



## INTRODUÇÃO

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, considerando 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.

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.

## METODOLOGIA

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 PRATICADO NO BRASIL

A prática do crime de estelionato via *WhatsApp* é realizada, 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 –, coloca-a 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 quantia em dinheiro, via PIX ou transferência bancária.

Com a implantação do PIX, pelo Banco Central, 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.

Insta mencionar, a possibilidade de estorno deste PIX, quando contacta com a instituição bancária responsável, considerando que a maioria delas não estornam, tampouco investigam tal prática. Dessa forma, elas apenas investigam previamente apenas para constatarem se realmente houve golpe.

Considerando a reincidência desta prática a Lei 14.155 de 2021 trouxe uma inovação para o Código Penal (*novatio legis in pejus*) quando tratar-se de fraude 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.

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.

## COMO AS INVESTIGAÇÕES ACONTECEM NA PRÁTICA

Um marco com o fim de sanar invasões cibernéticas no Brasil, bem como de reprimi-las, foi a publicação da Lei Carolina Dieckmann – 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.

A nossa 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.

É possível perceber que a investigação é cautelosa e exige o preenchimento de requisitos específicos, conforme mencionado no artigo 10-A da Lei 12.850/2013.

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.

## AS DIFICULDADES NA INVESTIGAÇÃO E NA PROCURA DO PATRIMÔNIO DA VÍTIMA

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.

A respeito do tema, pode-se citar, a título de exemplo, um precedente 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).

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