CRIMES DIGITAIS: análise sobre o Estelionato virtual

Samuel Martins Gonçalves[1]

Thiago Alves Henriques[2]

RESUMO

Esta pesquisa teve por objetivo analisar o crime de estelionato cometido no ambiente virtual, uma manifestação crescente e complexa da criminalidade cibernética que ameaça à segurança das transações e informações online. Utilizando como método de pesquisa básica e a revisão bibliográfica, o estudo examina o aspecto histórico do surgimento da internet e uma revisão das definições legais e doutrinárias dos crimes digitais e do estelionato tradicional; em seguida, explora-se a transposição desses elementos para o cenário virtual, analisando como a utilização de dispositivos eletrônicos e plataformas online influencia a execução do estelionatos virtuais; os elementos-chave desse crime, suas implicações legais, as modalidades e os desafios enfrentados pelo sistema jurídico. A pesquisa realizada neste trabalho pode ser classificada quanto à natureza como pesquisa básica, pois objetivou gerar conhecimentos novos úteis para o avanço da ciência sem aplicação prática prevista e envolveu verdades e interesses universais. Da forma de abordagem do problema a pesquisa se classificou como qualitativa por utilizar conteúdos já publicados para a análise do problema, explorando levantamentos bibliográficos, análises de exemplos que estimulem a compreensão e explicativa porque visou a identificar os fatores que determinam ou contribuem para a ocorrência do problema. Quanto à metodologia o trabalho em mãos fez a opção pelo método hipotético-dedutivo. Esta opção se justifica porque o método escolhido permite ao pesquisador propor uma hipótese e parte, por meio da dedução, para a sua comprovação ou não. Enquanto procedimento, este trabalho foi conduzido por meio de pesquisa de fontes bibliográficas, uma vez que foi construído com base em conteúdos disponibilizados em livros, artigos, dissertações, teses e, mais recentemente, na internet. Além disso, assumiu um caráter quantitativo, visto que envolveu a utilização de representações gráficas. É partindo das premissas superiores que se frisou e se despertou compreender as nuances desse crime no ambiente digital, considerando as características específicas da tecnologia como facilitadora do delito. Por fim, o artigo conclui enfatizando a importância de uma legislação atualizada e de medidas de conscientização pública para prevenir o estelionato virtual. Também ressalta a necessidade de investimentos em tecnologias de segurança cibernética e na capacitação das forças de segurança para lidar de maneira eficaz com os crimes digitais.

Palavras-chave: Crimes digitais; Estelionato Virtual; Lei n° 14.555; Segurança cibernética.

[1] Bacharelando em Direito pela Faculdade de Ipatinga.

[2] Bacharel em Direito pela Universidade Federal do Estado do Rio de Janeiro (2008), pós-graduado lato sensu em Ciências Criminais pela Universidade Estácio de Sá (2017) e extensão universitária em Direito Civil e Processual Civil pelo Centro Universitário UNISEB (2011). Delegado de Polícia Civil do Estado de Minas Gerais.

1 INTRODUÇÃO

Na era da informação e da tecnologia, as fronteiras tradicionais do crime têm se estendido para o ciberespaço, dando origem a uma série de desafios jurídicos complexos e multifacetados. No contexto brasileiro, assim como em muitas outras nações, o advento da era digital tem levantado questões substanciais relacionadas aos crimes de fraude eletrônica. A rápida evolução das tecnologias digitais tem proporcionado um ambiente propício para a perpetração de delitos que exploram as vulnerabilidades das redes eletrônicas, desafiando os alicerces do sistema jurídico.

Neste cenário, a análise do crime de estelionato virtual assume uma relevância extraordinária. Os avanços tecnológicos têm permitido aos perpetradores de crimes explorar brechas em sistemas eletrônicos, muitas vezes com uma capacidade de ocultação e rastreamento dificilmente precedentes. A natureza virtual desses delitos, aliada à sua transnacionalidade, cria um ambiente onde os limites jurisdicionais tradicionais se tornam turvos, exigindo uma abordagem legal inovadora e adaptativa, capaz de abranger nuances específicas dos delitos cibernéticos.

Além disso, o trabalho abordará as complexidades inerentes à coleta de evidências eletrônicas, a cooperação internacional em investigações transfronteiriças e a capacitação contínua das autoridades encarregadas da aplicação da lei, fatores cruciais para o efetivo enfrentamento desses crimes no contexto brasileiro.

Ao analisar a eficácia da legislação e identificar os obstáculos enfrentados nas investigações dos crimes de estelionato virtual, este estudo busca contribuir para a compreensão mais profunda do cenário dos crimes digitais no Brasil e proporcionar compreensões relevantes para o fortalecimento das estratégias legais e de aplicação da lei nesse campo desafiador e em constante evolução.

Este trabalho visa elucidar a seguinte questão: o que é o crime de estelionato virtual e quais os obstáculos enfrentados na identificação dos autores desse tipo de crime.

A relevância da pesquisa está exatamente no ponto acima destacado. Atentar-se para este tipo de crime que tem crescido cada vez mais dentro do país e a sensação de insegurança no ambiente digital.

A pesquisa realizada neste trabalho pode ser classificada quanto à natureza como pesquisa básica, pois objetivou gerar conhecimentos novos úteis para o avanço da ciência sem aplicação prática prevista e envolveu verdades e interesses universais. Da forma de abordagem do problema a pesquisa se classificou como qualitativa por utilizar conteúdos já publicados para a análise do problema.

Conseguinte, quanto aos objetivos será uma pesquisa exploratória porque envolve levantamento bibliográfico, análise de exemplos que estimulem a compreensão e explicativa porque visa a identificar os fatores que determinam ou contribuem para a ocorrência do problema. Quanto à metodologia o trabalho em mãos fez a opção pelo método hipotético-dedutivo. Esta opção se justifica porque o método escolhido permite ao pesquisador propor uma hipótese e parte, por meio da dedução, para a sua comprovação ou não.

Enquanto procedimento, este trabalho foi conduzido por meio de pesquisa de fontes bibliográficas, uma vez que foi construído com base em conteúdos disponibilizados em livros, artigos, dissertações, teses e, mais recentemente, na

internet. Além disso, assumiu um caráter quantitativo, visto que envolveu a utilização de representações gráficas.

Esses instrumentos possibilitarão uma investigação minuciosa a respeito do tema apresentado. A informação registrada, juntamente com suas análises correspondentes, será estruturada em relatórios de pesquisa, os quais constituem parte integral do projeto de desenvolvimento da monografia em questão.

2 O SURGIMENTO DO AMBIENTE DIGITAL

O ambiente digital emergiu a partir da evolução tecnológica que culminou na criação da internet, a "rede das redes", como definida por Tim Berners-Lee, em meados da década de 1960, durante a Guerra Fria, quando o Departamento de Defesa dos Estados Unidos criou a ARPANET, uma rede de comunicação descentralizada que visava garantir a comunicação e transmissão de informações entre computadores totalmente interligados em caso de ataques nucleares.

O ambiente digital no Brasil teve suas raízes nos anos 1980, quando a conexão à internet começou a se estabelecer no país. Inicialmente restrita a universidades e centros de pesquisa, a rede rapidamente se expandiu, promovendo a troca de informações e conhecimento. O primeiro ponto de acesso à internet no Brasil foi estabelecido em 1991, marcando o início de uma era de comunicação global.

A década de 1990 foi marcada por avanços significativos no ambiente digital brasileiro. Em 1995, o governo lançou o projeto "Rede Nacional de Ensino e Pesquisa" (RNP), impulsionando a conectividade acadêmica e de pesquisa. O ano de 1996 viu a primeira conexão comercial à internet, permitindo que empresas e indivíduos acessassem a rede mundial.

Desde cedo, o governo brasileiro percebeu o potencial da internet como uma ferramenta para impulsionar o desenvolvimento e promover a inclusão social. A partir dos anos 2000, políticas públicas foram implementadas para promover a inclusão digital, como o programa "Computador para Todos", que buscava tornar os computadores mais acessíveis à população de baixa renda. Além disso, o Plano Nacional de Banda Larga, lançado em 2010, buscou expandir o acesso à internet em alta velocidade em todo o país

No entanto, a rápida proliferação do ambiente digital trouxe à tona uma série de desafios legais que demandam uma resposta adequada por parte do sistema jurídico. Um dos principais desafios reside na adaptação das leis existentes para esse novo espaço virtual, no qual as fronteiras geográficas são diluídas e as atividades transcendem as jurisdições nacionais. A identificação de responsabilidades em casos de crimes cibernéticos, a proteção da privacidade dos indivíduos e a regulamentação do comércio eletrônico são apenas alguns exemplos das questões que os sistemas legais devem abordar.

3 ASPECTOS HISTÓRICOS E DEFINIÇÃO DE CRIME DIGITAL

3.1 Aspectos históricos dos crimes digitais

A literatura científica internacional revela que os primórdios dos delitos cibernéticos tiveram sua gênese no século XX, mais precisamente em 1960,

quando surgiram as primeiras menções sobre esse gênero de crimes em diversas categorias, com maior ocorrência em situações de manipulação e sabotagem de sistemas computacionais.

Durante os anos 70, o perfil do Hacker já era mencionado à medida que emergiam crimes como a invasão de sistemas e o roubo de programas, no entanto, foi somente em 1980 que ocorreu uma disseminação mais acentuada das variadas formas de crimes, tais como pirataria, exploração infantil online, invasões de sistemas e disseminação de códigos maliciosos. Isso gerou a necessidade premente de se direcionar maiores atenções para a segurança virtual, que requer uma dedicação especial à identificação e punição dos responsáveis. Nesse ponto, é importante ressaltar que tais indivíduos estão presentes em todas as partes do globo, como exemplificado pela intensa busca do governo dos Estados Unidos por Kevin Mitnick, um dos hackers mais renomados globalmente, que, atualmente, desempenha uma função na área de segurança da informação dentro do governo norte-americano.

3.2 Definição dos crimes digitais

O artigo 1º da Lei de Introdução ao Código Penal (Decreto-Lei nº 3.914/41), enuncia o subsequente teor respeito da definição de crime:

> Considera-se crime a infração penal a que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente.

Segundo Capez (2011, p. 137), o conceito de crime pode ser compreendido como uma conduta humana que lesiona ou coloca em perigo bens jurídicos fundamentais para a convivência em sociedade.

Assis Toledo, que utiliza do da teoria tripartida do crime, expõe da seguinte maneira:

> Substancialmente, o crime é um fato humano que lesa ou expõe a perigo bens jurídicos (jurídico-penais) protegidos. Essa definição é, porém, insuficiente para a dogmática penal, que necessita de outra mais analítica, apta a pôr à mostra os aspectos essenciais ou os elementos estruturais do conceito de crime. E dentre as várias definições analíticas que têm sido propostas por importantes penalistas, parece-nos mais aceitável a que considera as três notas fundamentais do fato-crime, a saber: ação típica (tipicidade), ilícita ou antijurídica (ilicitude) e culpável (culpabilidade). O crime, nessa concepção que adotamos, é, pois, ação típica, ilícita e culpável (Toledo *apud* Greco, 2013, p. 143).

No entanto, há uma controvérsia dentro da literatura jurídica em relação à designação dos crimes ocorridos no contexto do ambiente digital. Por isso, são atribuídos diversos termos à essas práticas, como por exemplo: crimes cibernéticos, crimes digitais e crimes informáticos. Esta ação criminosa, de certa maneira, engloba todas as ações definidas como criminosas que são executadas por meio do uso de tecnologia. No entanto, as interpretações são vastas e flutuam conforme a perspectiva de cada indivíduo.

De acordo com Crespo (2022), os crimes digitais são todas as condutas previstas em lei que sejam punidas com pena criminal e cuja prática envolva aparatos tecnológicos, seja porque a conduta destina-se contra os sistemas informatizados e contra dados, seja porque o meio utilizado é tecnológico, embora o crime pudesse ser praticado de outra forma.

A doutrinadora Ivette Senise Ferreira (2005) define os crimes digitais como:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial.

Sandra Gouvêa possui uma inclinação pelo emprego da terminologia "crimes por meio da informática", embasando sua seleção na argumentação de que os computadores não representam os exclusivos dispositivos aptos a serem utilizados nas ações ilícitas (Gouvêa *apud* Crespo, 2011, p. 48).

Da mesma maneira, de acordo com as ideias de Fabrizio Rosa (2002, p. 53-54), é possível também definir o delito virtual como:

> É a conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O 'Crime de Informática' é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o 'Crime de Informática' pressupõe dos elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetra-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença a ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc.

Portanto, constata-se que não existe uma terminologia estabelecida pelos especialistas no assunto relativa à definição de crimes digitais. De uma maneira ou de outra, a única variável é o rótulo dado a essas infrações, uma vez que é necessário considerar a utilização de sistemas eletrônicos, a infraestrutura de comunicação de informações para fins criminosos, o interesse jurídico prejudicado, e também é imperativo que a ação seja enquadrada como típica, antijurídica e culpável.

4 OS CRIMES DIGITAIS E A LEGISLAÇÃO NACIONAL VIGENTE

As legislações são estabelecidas conforme as exigências que emergem devido à constante evolução da sociedade. Antes do ano de 2012, o Brasil carecia de uma legislação específica que definisse claramente as condutas intencionais voltadas para a violação ou intrusão em sistemas e dispositivos digitais. Foi somente em 2 de dezembro de 2012, por meio de publicação no Diário Oficial da União, que um passo significativo foi dado em nosso sistema legal, a chegada da Lei n.º 12.737/2012 Lei dos Crimes Cibernéticos (Lei Carolina Dieckmann). Esse marco representou um avanço limitado no contexto de nossa estrutura jurídica, especialmente no âmbito do enfrentamento de crimes virtuais. O crime de Invadir Dispositivo Informático foi tipificado, conforme previsto no artigo 154-A do Código Penal, que posteriormente foi modificado pela Lei n° 14.155/21.

Em 2014, entrou em vigor a Lei n.º 12.695/2014 (Marco Civil da Internet), uma lei que teve como propósito eliminar a percepção de um espaço sem normas, introduzindo direitos, responsabilidades e proteções que viabilizassem o controle da utilização das redes no Brasil. Isso se tornou essencial dada a considerável urgência em resguardar a privacidade dos utilizadores da internet e garantir a intangibilidade e confidencialidade das trocas de informações.

A legislação igualmente estabelece e assegura que os prestadores de serviços não têm permissão para transgredir ou comprometer o direito à privacidade e à vida privada de seus utilizadores. Isso significa que eles não estão autorizados a monitorar as informações transmitidas pela rede ou a divulgá-las, a menos que haja consentimento explícito ou uma ordem judicial vigente. Além disso, a lei também garante a liberdade de expressão dentro dos limites legais, enquanto combate a prática de censura. Isso contribui para tornar o ambiente virtual mais seguro e inclusivo para todos os utilizadores, sem exceção.

Essencialmente, essa lei tem a finalidade de resguardar as informações individuais presentes nas plataformas digitais, a fim de prevenir a utilização inadequada por partes com intenções maliciosas. Ao assegurar que os usuários tenham o direito de acessar o tratamento de seus dados e também a responsabilidade por eventuais prejuízos, o propósito dessa lei é garantir igualdade para todos, independentemente de suas características, promovendo um ambiente digital digno e saudável para que possam cultivar suas identidades e exercer seus direitos de cidadania.

A Lei Geral de Proteção de Dados Pessoais, numerada como Lei 13.709/18, foi promulgada com o propósito de resguardar os direitos essenciais relacionados à liberdade, privacidade e à formação individual de cada pessoa. Seu objetivo é estabelecer normas para a gestão e proteção dos dados pessoais, tanto de indivíduos quanto de entidades empresariais, garantindo assim os direitos dos cidadãos e impondo regulamentos sobre as operações de processamento efetuadas por instituições públicas ou organizações privadas.

A motivação subjacente à criação dessa nova lei reside na necessidade de prevenir abusos em relação à privacidade e à intimidade dos usuários, resguardando seus direitos fundamentais e evitando a utilização inadequada de seus dados pessoais. A LGPD reforça e efetiva direitos já previstos na Constituição Federal de 1988, atuando como um complemento à proteção concedida pelo Código de Defesa do Consumidor e pelo Marco Civil da Internet.

Ela concede aos cidadãos o poder de controlar suas informações pessoais, fortalecendo, assim, a prática da liberdade de expressão, o acesso à informação, bem como os direitos ligados à privacidade, honra e imagem.

Diante disso, tanto instituições públicas quanto privadas devem assegurar que qualquer manipulação de informações pessoais esteja ancorada em bases legais sólidas. Isso implica na manutenção de registros precisos de todas as atividades de tratamento de dados, na elaboração de relatórios de avaliação dos impactos sobre a proteção de dados quando os processamentos possam implicar riscos para liberdades civis e direitos fundamentais dos titulares. Também é crucial criar sistemas de segurança que garantam a proteção das informações desde a sua gênese. Caso ocorram violações de segurança que possam resultar em riscos ou danos relevantes, tanto o titular dos dados quanto a Autoridade Nacional de Proteção de Dados (ANPD) devem ser prontamente informados, com medidas adequadas de contenção ou mitigação.

Além disso, caso haja alterações na finalidade da coleta de dados, os titulares devem ser informados. As organizações também são obrigadas a reparar os danos decorrentes de tratamentos inadequados de dados, em conformidade com a legislação. É necessário confirmar a existência dos dados pessoais mediante solicitação do titular, bem como divulgar os tipos de dados coletados, os métodos de coleta e compartilhamento, e as medidas adotadas para garantir a segurança das informações. Avaliações regulares das salvaguardas e mecanismos de mitigação de riscos são essenciais, e é obrigatório nomear um Encarregado de Dados Pessoais, cujas informações de contato devem ser tornadas públicas. As instituições também são responsáveis por receber reclamações, comunicações e prestar esclarecimentos aos titulares de dados quando necessário.

5 DO ESTELIONATO VIRTUAL

Perambulando pela exposição, a fim de chegar à conclusão mais sólida sobre a questão em análise, é necessário apresentar algumas considerações preliminares sobre o crime de estelionato.

O Código Penal Brasileiro –Decreto Lei nº. 2.848, de 7 de dezembro de 1940, em seu capítulo V, descreve no artigo 171 o que tipifica o crime de estelionato:

> Art. 171 - 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: Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.

A expressão jurídica estelionato advém da palavra grega *stelio*, que nomeia uma espécie de lagarto que muda de cor para iludir suas presas. A origem da palavra combina com a nomenclatura atribuída a quem pratica o tipificado no delito, que, nesse caso, utiliza artimanhas para enganar determinada pessoa (Ribeiro, 2019).

Trata-se de crime contra o patrimônio, em que a legislação penal visa proteger a inviolabilidade patrimonial orientada pela prática de atos que visam enganar a vítima e beneficiar o agente (Cunha, 2019).

Para sua tipificação, o crime de estelionato exige quatro requisitos obrigatórios: 1) obtenção de vantagem ilícita; 2) causar prejuízo a outra pessoa;

3) uso de meio de ardil, ou artimanha, 4) enganar alguém ou a leva-lo a erro. A ausência de um dos quatro elementos, seja qual for, impede a sua caracterização.

É importante ressaltar que no crime de estelionato não há o uso de violência ou grave ameaça por parte do perpetrador, ou seja, aquele que comete o crime.

Nesse sentido, o doutrinador Fernando Capez afirma que:

> Trata-se de crime em que, em vez da violência ou grave ameaça, o agente emprega um estratagema para induzir em erro a vítima, levando-a a ter uma errônea percepção dos fatos, ou para mantê-la em erro, utilizando-se de manobras para impedir que ela perceba o equívoco em que labora (Capez, 2020, p. 842).

Com base nas informações apresentadas até o momento, é possível compreender inicialmente que o estelionato virtual se caracteriza pelo uso de dispositivos tecnológicos e conexão à internet por um indivíduo para executar ações que se enquadram nos termos do artigo 171 do Código Penal.

Nesse contexto, o indivíduo age visando obter benefício próprio ou em favor de terceiros, resultando em prejuízo para outras pessoas, ao conduzir práticas que levam as vítimas ao erro, por meio de métodos fraudulentos, com o intuito de alcançar ganhos ilegítimos.

Com a eclosão da pandemia do novo Coronavírus (COVID-19), uma das ações mais amplamente adotadas em todo o globo foi a prática de distanciamento social. Isso resultou na necessidade da maioria das pessoas aderirem ao trabalho em formato remoto, com o intuito de reduzir ou evitar aglomerações nos locais de trabalho e minimizar a disseminação do vírus. Consequentemente, ocorreu um aumento substancial no número de dispositivos eletrônicos conectados de maneira simultânea, o que acabou por facilitar ainda mais a execução desse tipo de crime.

A sociedade como um todo, além de lidar com os desafios do Covid-19, enfrentou também crises políticas e econômicas no país, além de instabilidades financeiras e emocionais, em grande parte originadas pela pandemia. Além desses fatores, foi necessário estar alerta para a incidência de crimes cibernéticos. Em meio a todo o caos vivenciado no país, surgiu uma oportunidade para os criminosos.

Segundo dados uma pesquisa feita pelo Fórum Brasileiro de Segurança Pública (FBSP) houve um aumento alarmante nos casos de estelionato eletrônico, “em 2021, foram 115 estelionatos eletrônicos a cada 100 mil habitantes no país. No ano seguinte, foram 189,9, um aumento de 65,1%” (Honório; Stabile; Paiva (2023).

Nessa perspectiva, diante do crescente e acentuado aumento das fraudes online, o legislador brasileiro teve que tomar medidas para conter as atividades criminosas.

A Lei n° 14.155/21 foi promulgada em 28 de maio de 2021, introduzindo várias alterações tanto no Código Penal quanto no Código de Processo Penal. O objetivo era intensificar a repressão dos delitos de maneira mais eficiente, dada a atual recorrência dessas condutas. Portanto, essa lei em questão apresenta uma série de disposições que estabelecem penalidades mais severas para a prática de crimes no ambiente virtual.

Vale ressaltar que, por meio da Lei 14.155 de 2021, também foram incluídos no Código Penal os §2°-A e §2°-B, tratando de maneira explícita sobre o crime de estelionato ocorrido virtualmente, identificando-o como Fraude Eletrônica.

> **Estelionato**
> Art. 171 - 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:
> **Fraude eletrônica**
> § 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.
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

Também ocorreram modificações também no parágrafo 4º do artigo 171 do Código Penal. Essas alterações resultaram em uma ampliação das penalidades aplicáveis em situações de estelionato eletrônico cometida contra indivíduos idosos ou em condição de vulnerabilidade. Esse ajuste ocorreu nos seguintes moldes: “§ 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso” (Redação dada pela Lei nº 14.155, de 2021).

Resumidamente, é possível afirmar que a principal disparidade entre o estelionato denominado como convencional ou tradicional e o estelionato virtual reside na forma de atuação utilizada. O primeiro ocorre no mundo físico. Por outro lado, o segundo se concretiza no cenário virtual.

5.1 Do Estelionato Virtual cometido no Estado de Minas Gerais

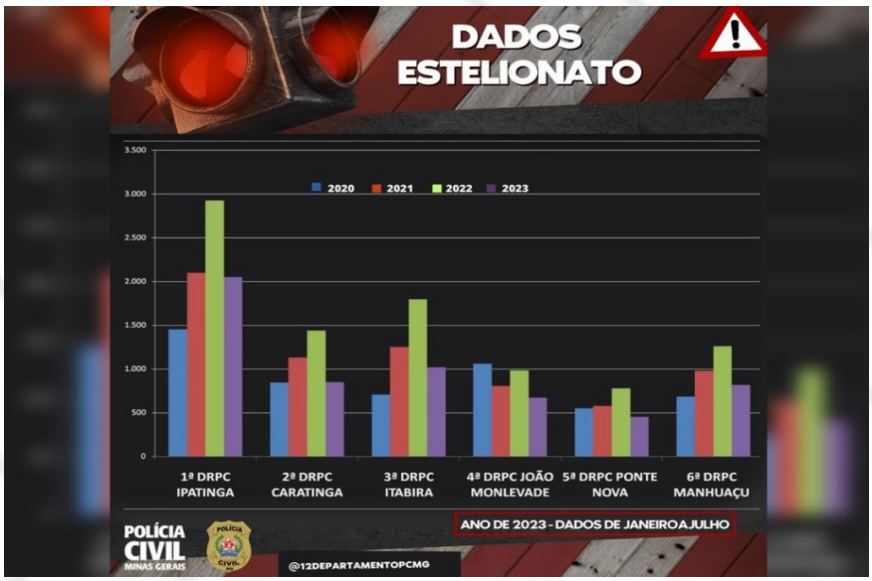
O estado de Minas Gerais, segundo informações tornadas públicas pelo Fórum Nacional de Segurança Pública, observou um crescimento de 39,7% nos delitos relacionados a estelionato virtual no período de 2021 a 2022. As informações indicam que no último ano, acima de 35 mil indivíduos sofreram prejuízos em virtude de artimanhas praticadas na internet ou por meio do aplicativo Whatsapp. Isso se contrasta com os mais de 25 mil incidentes ocorridos no intervalo de tempo anterior. Em escala nacional, o número de registros dessa modalidade de crime alcançou a marca de 200 mil.

No Região Metropolitana do Vale do Aço - região metropolitana brasileira no interior do estado de Minas Gerais, na Região Sudeste do país. Foi reconhecida pela lei complementar nº 51, de 30 de dezembro de 1998, sendo efetivada como região metropolitana em 12 de janeiro de 2006 - também houve um aumento expressivo do número de crimes de estelionato eletrônico, segundo dados do 12º Departamento de Polícia Civil (DPC), que são demonstrados a partir dos seguintes gráficos:

Figura 1: Dados dos estelionatos da Polícia Civil

Fonte: https://www.diariodoaco.com.br/noticia/0109141-pc-revela-tendencia-de-aumentos-de-crimes-de-estelionato-no-vale-do-aco

Figura 2: Dados dos estelionatos da Polícia Civil



Fonte: https://www.diariodoaco.com.br/noticia/0109141-pc-revela-tendencia-de-aumentos-de-crimes-de-estelionato-no-vale-do-aco.

6 SUJEITOS DO CRIME

As noções de quem são os sujeitos do tipo penal são de extrema importância para determinar quem praticou a infração (sujeito ativo) e quem experimentou as consequências do delito (sujeito passivo).

6.1 Sujeito ativo

É um equívoco pensar que os crimes cibernéticos são exclusivamente perpetrados por especialistas, especialmente na sociedade contemporânea, onde o uso de computadores está em constante expansão, sendo essa expansão correlacionada com o crescimento da Internet. Com o progresso dos meios de comunicação, o aumento de dispositivos eletrônicos, o avanço da tecnologia e, acima de tudo, a maior acessibilidade e a disponibilidade de sistemas, indivíduos com apenas um nível mínimo de conhecimento na área têm a capacidade de se tornarem infratores na área de Informática.

Portanto, observa-se que a Internet é uma ferramenta que sem dúvida ampliou o conhecimento dos usuários, incluindo aqueles que negligenciam o respeito pelos limites legais. O aspecto em tempo real, o método de tentativa e erro, a sequência de ações e reações, enfim, a maneira interativa pela qual as informações são disseminadas para todos os lugares, ampliaram consideravelmente o leque de possibilidades. Daí decorre o surgimento de um grande número de indivíduos com o mínimo de conhecimento necessário para cometer crimes em um ambiente online. Em outras palavras, o acesso a qualquer tipo de informação, inclusive aquela de natureza criminosa, facilitou a proliferação de criminosos atuando no ambiente virtual.

O anonimato igualmente contribuiu para o desenvolvimento desse solo fértil destinado à prática criminosa. As mais avançadas aplicações de rastreamento (por meio do endereço IP, entre outros) podem até viabilizar a identificação do dispositivo a partir do qual o ato delituoso foi executado, porém não necessariamente revelam a identidade da pessoa que efetuou o uso do aparelho. Além disso, os locais conhecidos como Cyber Cafés[1] oferecem a infraestrutura essencial para que esse processo ocorra, considerando que não há regulamentação alguma que discipline a operação desse tipo de empreendimento, o que é absolutamente imprescindível.

Cecílio da Fonseca (2002, p.1) sustenta que:

> Os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas[2].

Há algumas classificações, para esses sujeitos ativos. Crespo (2011, p. 95) entende que:

> Hacker é o nome genérico dado aos chamados “piratas” de computador. Essa expressão surgiu nos laboratórios de computação do MIT (Massachusetts Institute of Technology), onde estudantes passavam noites em claro averiguando tudo o que se podia fazer com o computador.

O cracker já é alguém que utiliza o computador de forma maliciosa por diversão, e consegue entrar em sistemas de computador sem permissão, com a

---

[1] Cybercafé é um local que, pode funcionar como bar ou lanchonete, oferece a seus clientes acesso à Internet, mediante a pagamento de uma taxa, usualmente cobrada por hora.

[2] Aquele que é adepto de uma causa, de uma instituição, movimento

intenção de vencê-los. Eles podem realizar o roubo de informações relacionadas a contas bancárias e cartões de crédito, ou até mesmo causar a destruição de dados.

Carders são os indivíduos especializados na fabricação de réplicas de cartões sejam eles de crédito, telefônicos, magnéticos, entre outros, com o propósito enganoso de usá-los ilegalmente junto às empresas que operam no contexto online. Distinguem-se dos falsificadores e golpistas convencionais devido à sua atuação restrita ao ambiente virtual.

No que diz respeito aos phreakers, são indivíduos que operam no campo dos telefones. Eles atuam no âmbito das telecomunicações, manipulando o sistema que controla as chamadas, podendo através do computador escutar as conversas alheias, assim como utilizar o telefone dessa pessoa em seu próprio benefício, realizando chamadas sem custo. É possível alcançar ligações após invadir os sistemas telefônicos, desconcertando os operadores da linha, sem necessariamente utilizar a linha pessoal de alguém. Entretanto, a fraude acaba sendo custeada por um usuário da empresa de telefonia.

Confirma-se, portanto, que o indivíduo hacker, a quem todos rotulam como delinquente digital, na realidade não o é em todas as ocasiões.

6.2 Sujeito passivo

Primeiramente, é essencial estabelecer que o sujeito passivo dos crimes virtuais, é aquele sobre o qual incide a ação criminosa de não fazer algo ou de fazer algo por parte da pessoa que comete o crime, e no que se refere às atividades criminosas relacionadas à tecnologia da informação, podem ser afetadas pessoas, organizações financeiras, entidades governamentais e outras entidades que utilizem sistemas automatizados de dados, independentemente de estarem conectadas à internet ou não.

É fundamental ressaltar, todavia, que a grande parte dos crimes de estelionato virtual não chega ao radar das autoridades para ser devidamente investigada, devido às corporações ou entidades financeiras. Cita-se, a título de exemplo, que o crime de estelionato virtual pode acarretar desvalorização e comprometimento da confiabilidade, visto que pode criar a percepção de que esta ou aquela organização carece de sistemas de segurança eficazes. É exatamente esse 'código de silêncio' que está encorajando, de certa maneira, os infratores a prosseguirem com suas atividades ilegais.

7 COMPETÊNCIA DE JULGAMENTO

Os delitos cometidos por meio eletrônico têm o potencial de afetar múltiplas localidades dentro de um mesmo território e, inclusive, transcender fronteiras internas, alcançando uma escala global.

Por isto, A Lei 14.155/2021 trouxe uma significativa alteração no que diz respeito à autoridade responsável por julgar os casos de estelionato eletrônico, incluindo no artigo 70 do Código de Processo Penal o parágrafo 4º, com o seguinte teor:

> § 4º 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. (Incluído pela Lei nº 14.155, de 2021).

Assim, nos casos de estelionato eletrônico, a competência será definida pelo local do domicílio da vítima, e, em casos de pluralidade de vítimas, pela prevenção.

Com base nesse regulamento, o legislador tem como objetivo fortalecer a proteção das pessoas prejudicadas pelo estelionato eletrônico, especialmente diante da considerável controvérsia que surgiu em relação à jurisdição territorial para julgar esses crimes.

Nesse sentido a jurisprudência do Superior Tribunal de Justiça dispõe que:

> CONFLITO NEGATIVO DE COMPETÊNCIA. ESTELIONATO. MODUS OPERANDI NÃO CONTEMPLADO PELA LEI N. 14.155/2021. NÃO CONFIGURAÇÃO DAS HIPÓTESES DESCRITAS NO § 4º DO ART. 70 DO CÓDIGO DE PROCESSO PENAL - CPP. INCIDÊNCIA REGRA GERAL PREVISTA NO ART. 70, CAPUT, DO CPP. COMPETÊNCIA DO LOCAL NO QUAL SE AUFERIU O PROVEITO DO CRIME.
> 1. O presente conflito de competência deve ser conhecido, por se tratar de incidente instaurado entre juízos vinculados a Tribunais distintos, nos termos do art. 105, inciso I, alínea d da Constituição Federal - CF.
> 2. No caso dos autos, um ex-funcionário da empresa vítima, atuante no ramo de turismo, em associação com os outros dois agentes delituosos, teriam simulado contratos de parcerias com empresas terceiras, com a intenção de obter para si vantagens ilícitas, a saber: passagens aéreas e reserva de veículos e hotéis. De acordo com inquérito policial, o estelionatário fazia uso próprio de tais passagens, bem como as repassava para terceiros, obtendo o proveito do crime. A empresa vítima possui sede em Brasília/DF, contudo o ex-funcionário apontado como estelionatário trabalhava como representante comercial na filial localizada no município de São Paulo, onde os golpes teriam sido praticados em conluio com outros dois agentes, também residentes em municípios localizados no Estado de São Paulo.
> 3. O núcleo da controvérsia consiste em definir se o julgamento do delito de estelionato compete ao Juízo de Direito da 4ª Vara Criminal de Brasília/DF, considerando-se o local da sede da empresa vítima e de sua agência bancária; ou ao Juízo de Direito da Vara Criminal do Foro Central Barra Funda/SP, em razão do local onde o agente delituoso auferiu o proveito do crime.
> 4. O dissenso jurisprudencial retratado nos precedentes colacionados pelos Juízos envolvidos neste conflito deixou de existir com o advento da Lei 14.155/2021, que acrescentou o § 4º do art. 70 do Código de Processo Penal - CPP com o seguinte teor: "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".
> Todavia, a inovação legislativa disciplinou a competência do delito de estelionato em situações específicas descritas pelo legislador, as quais não ocorrem no caso concreto, porquanto os autos não noticiam a ocorrência transferências bancárias ou depósitos efetuados pela

empresa vítima e tampouco de cheque emitido sem suficiente provisão de fundos.
5. No contexto dos autos, não identificadas as hipóteses descritas no § 4º do art. 70 do CPP deve incidir o teor do caput do mesmo dispositivo legal, segundo o qual "a competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução". Sobre o tema a Terceira Seção desta Corte Superior, recentemente, pronunciou-se no sentido de que nas situações não contempladas pela novatio legis, aplica-se o entendimento pela competência do Juízo do local do eventual prejuízo. Precedente: CC 182.977/PR, Rel. Ministra LAURITA VAZ, TERCEIRA SEÇÃO, DJe 14/3/2022.
6. Destarte, na espécie, a competência deve ser fixada no local onde o agente delituoso obteve, mediante fraude, em benefício próprio e de terceiros, os serviços custeados pela vítima.
7. Conflito conhecido para declarar competente o Juízo de Direito da Vara Criminal do Foro Central Barra Funda - DIPO 4 - SÃO PAULO - SP, o suscitado.
(CC n. 185.983/DF, relator Ministro Joel Ilan Paciornik, Terceira Seção, julgado em 11/5/2022, DJe de 13/5/2022.).

8 MODALIDADES DE ESTELIONATO VIRTUAL

8.1 O golpe do Whatsapp

Uma das principais modalidades de golpe utilizada pelos estelionatários virtuais em voga atualmente é denominada de "Clonagem do WhatsApp". Desde a introdução desse aplicativo de comunicação, os métodos empregados para executar essa fraude têm sido alterados e apresentam diversas variantes.

Para perpetrar esse ato ilícito, o fraudador necessita ter acesso ao número de telefone utilizado pela vítima no aplicativo WhatsApp e sua senha de entrada, ou seja, o código de autenticação composto por seis dígitos obtido por meio do mecanismo de segurança conhecido como "Verificação em duas etapas", que consiste essencialmente em uma senha personalizada definida pelo usuário para acessar o aplicativo.

Em essência, o inicial dado (contato telefônico da pessoa afetada), geralmente é adquirido sem dificuldades em anúncios veiculados em plataformas de comércio online e nas mídias sociais do indivíduo prejudicado; por outro lado, o código de verificação é cedido ao delinquente pela própria vítima, sem que esta tenha consciência das ações que está realizando.

Tendo em mãos o número de telefone da pessoa prejudicada, o delinquente (valendo-se de qualquer dispositivo telefônico) procura ingressar na conta de WhatsApp pertencente à vítima. Com o objetivo de validar sua identidade como proprietário legítimo da conta, o aplicativo encaminha uma mensagem de texto SMS contendo um código para o número registrado, isto é, o telefone da vítima.

Logo após o impostor, assumindo a identidade de um empregado vinculado a um portal de transações comerciais ou uma plataforma de interação social online, estabelece comunicação com a vítima. Ele requer a confirmação de informações pessoais da vítima (como nome completo, número de CPF, identidade e endereço), juntamente com a exigência de compartilhar um código numérico de seis dígitos. Nesse contexto, pode alegar, por exemplo, que o código é indispensável para ativar (validar) um anúncio ou comunicar que

ocorreu um contratempo relacionado ao anúncio em questão, afirmando que a resolução do problema requer o fornecimento desse código.

Ao obter conhecimento dos dígitos do código de verificação, o infrator os insere no aplicativo WhatsApp instalado em seu próprio dispositivo móvel, permitindo-lhe se apropriar da conta da vítima e, assim, consumar o ardiloso esquema conhecido como "golpe de clonagem do WhatsApp". De maneira simultânea, a vítima perde o acesso à sua própria conta no aplicativo.

Através desse acesso ilícito, o criminoso avança para a etapa subsequente do esquema: a obtenção de benefício financeiro indevido. Em resumidas palavras, o trapaceiro, fazendo-se passar pela vítima, interage com familiares, cônjuge, parceiro(a), amigos, clientes e colegas de trabalho da vítima, alegando enfrentar dificuldades para quitar algum boleto ou acessar sua conta bancária. Ele menciona ter ultrapassado o limite diário de transações ou enfrentar problemas com o cartão de crédito, e solicita que a pessoa abordada (a nova vítima) realize a transação. Tudo isso é acompanhado da promessa de reembolso no dia seguinte.

A pessoa prejudicada, acreditando estar em diálogo com o(a) conhecido(a), descendente, progenitor(a) ou cônjuge, efetua o pagamento do boleto ou executa a transferência para a conta do fraudador (ou de um intermediário), resultando na consumação de mais uma infração.

A revelação de que ocorreu um golpe, em geral, só se dá quando o titular original do WhatsApp (a primeira vítima) consegue se comunicar com as demais partes envolvidas.

8.2 O golpe do boleto falso

O esquema do boleto falso constitui outra modalidade de estelionato virtual cuja prática está em ascensão no território nacional e se manifesta, sobretudo, através do encaminhamento por correio eletrônico. Entretanto, dada a ampliação do comércio digital, é também bastante frequente a execução desse ardil por meio de plataformas de redes sociais, WhatsApp, páginas fraudulentas, entre outras vias. Vários são os truques usados para enganar a vítima e induzi-la a pagar o documento fraudulento (Alves, 2019).

Uma parcela significativa das infrações ligadas aos boletos falsos segue o seguinte padrão: o indivíduo lesado recebe em sua caixa de entrada eletrônica um boleto genuíno referente a uma compra específica realizada ou um serviço contratado. Antes de realizar o pagamento, a vítima é contatada por outro e-mail contendo um novo boleto, porém com um montante menor. No conteúdo do e-mail, é comunicado que um cálculo de imposto teve um equívoco ou que o cliente foi agraciado com um abatimento.

O cliente, alicerçado na crença de ter recebido legitimamente o boleto da entidade responsável pelo produto ou serviço, procede com o pagamento. Algum tempo depois, passa a receber cobranças da empresa, as quais sustentam que o boleto não foi saldado. Incapaz de compreender a situação, a vítima reporta o pagamento e envia o recibo à empresa, nesse momento identificando-se a fraude presente no boleto.

8.3 O golpe do amor

O golpe do amor representa mais um crime direcionado aos utilizadores da web (frequentemente mulheres), os quais, nesta instância, se encontram em busca de um vínculo amoroso.

As vítimas comumente são abordadas pelos infratores por meio de perfis fictícios presentes em plataformas sociais ou outros portais de encontros online e, ao estabelecerem uma certa proximidade, iniciam a troca de mensagens pelo WhatsApp, Messenger ou e-mails, a título de exemplo. Nas conversações, os trapaceiros exibem afeto e devoção intensos às vítimas; proferem declarações de amor e oferecem a intenção de visitá-las. Normalmente, relatam ser indivíduos estrangeiros, frequentemente alegando ser fuzileiros ou marinheiros estadunidenses estacionados no Iraque ou Afeganistão, devido a operações de paz ou conflito.

Depois de envolver a vítima com manifestações amorosas, descreve dificuldades pessoais pelas quais está atravessando, como um filho doente, a falta de recursos para se alimentar ou regressar para casa, e solicita auxílio financeiro da parte da vítima para resolver a situação. A pessoa prejudicada, iludida e apaixonada, remete grandes somas de dinheiro ao criminoso, utilizando a conta bancária indicada (seja do próprio criminoso ou de intermediários).

Em outras circunstâncias, o fraudador comunica à vítima que enviará um presente (tais como joias, ouro, dólares) e, após decorrido um certo tempo, informa que o pacote ficou retido na alfândega. Para desbloquear o pacote, é alegadamente necessário efetuar um pagamento de taxa e a pessoa prejudicada, ansiosa para receber a encomenda, acaba concordando em transferir dinheiro para a conta bancária indicada pelo vigarista. Em muitas ocasiões, é o próprio criminoso que faz uma ligação para a vítima, fazendo-se passar por um funcionário da alfândega.

Torna-se evidente que a fraude se estende até que a vítima perceba ter sido enganada, o que normalmente ocorre após já ter sofrido prejuízos financeiros significativos. Os fictícios "namorados" desaparecem e as vítimas, então, tomam consciência de toda a trama na qual foram enredadas.

8.4 O golpe do site “fake”

Fake é uma palavra da língua inglesa que significa falso ou falsificação. Pode ser uma pessoa, um objeto ou qualquer ato que não seja autêntico. Dentro do contexto do comércio online, um esquema adicional que tem se tornado frequentemente observado é o golpe relacionado a sites fraudulentos. Geralmente, as pessoas não possuem o hábito de verificar os aspectos essenciais de segurança para garantir a autenticidade dos websites, o que as coloca em situação de vulnerabilidade diante das fraudes.

Nesse tipo de delito, o fraudador tem como alvo os usuários de plataformas de comércio eletrônico e, para atingir seu intento, elabora uma página virtual quase indistinguível da legítima. As vítimas, ao acreditarem estar acessando o site genuíno, selecionam os produtos desejados e realizam o pagamento, utilizando métodos como boleto bancário, cartão de crédito, depósito em conta ou transferência. Entretanto, tais indivíduos nunca recebem os produtos adquiridos.

Para além do adquirente, responsável pelo desembolso financeiro sem receber a mercadoria, esse gênero de atividade delituosa pode ocasionar

prejuízos a outras partes, tais como: uma corporação renomada e respeitável, cujo nome tenha sido associado à artimanha; um portal de ofertas coletivas ou instituição financeira, caso tenha intermediado a transação; um indivíduo, cujas informações tenham sido empregadas para a concepção do sítio eletrônico ou para a constituição de firmas fictícias.

8.5 Golpe do e-mail falso

Esse esquema visa pessoas que colocam à venda produtos em plataformas online.

De maneira resumida, o delito transcorre da seguinte forma: o indivíduo mal-intencionado identifica um item que lhe interessa e, dentro da seção de 'Perguntas e Respostas' do site, sob o pretexto de buscar mais informações para uma possível transação, requer o número de telefone e endereço de e-mail do vendedor (a futura vítima). O vendedor, que não está ciente das normas de confidencialidade da plataforma ou opta por ignorá-las, compartilha as informações requisitadas.

Subsequentemente, a vítima recebe um e-mail fraudulento supostamente do site em eu colocou seu produto à venda, comunicando que o produto foi vendido e deve ser remetido para o endereço indicado. As mensagens contêm expressões como "Seu produto foi adquirido" ou "A venda foi concluída!".

É frequente encontrar em e-mails fraudulentos orientações para interromper a exibição do anúncio e encaminhar o documento que comprova o envio da mercadoria (juntamente com o número de rastreamento). Além disso, pode incluir uma comunicação indicando que o destinatário (o vendedor) deve efetuar o pagamento referente ao transporte, o qual será restituído futuramente

Logo após, o criminoso estabelece comunicação com a vítima, alegando ter efetuado a aquisição do item e exerce pressão para que esta despache a encomenda no menor intervalo de tempo possível. A vítima, confiando ter obtido uma autêntica validação da transação efetuada através da plataforma de vendas, remete o produto e fornece ao fraudador o código de rastreamento utilizado pelos Correios. O indivíduo sob suspeita, nesse momento, monitora a entrega da mercadoria e, ao se consumar, bloqueia quaisquer meios pelos quais a vítima possa tentar estabelecer contato.

Em geral, o vendedor somente percebe ter caído na armadilha ao constatar que não recebeu o pagamento referente à venda e, ao entrar em comunicação com a plataforma de vendas, é esclarecido de que o e-mail recebido confirmando a transação era falso.

8.6 Golpe do leilão falso

Atualmente, na internet, é possível encontrar uma ampla diversidade de plataformas de leilão online que foram concebidas com a única finalidade de executar artimanhas enganosas. Os delinquentes divulgam anúncios destes portais através do Google e de outros motores de busca, com o claro propósito de aumentar a visibilidade destes sítios e, ao mesmo tempo, incrementar as chances de sucesso nas atividades fraudulentas. Recentemente, foram detectadas instâncias de websites falsos que copiam o design dos sites associados aos Detrans (os Departamentos Estaduais de Trânsito são os órgãos

do Poder Executivo Estadual que fiscalizam o trânsito de veículos terrestres em suas respectivas jurisdições, no território Brasileiro).

Para clarificar, a mecânica destes ardilosos esquemas é a seguinte: indivíduos interessados em adquirir automóveis a preços mais acessíveis, ao depararem-se com os anúncios online, acessam os portais falsificados e efetuam um registro, o qual exige o envio de cópias de documentos pessoais por meio de e-mail ou WhatsApp. Posteriormente, eles recebem chamadas de supostos funcionários do website, que confirmam os dados pessoais das futuras vítimas e comunicam que, a partir daquele momento, possuem permissão para acompanhar os leilões virtuais e colocar lances.

De forma rotineira, as vítimas conseguem adquirir os veículos desejados logo nos primeiros lances. Logo após, elas recebem uma carta ou termo de arrematação, incluindo informações relacionadas às contas bancárias de indivíduos particulares (pertencentes aos perpetradores do esquema ou a intermediários), destinadas a receber os pagamentos pelos automóveis.

As pessoas lesadas realizam os pagamentos e enviam os registros de confirmação. Após verificarem o recebimento do pagamento, os criminosos bloqueiam o acesso das vítimas ao WhatsApp e recusam futuras chamadas. Consequentemente, as vítimas, que nunca irão de fato adquirir os automóveis, acabam percebendo que foram envolvidas em uma artimanha.

No que diz respeito a essa conduta delituosa, é relevante enfatizar duas das táticas mais frequentes empregadas para ludibriar as vítimas: a exploração de nomes de plataformas de leilões de renome no Brasil e a constituição de websites utilizando domínios que se assemelham aos autênticos. Como exemplo ilustrativo, podemos mencionar o sítio www.copart.com.br (GENUÍNO) e o sítio www.copartleilao.com (FALSO). É perceptível que no sítio fraudulento, a palavra 'leilao' foi inserida ao título e o sufixo de domínio usado foi '.com' (em vez de 'com.br'), sugerindo que o site está hospedado em um servidor internacional. Esses pormenores são aparentemente simples, mas se negligenciados, podem induzir incontáveis clientes a se tornarem vítimas do ardil do falso leilão.

9 AS DIFICULDADES DE INVESTIGAÇÃO

À medida que as inovações tecnológicas continuam a acontecer, os crimes virtuais estão aumentando em proporção, e são diversas as maneiras de cometer um crime cibernético. Portanto, para que as investigativas sejam bem-sucedidas ao tomar ciência da realização de um crime dessa índole, é necessário esboçar qual foi a ferramenta empregada pelos infratores para a conduta ilegal.

O crime pode ter ocorrido através da manipulação de softwares nocivos, aplicativos de mensagens em tempo real, correio eletrônico, páginas da web, softwares de compartilhamento de dados, fóruns de discussão, plataformas sociais, comércio online, dentre uma ampla variedade de outros meios. Dependendo do canal utilizado, as abordagens empregadas para desvendar a autoria variarão.

Nesse sentido, a investigação abarca o conjunto de ações que, conforme as disposições da legislação processual penal, têm o propósito de examinar a presença de uma transgressão, identificar seus perpetradores e sua culpabilidade, além de revelar e coletar as evidências, no decurso do procedimento.

Jorge, (2020, p. 17) sustenta que:

> A investigação criminal tecnológica é o conjunto de recursos e procedimentos, baseados na utilização da tecnologia, que possuem o intuito de proporcionar uma maior eficácia na investigação criminal, principalmente por intermédio da inteligência cibernética; extração de dados de dispositivos eletrônicos; novas (e velhas) modalidades de afastamento de sigilo; utilização de fontes abertas; equipamentos e softwares específicos que permitem a análise de grande volume de dados; identificação de vínculos entre alvos; obtenção de informações impossíveis de serem agregadas de outra forma.

As principais ferramentas empregadas na investigação de delitos cibernéticos incluem: Análise de Registros e servidores; Monitoramento de comunicações eletrônicas; Avaliação de fluxos de dados; Identificação de plataformas; Reconhecimento visual de rostos; Observação do ambiente circundante, e outras técnicas.

Os métodos estabelecidos pela legislação do Brasil para a obtenção de evidências são os seguintes: Infiltração Policial Real conforme a Lei n° 12.850/2013; Infiltração Virtual segundo a Lei n° 13.441/2017, combinada com a Lei 12.850/2013 (acrescentada pelo Pacote Anticrime – Lei n° 13.964/2019); Acesso a informações telemáticas protegidas por sigilo; Quebra de confidencialidade de comunicações telefônicas; Acesso a registros de atividades e endereços IP; Interceptação do ambiente físico; Disposições dos Artigos 7°, 10 e 22 da Lei 12.965/2014 (Marco Civil da Internet); Emendas da Lei Anticrime (Lei n° 13.964/19) – introduzindo o artigo 3°-A até o artigo 3°-F ao CPP - Implementação do Juiz das Garantias.

O objetivo primordial do procedimento de investigação consiste em descobrir informações proveitosas, essenciais e oportunas, e ajudar o pesquisador a evitar desperdício de tempo com aquilo que estão prontamente acessível.

São numerosos os obstáculos que as instituições do Ministério Público, da Polícia e do Poder Judiciário no Brasil enfrentam ao tentar sancionar os perpetradores envolvidos em atividades de cibercrime. Uma destas barreiras consiste na carência de diretrizes claras que definam os delitos cibernéticos e os categorizem de forma organizada. Neste contexto legal, a aplicação de penalidades somente pode ser efetivada quando há certeza quanto à ocorrência do crime, sendo imprescindível a apresentação de provas concretas da autoria e materialidade, ou a presença de evidências substanciais que apontem a atuação do indivíduo na prática criminosa. Adicionalmente, deficiências tecnológicas e a escassez de especialistas contribuem para a ineficaz abordagem à questão dos cibercrimes.

Para além da essencial necessidade de evidências e identificação dos autores, as provas obtidas para respaldar os casos de crime devem ser coletadas de maneira lícita, ou seja, em conformidade com as leis vigentes. Tal condição complica a condução das investigações sobre delitos cibernéticos, pois no estágio inicial da investigação, a polícia busca determinar a natureza e localização do crime, e posteriormente procura rastrear o endereço de IP (um número que identifica um dispositivo na rede). Uma vez obtido o IP do infrator, a divisão de investigação policial entra em contato com a empresa que atribuiu o número à rede, e somente então a identificação do indivíduo criminoso é possível.

Em diversos cenários, para obter informações de identificação do IP, a autorização judicial se faz necessária a fim de conduzir investigações e interações com as empresas que detêm informações sobre a localização dos criminosos, respeitando o respaldo legal que salvaguarda a privacidade e os dados dos usuários. Esse processo, contudo, resulta em atrasos consideráveis na obtenção de evidências. Além da morosidade processual, algumas empresas de informação, mesmo com a aprovação do sistema judiciário, optam por não compartilhar informações sobre os usuários sob investigação, retardando e prejudicando a coleta de provas essenciais no decorrer da investigação.

Consequentemente, os desafios ligados à identificação da autoria não estão centrados na identificação do computador do qual a atividade ilícita se originou ou no responsável por tal máquina; ao invés disso, o cerne do problema é localizar a pessoa que agiu com a intenção de cometer a ação ilegal ou que de alguma forma colaborou com a conduta em questão. De fato, a principal dificuldade decorre da complexa tarefa de correlacionar um computador a um indivíduo que o operou em um determinado espaço de tempo.

Apesar das ações tomadas e introduzidas recentemente, é crucial promover um contínuo aprimoramento das estratégias para enfrentar os delitos cometidos no espaço digital. É necessário buscar de forma constante um maior acúmulo de conhecimento, que viabilize uma atuação eficaz. Isso envolve a promoção de uma especialização mais aprofundada dos profissionais, o aperfeiçoamento das habilidades em informática, a alocação de investimentos em tecnologias que ampliem as capacidades de detecção dos crimes, a capacitação dos policiais por meio de treinamento especializado, a expansão do número de delegacias com equipes dedicadas ao cenário virtual e a atualização das leis pelo legislador diante da evolução de novos comportamentos, possibilitando a formulação de legislações adaptadas à situação atual. Dada a tendência de aumento dos delitos, em paralelo ao avanço tecnológico constante, tais incidentes demandam uma resposta das autoridades em escala equivalente.

10 CONCLUSÃO

Com base no exposto, fica evidente que o Estado confronta desafios consideráveis ao tentar reprimir o estelionato eletrônico. A carência de vontade e clareza, apesar das alterações recentes na legislação, bem como a ausência de uma estrutura adequada para investigações nesse âmbito, são fatores que contribuem para essa situação.

Perante essa conjuntura, é essencial adotar a prevenção como a rota mais adequada. Investir em medidas de proteção para salvaguardar as informações disponibilizadas online é de suma importância, visando evitar uma série de danos, incluindo prejuízos à reputação das organizações.

Adicionalmente, é fundamental promover a conscientização e a inclusão digital na sociedade, educando as pessoas sobre o uso prudente e seguro das ferramentas informáticas. Contudo, é necessário reconhecer que a abordagem criminal também carece de aprimoramento para lidar com as novas realidades sociais, garantindo a aplicação de sanções em conformidade com o princípio da proporcionalidade.

O Estado deve incessantemente buscar a renovação e a inovação de suas leis, políticas públicas e iniciativas, antecipando-se aos movimentos da

criminalidade e compreendendo as peculiaridades da era contemporânea e a crescente imersão tecnológica.

Para eficazmente combater a fraude digital e outros delitos perpetrados no meio virtual, é imperativo o esforço conjunto da sociedade, dos poderes estabelecidos e de outras entidades públicas. Isso requer apropriados investimentos em medidas preventivas, a manutenção das já existentes e uma repressão bem qualificada.

A união de todos é indispensável para fomentar um ambiente seguro e para assegurar que aqueles que insistem em agir à margem da sociedade sejam devidamente responsabilizados, respeitando os preceitos de cidadania.

No contexto atual, é claro a complexidade enfrentada pelas forças de segurança ao lidar com a investigação e identificação dos diversos fraudadores presentes no ambiente virtual.

Diante dessa realidade, é crucial que o Estado aumente a alocação de recursos para as agências de polícia judiciária, com o objetivo de simplificar e agilizar as atividades diárias nesse domínio.

Para isso, é necessário priorizar investimentos nas delegacias especializadas em crimes cibernéticos, tanto em termos de equipamentos como no aumento do quadro de agentes.

Vale enfatizar que, embora a tecnologia seja uma facilitadora em diversas atividades, em algumas situações, também representa um custo significativo.

Por conseguinte, é imprescindível investir em tecnologias e equipamentos que possam aprimorar e agilizar os serviços cotidianos, como uma medida essencial para progredir no enfrentamento da criminalidade e da fraude virtual.

Além das medidas sugeridas anteriormente, é importante destacar que existem outras soluções que podem contribuir eficazmente para combater a criminalidade digital.

Por fim, o enfrentamento desses delitos requer um conjunto amplo e contínuo de ações, capaz de confrontar os desafios em constante evolução no ambiente virtual. É necessário estar preparado para adaptar e aprimorar constantemente as estratégias utilizadas, a fim de garantir um ambiente virtual mais seguro e protegido para todos.

REFERÊNCIAS

ALVES, Paulo. Golpe do boleto falso: sete dicas para não cair em armadilhas. **TechTudo**, 20 out. 2019. Disponível em: https://www.techtudo.com.br/listas/2019/10/golpe-do-boleto-falso-sete-dicas-para-nao-cair-em-armadilhas.ghtml. Acesso em: 1º jul. 2023.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, DF: Presidência da República, [1991]. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htmAcesso em: 22 jul. 2023.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Brasília, DF: Presidência da República, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm. Acesso em: 22 jul. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 22 jul. 2023.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 29 jul. 2023.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília, DF: Presidência da República, 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 29 jul. 2023.

BRASIL. Superior Tribunal de Justiça. Lei 14.555/2021 só alterou competência para julgamento de estelionato em casos específicos. **Notícias**, 30/05/2022. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/30052022-Lei-14-5552021-so-alterou-competencia-para-julgamento-de-estelionato-em-casos-especificos.aspx. Acesso em: 29 jul. 2023.

BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. **Estelionato**. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/estelionato#:~:text=O%20crime%20de%20estelionato%20exige,a%20leva%2Dlo%20a%20erro. Acesso em: 29 jul. 2023.

CAPEZ, Fernando. **Curso de direito penal, v. 1:** parte geral: arts. 1º a 120. 15. ed. São Paulo: Saraiva Educação, 2011.

CAPEZ, Fernando. **Curso de direito penal, v. 2:** parte especial: arts. 121 a 212. 20. ed. São Paulo: Saraiva Educação, 2020.

CAPEZ, Fernando. **Curso de direito penal, v.3**: parte especial: arts. 213 a 359-T. 18. ed. São Paulo: Saraiva Educação, 2020.

CARNEIRO, Adeneele Garcia. **Crimes virtuais:** elementos para uma reflexão sobre o problema na tipificação. 1 abr. 2012. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. Acesso em: 31 jul. 2023.

CAVALCANTE, Márcio André Lopes. No crime de estelionato, não identificadas as hipóteses descritas no § 4º do art. 70 do CPP, a competência deve ser fixada no local onde o agente delituoso obteve, mediante fraude, em benefício próprio

e de terceiros, os serviços custeados pela vítima. **Buscador Dizer o Direito**, Manaus. Disponível em: https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/0a66e17d3ccde15bdecb253e7e293294. Acesso em: 24 ago. 2023.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.

CRESPO, Marcelo Xavier de Freitas. Crimes digitais: do que estamos falando. **Canal Ciências Criminais**. 11/08/2022. Disponível em: https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/. Acesso em: 24 ago. 2023.

CUNHA, Rogério Sanches. **Manual de direito penal:** parte especial (arts. 121 ao 361). 11.ed. rev., ampl. e atual. Salvador: JusPodivm, 2019.

DUARTE, Samuel Victor; ALMEIDA, Tyciano Magno de Oliveira. Coagindo Crimes Cibernéticos: uma análise do Arcabouço Legal Brasileiro para a Segurança Digital e Comunicação. **Altus Ciência**, v.18, ago. a dez. 2023. Disponível em: http://revistas.fcjp.edu.br/ojs/index.php/altusciencia/article/view/148/115. Acesso em: 24 ago. 2023.

FERREIRA, Ivette Senise. **Direito & internet**: aspectos jurídicos relevantes. 2. ed. São Paulo: Quartier Latin, 2005.

GARUTTI, Hallifer Augusto; BRITO, Alexis Couto de. **Crimes cibernéticos:** uma análise sobre o estelionato virtual. Disponível em: https://revista.pgm.fortaleza.ce.gov.br/revista1/article/view/412/347. Acesso em: 31 jul. 2023.

GOLPISTA falsifica anúncio e engana vendedor e comprador ao mesmo tempo. **Balanço Geral**. 2019. Disponível em: https://www.youtube.com/watch?v=zNyVie0YsfI. Acesso em: 31 jul. 2023.

GRECO, Rogério. **Curso de direito penal, v. 1:** artigos 1º a 120 do Código Penal. 15. ed. Rio de Janeiro: Impetus, 2013.

HENIS, Débora. **Sofri um golpe no mercado livre!** 2020. Disponível em: https://www.youtube.com/watch?v=6C3_46wm5uY. Acesso em: 31 jul. 2023.

HONÓRIO, Gustavo, STABILE Arthur; E PAIVA, Deslange. **Estelionatos no Brasil mais que quadruplicam em cinco anos, e golpes virtuais disparam após pandemia, revela Anuário:** de acordo com dados do Anuário Brasileiro de Segurança Pública 2023, em 2022, foram 151,6 mil casos por mês ou 208 golpes por hora. 20/07/2023. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2023/07/20/estelionatos-no-brasil-mais-que-triplicam-em-cinco-anos-e-golpes-virtuais-disparam-apos-pandemia-revela-anuario.ghtml. Acesso em: 31 jul. 2023.

JORGE, Higor Vinícius Nogueira. **Tratado de investigação criminal tecnológica.** Salvador: JusPodivm, 2020.

LIMA, Renato Brasileiro. **Manual de processo penal**. 7. ed. rev., atual. e ampl. Salvador: JusPodivm, 2019. 2v.

MALHEIRO, Emerson Penha. **Delitos virtuais praticados na sociedade da informação**. Disponível em: https://rkladvocacia.com/delitos-virtuais-praticados-na-sociedade-da-informacao/. Acesso em: 10 jul. 2023.

FARIA, Pedro. Minas é o segundo estado com mais golpes virtuais no país. **Estado de Minas**, 20/07/2023. Disponível em: https://www.em.com.br/app/noticia/gerais/ 2023/07/20/interna_gerais,1522879/minas-e-o-segundo-estado-com-mais-golpes-virtuais-no-pais-veja-numeros.shtml. Acesso em: 10 jul. 2023.

PC revela tendência de aumento de crimes de estelionato no Vale do Aço. Disponível em: https://www.diariodoaco.com.br/noticia/0109141-pc-revela-tendencia-de-aumentos-de-crimes-de-estelionato-no-vale-do-aco. Acesso em: 10 jul. 2023.

POLICIA Civil investiga ocorrências de golpes de boletos falsos em Montes Claros. **MG Inter TV**, 2018. Disponível em: https://globoplay.globo.com/v/7106735/. Acesso em: 31 jul. 2020.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. **Jus Navigandi**, Teresina, ano 7, n. 60, 1 ago. 2002. Disponível em: https://jus.com.br/artigos/3186/o-problema-na-tipificacao-penaldos-crimes-virtuais. Acesso em: 12 fev. 2023.

RIBEIRO, Eliete da Silva. **Crime de estelionato:** uma análise da evolução sob a égide da impunidade na cidade de Manaus. 2019. Disponível em: https://semanaacademica.org.br/system/files/artigos/crime_de_estelionato_-_uma_analise_da_evolucao_sob_a_egide_da_impunidade_na_cidade_de_manaus_eliete_ da_silva_ribeiro_0.pdf. Acesso em: 03 mar. 2023.

ROSA, Fabrizio. **Crimes de informática**. Campinas: Bookseller, 2002.

SAIBA como se proteger do golpe da clonagem do WhatsApp. Hoje em Dia. 2020. Disponível em: https://www.youtube.com/watch?v=0mN_WQJ_J4M. Acesso em: 31 jul. 2023.

SILVA, Patrícia Santos da. **Direito e crime cibernético:** análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015. Disponível em: https://profmatheus.com/wp-content/uploads/2017/05/direito-crime-cibernetico.pdf. Acesso em: 31 jul. 2023.