou.

A RELAÇÃO DA VIOLABILIDADE DA INTIMIDADE E DA VIDA PRIVADA QUANTO À PRÁTICA DO ESTELIONATO

Como anteriormente já comentado, o golpe via internet que se tornou mais popular é o de clonagem de WhatsApp, também conhecido como phishing. Segundo a BL Consultoria Digital (2021), os cibercriminosos entram em contato oferecendo links ou ofertas falsas para obterem acesso aos dados da conta das vítimas e de imediato iniciam o processo de estelionato, qual seja, a solicitação de valores aos contatos existentes na conta invadida.

Diante disso, percebe-se uma clara violação da intimidade, preceito considerado como um direito fundamental perante a Constituição da República, mais especificamente em seu artigo 5º, inciso X:

> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. (BRASIL, 1988).

Essa percepção é devida tendo em vista o amplo acesso a dados conseguidos através dos dispositivos das vítimas, por exemplo: acesso a contatos, conversas, dados

compartilhados entre a vítima e seus contatos, entre outras.

A respeito do tema, pode-se citar, a título de exemplo, um precendente da 4ª (quarta) Vara do Juizado Especial. A MMª Juíza da Vara condenou o Facebook a pagar indenização por danos morais a três vítimas, e duas delas ainda receberam pelos danos materiais sofridos. Nesse caso, a vítima foi contactada após anunciar que seu computador estava à venda; o golpista solicitou o envio de um código de ativação do WhatsApp; assim, teve acesso à conta da vítima e passou a solicitar valores a seus contatos. A vítima solicitou o cancelamento de sua conta, via e-mail, junto ao Facebook, o que só ocorreu 3 (três) dias após o pedido (BL Consultoria Digital, 2021).

A MMª Juíza Oriana Piske fundamentou sua decisão com base no Código de Defesa do Consumidor e Marco Civil da Internet, nos seguintes termos:

> (...) O fato deve ser analisado sob a ótica do Código de Defesa do Consumidor em conjunto com a Lei nº 12.965/2014 (Marco Civil da Internet). A uma, porque se tratam de sociedades empresárias fornecedoras de serviços (rede de dados e aplicativos de conversas), sendo os autores de ambos os processos adquirentes e usuários dos mencionados serviços como destinatários finais (art. 2º do CDC). A duas, porque o art. 3º, incisos II e III da Lei nº 12.965/2014 estabelecem, como Princípios para o uso da internet no Brasil, a proteção da privacidade e dos dados pessoais. A três, porque o art. 7º, inciso I, também, da Lei nº 12.965/2014 garante, aos usuários de internet, o direito à inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação.(...) (BL Consultoria Digital, 2021).

Sendo assim, foi possível perceber que há nítida violação dos direitos da intimidade e vida privada, considerando que os agentes passam a ter amplo acesso de todos os dados das vítimas.

CONSIDERAÇÕES FINAIS

O objetivo geral deste estudo consistiu em analisar as dificuldades à investigação do crime de estelionato e como ele de fato acontece, no âmbito do WhatsApp.

As limitações de pesquisa encontradas no presente trabalho foram, basicamente, encontrar materiais acadêmicos e confiáveis para embasamento e escrever propriamente sobre o assunto, considerando a atualidade da matéira abordada. Sendo assim, percebe-se que uma forma de contribuir ainda mais para a elucidação do assunto abordado seria avaliar como as vítimas podem se proteger das práticas criminosas mencionadas, fazendo com que deixem de perder bens, dinheiro, entre outros.

Com base na revisão bibliográfica, pode-se perceber como aumentou, significativamente, a prática do crime de estelionato com a utilização do WhatsApp, como meio de contato entre o criminoso e a vítima. Fato é que a tecnologia como um todo nos aproxima uns dos outros cada dia mais e essa rede social desempenha bem

esse papel. Assim, com um grande número de pessoas a utilizando, sejam informadas ou desinformadas, facilita ainda mais para os cibercriminosos, considerando o meio ardil que utilizam para a prática criminosa, qual seja o WhatsApp e a função PIX dos aplicativos bancários.

Foi possível perceber que as investigações das práticas delituosas nesse âmbito exigem uma qualificação considerável por parte dos policiais, além de delegacias especializadas para isso, tendo em vista todo o dispêndio de tempo para que as investigações de fato aconteçam, e o fato de, na maioria das vezes, haver criminosos que atuam de forma conjunta. Atrelado às delegacias está o Ministério Público, que possui um grupo de promotores na função apenas da investigação de crimes cibernéticos, junto a uma imersão em políticas preventivas em escolas com o intuito de conscientizar crianças e adolescentes sobre o perigo da internet.

Verifica-se que um grande problema na questão do estelionato praticado via WhatsApp refere-se à busca do patrimônio da vítima após a prática delituosa, tendo em vista essa prática se basear em transferências bancárias via PIX, que são instantâneas, e, quando as vítimas se dão conta de que foram alvo de cibercriminosos, seu dinheiro já percorreu várias contas de pessoas que também tiveram suas contas clonadas, ficando praticamente impossível rastrear o destino do dinheiro vítimas. Não menos importante, há várias camadas da internet que são usadas para burlar IPs, isto é, tornar o endereço dos cumputadores inacessível.

Constatou-se que o agente, a partir do momento em que passa a ter acesso ao WhatsApp da vítima, ou seja, quando os dados das redes sociais passam para a do criminoso, por meio de conversas, vídeos, fotos, contatos, já está violado todo o direito caracterizado como fundamental, como a intimidade. Isso interfere diretamente na seara da vida privada da vítima, considerando que a rede social WhatsApp é uma ferramenta de bate-papo com diversos tipos de pessoas, as quais fazem parte do círculo familiar e empregatício, até amizades, íntimas ou não.

REFERÊNCIAS

BL Consultoria Digital. **Facebook é condenado e pagará indenização por clonagem de WhatsApp**. São Paulo, 2021. Disponível em: https://blconsultoriadigital.com.br/facebook-e-condenado-e-pagara-indenizacao-por-clonagem-de-whatsapp/. Acesso em: 02 ago. 2022.

BRANCO, Dácio. Veja como solicitar reembolso de valores roubados com pix nos principais bancos. Cidade. 27 de dezembro de 2021, às 19h09. **Canaltech**. Disponível em: https://canaltech.com.br/seguranca/veja-como-solicitar-devolucao-de-fraudes-do-pix-em-bancos-205342/. Acesso em: 08 maio 2022.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Constituição**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 jul. 2022.

BRASIL. Decreto Lei 2848 de 07 de dezembro de 1940. **Código Penal**. Disponível em: http://www.

planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 24 maio 2022.

BRASIL. Lei 12.737 de 30 de novembro de 2012. **Diário Oficial da União**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 17 jul. 2022.

BRASIL. Lei 12.850 de 02 de agosto de 2013. **Lei 12.850/2013**. Disponível em: http://www.planalto. gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 18 jul. 2022.

BRASIL. Lei 13.964 de 24 de dezembro de 2019. **Lei 13.964/2019**. Disponível em: http://www. planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 18 jul. 2022.

BRASIL. Lei 14.155 de 27 de maio de 2021. **Diário Oficial da União**. Disponível em: www.in.gov.br/ en/web/dou/-/lei-n-14.155-de-27-de-maio-de-2021-322698993. Acesso em: 24 maio 2022.

BRASIL. Lei 9.296 de 24 de julho de 1996. **Lei 9.296/96**.Disponível em: http://www.planalto.gov.br/ ccivil_03/leis/l9296.htm. Acesso em: 24 maio 2022.

BRASIL. Resolução 8004, de 14 de março de 2018. **Resolução 8004 de 14/03/2018.** Disponível em: http://pesquisalegislativa.mg.gov.br/LegislacaoCompleta.aspx?cod=182094&marc=. Acesso em: 19 jul. 2022.

CILDO JR, Giolo. Uso da tecnologia para fins ilícitos: a violação da intimidade por meio de crimes informáticos. **Revista de Direito Brasileira**, Florianópolis, SC., p. 305-323.

DG solutions. **Por que a gestão de WhatsApp é tão importante para sua empresa**. Disponível em: https://dgsolutions.com.br/gestao-de-whatsapp/#:~:text=Como%20muitas%20pessoas%20usam%20diariamente,a%20empresa%20atrav%C3%A9s%20do%20WhatsApp. Acesso em: 06 jul. 2022.

MARIN, Jorge. WhatsApp: 43% dos usuários foram vítimas de golpes, diz pesquisa. Curitiba. 2022. **Tec Mundo**. Disponível em: https://www.tecmundo.com.br/seguranca/234500-whatsapp-43-usuarios-vitimas-golpes-diz-pesquisa.htm Acesso em: 06 maio 2022.

MOURA, M. Grégore. **Curso de direito penal informático**. Belo Horizonte; São Paulo: D´Plácido, 2021. 283p.

MOURA, M. Grégore. **Curso de direito penal informático**. Belo Horizonte. São Paulo: D´Plácido, 2021. 58 p. Disponível em: https://mundomaistech.com.br/segurança/conheça-a-diferença-entre-surface-web-deep-web-e-dark-web/. Acesso em: 21 jun. 2020.

OLEGÁRIO, Steffanny A. S. **Aumento da criminalidade virtual e a perspectiva da legislação brasileira**. Disponível em: http://65.108.49.104/xmlui/handle/123456789/387. Acesso em: 20 maio 2022.

VERGARA, S. C. **Projetos e relatórios de pesquisa em administração**. 7. ed. São Paulo: Atlas, 2006.