ESTELIONATO VIRTUAL:
Uma análise da prática e repressão desse crime na cidade de Macapá-AP, entre os anos de 2018 a 2021

Daniela Regina Gabriel Machado[1]
Sérgio Grott[2]

RESUMO

O presente artigo discorre sobre o conceito do crime de estelionato praticado em ambiente virtual e tem como propósito apresentar a atividade especializada, desempenhada pelas autoridades policiais, por meio da Delegacia de Repressão aos Crimes Cibernéticos (DR-CCiber), na cidade de Macapá. Desta feita, apresenta- se o seguinte questionamento: A atuação deste órgão especializado traz resultados mais efetivos à sociedade, se comparado às delegacias comuns? A pesquisa adotou como forma de abordagem o método hipotético-dedutivo, além de uma pesquisa exploratória realizada por e-mail. O objetivo geral deste artigo é esclarecer à sociedade amapaense a forma pela qual agem esses criminosos atuantes no Estado do Amapá. Outrossim, na busca de respostas ao problema da pesquisa, por meio dos objetivos específicos foram descritas, a importância da criação e atuação da DR-CCiber, a abordagem das práticas de estelionato virtual e as formas de acesso com segurança ao ambiente virtual, e por fim, a necessária identificação de meios para evitar ser uma vítima desse golpe.

Palavras-chave: Estelionato virtual. Crimes cibernéticos. Segurança.

ABSTRACT

This article discusses the concept of embezzlement crime practiced in a virtual environment and aims to present the specialized activity performed by police authorities, through the Police Office for the Repression of Cyber Crimes – DR- CCiber, in the city of Macapá. This time, the following question is presented: Does the performance of this specialized body bring more effective results to society, if compared to common police stations? The research adopted as a way of approaching the hypothetical-deductive method, in addition to an exploratory research carried out by e-mail. The general objective of this article is to clarify to the society of Amapá the way in which these criminals acting in the State of Amapá act. Furthermore, in the search for answers to the research problem, the importance of the creation and performance of DR-CCiber, the approach of virtual embezzlement practices and ways to safely access the virtual environment were described through the specific objectives, and by and finally, the necessary identification of means to avoid being a victim of this scam.

Keywords: **V**irtual embezzlement. Cyber crimes. Safety.

[1] Graduanda em Direito pelo Centro de Ensino Superior do Amapá – CEAP. E-mail: profdanigabi@gmail.com
[2] Docente do Centro de Ensino Superior do Amapá. Mestre em Direito. Delegado de Policia.

1 INTRODUÇÃO

A realização de transações pela internet, nos últimos anos tornou-se corriqueira e atrativa, talvez pela facilidade e baixo custo que a tecnologia emergente promove. Esse aumento exponencial também mostra um lado negativo, que é constatado através da prática de estelionato virtual que tem crescido, principalmente na cidade de Macapá, no Estado do Amapá. Um dos motivos de tal crescimento nesse tipo de delito é a facilidade de acesso por meio de computador, tablet ou celular, conectado a um dispositivo que, em algumas situações abre caminho para atuação de indivíduos maliciosos e com inclinação para o mal, que acabam enganando pessoas em geral, as quais se tornam reféns e em muitas situações perdem dinheiro em espécie ou até mesmo, os seus patrimônios.

Outro motivo de aumento da prática desse crime tem sido a realização de atividades profissionais e pessoais pelos meios digitais, por causa da necessidade de distanciamento social imposta pela pandemia de Covid-19. Os estelionatos virtuais têm se expandido com técnicas cada vez mais engenhosas e consequentemente os resultados são devastadores vitimando e prejudicando centenas de pessoas todos os anos, além de serem crimes em que a identificação de seus autores, quase em sua maioria, é impossível acontecer, fazendo com que sua repressão fique aquém do que a sociedade espera.

Por esse motivo, as autoridades policiais entenderam necessária a criação de uma força policial especializada, onde foi inaugurada em 2021 a Delegacia de Repressão aos Crimes Cibernéticos (DR-CCiber). Assim, chegou-se ao problema dessa pesquisa no qual direciona ao seguinte questionamento: Como a atuação deste órgão especializado trará resultados mais efetivos à sociedade, se comparado com as delegacias comuns? Independente de graduação, todos estão a mercê de ações criminosas praticadas por pessoas mal intencionadas e ardilosas, que com lábia perspicaz convencem as vítimas e ganham confiança, tirando proveito da situação.

À vista disso, o objetivo geral deste trabalho é esclarecer à sociedade amapaense, a forma pela qual agem esses criminosos atuantes no Estado do Amapá e como a DR-CCiber vem atuando no combate a esse tipo de delito. Para tanto, torna-se necessário mostrar que ninguém está protegido, podendo se tornar uma vítima desse golpe. Para isso foram estabelecidos os seguintes objetivos específicos: a) Descrever o conceito de estelionato e suas facetas em ambiente virtual e a importância da segurança cibernética; b) Conhecer o rol de jurisprudências, legislações e doutrinas atuais que visam impedir ou punir quando da atuação de criminosos estelionatários; c) Demonstrar a atuação da DR-CCiber no combate aos crimes virtuais, especificamente, o estelionato virtual.

A finalidade deste artigo não é esgotar o assunto, mas realizar um breve estudo esclarecedor dos crimes de estelionato virtual utilizando-se como forma de abordagem o método hipotético-dedutivo, por meio de pesquisa bibliográfica, legislação vigente, consulta a fontes oficiais de informações concernentes ao tema no Estado do Amapá, análise documental, entrevista semiestruturada, além da pesquisa exploratória por e-mail, com apuração de dados da Polícia Civil no Estado do Amapá. Assim, o presente trabalho busca analisar as ocorrências e o impacto resultantes às vítimas, desse crime psicologicamente cruel e assim buscar sugestões e conhecimento para que as dúvidas e os medos sejam minimizados.

Desta forma, o presente artigo está organizado por essa introdução, quatro seções e considerações finais. A primeira seção descreve o conceito de estelionato e suas facetas em ambiente virtual e a importância da segurança cibernética. A segunda seção traz o rol de jurisprudências, legislações e doutrinas atuais que visam impedir ou punir quando da atuação de criminosos estelionatários. A terceira seção retrata a atuação da DR-CCiber, após sua criação, no combate aos crimes virtuais, especificamente o estelionato virtual. E a quarta e última seção orienta sobre formas para evitar ser uma vítima desse delito tão cruel e traiçoeiro e aponta vários crimes virtuais que foram e estão sendo praticados em Macapá-AP.

2 CONCEITO DO CRIME DE ESTELIONATO

Analisando o conceito de estelionato, destaca-se as explicações de Rogério Grecco (2020, p. 521-522), onde são identificados os elementos que envolvem o delito de estelionato, os quais retratam um tipo que exige o que podemos chamar de “cadeia causal”, melhor dizendo refere-se a uma sequência de atos cometidos, sendo a primeira atitude conhecida como utilização de artifícios ardilosos ou outro meio fraudulento de agir, sendo esse mecanismo astucioso considerado puramente intelectual.

O segundo ato sequenciado é a indução ou manutenção de alguém em erro. Isso ressalta a ideia de que a pessoa que está sendo enganada não possui a noção do que está acontecendo. O terceiro elemento do estelionato é a disposição patrimonial da qual decorre o binômio “vantagem ilícita em prejuízo alheio”. Entretanto, não basta a presença dos elementos citados, pois é imprescindível que exista entre esses o último elemento que é o nexo causal, ou seja, que se encontre a relação de causalidade entre eles. Assim, entre as faces do estelionato deve sobrevir uma incessante relação de causa e efeito (GRECO, 2020).

2.1 O CRIME DE ESTELIONATO EM AMBIENTE VIRTUAL

O estelionato, como modalidade de crime foi transportada para os ambientes virtuais, isto motivado pelos avanços tecnológicos e pela criação dos mais variados dispositivos que facilitam o cotidiano da sociedade. Tal crime com sua peculiar ligeireza adaptou-se a toda essa nova realidade virtual utilizando-se desses meios eletrônicos para o cometimento de muitos delitos, em especial o estelionato virtual. Para Roque (2007, p. 25), o crime cibernético é “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material.”

Destarte, em seu artigo intitulado “Crimes Cibernéticos”, Talles Leandro Ramos Nascimento (2018),

entende como crimes virtuais àqueles praticados pela internet, identificados pela falta de presença palpável do agente, os quais podem receber variadas nomenclaturas, tais como: crimes digitais, cibernéticos, virtuais, telemáticos, informáticos, entre outros. Nascimento destaca também, que o crime de estelionato em ambiente virtual está tipificado na mesma conduta apresentada no art. 171 do Código Penal (CP), e que a diferença entre eles é o formato, ou seja, o modus operandi do agente, para a prática de tais delitos.

Nesse sentido, é evidente que o maior motivo às práticas de crimes de estelionato virtual é atribuído a falsa sensação de que o ambiente virtual é um "lugar sem leis", o que não tem representado na atualidade, pois mesmo que de forma tímida e passageira, a punição aos infratores, tem sido a busca das autoridades responsáveis, como também, a repressão aos crimes praticados. Importante destacar também que, doutrinariamente o crime em ambiente virtual classifica-se de duas formas: crimes próprios e impróprios, e crimes puros, mistos e comuns.

Para Marcelo Crespo (2016), em seu artigo "Crimes digitais: do que estamos falando?", os crimes digitais são divididos em dois tipos, conforme se observa:

> 1. crimes digitais próprios ou puros (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os sistemas informáticos e os dados. São também chamados de delitos de risco informático. São exemplos de crimes digitais próprios o acesso não autorizado (hacking), a disseminação de vírus e o embaraçamento ao funcionamento de sistemas.
> 2. crimes digitais impróprios ou mistos (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os bens jurídicos que não sejam tecnológicos já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc). São exemplos de crimes digitais impróprios os contra a honra praticados na Internet, as condutas que envolvam trocas ou armazenamento de imagens com conteúdo de pornografia infantil, o estelionato e até mesmo o homicídio.

Assim, em detida análise, consideram-se crimes próprios aqueles em que o bem jurídico tutelado pela lei penal é a inviolabilidade das informações eletrônicas. Em contrapartida, os crimes impróprios são aqueles que afetam um bem jurídico comum, a exemplo de um sistema informático, como patrimônio individual. Portanto, independentemente do tipo, as condutas criminosas praticadas que envolvam tecnologia e estão previstas em lei, deverão ser punidas com pena criminal.

2.2 A SEGURANÇA DIGITAL COMO MEIO PARA PREVENIR A PRÁTICA DOS CRIMES DE ESTELIONATO

A importância da segurança digital tem sido um dos assuntos mais frequentes e necessário nos últimos tempos. Em matéria jornalística sobre cibercrime, a autora Fabiana Rolfini (2020), informa que de acordo com o levantamento da empresa tecnológica russa Kaspersky, a qual é especializada na produção de softwares de segurança para a internet, os ataques direcionados à ferramenta que permite acesso remoto aumentaram 333% no Brasil, entre fevereiro e abril de 2020.

Não obstante, importante destacar o conteúdo apresentado por Telium Networks (2018) sobre confidencialidade, integridade e disponibilidade: os três pilares que compõem a segurança da informação, os quais ressaltam a correta manutenção dos dados em relação aos sistemas e à infraestrutura tecnológica, senão vejamos: i) a confidencialidade, garante a disponibilidade da informação apenas para quem dela necessita fazer uso; ii) a integridade, a qual assegura que não houve alteração indevida na informação e que a mesma mantém sua exatidão e completude; e, por fim, iii) disponibilidade, que traz em seu conceito a comprovação de que a informação esteja disponível sempre que necessário.

Essas informações impulsionam à reflexão de que se torna cada vez mais necessário o cuidado com a segurança dos dados, seja ela em qualquer aspecto a ser considerado, como a tecnologia, os processos e o fator humano. Esses ataques, se permitido pelos usuários, podem danificar, destruir ou até mesmo tornar indisponível a comunicação de uma rede de sistemas. Sabe-se que a proteção no "mundo virtual" não é nada fácil, mas necessária, até pode ser uma tarefa árdua, mas trata-se de uma defesa para evitar transtornos e minimizar os problemas que surgirem. Por isso, é importante uma postura atenta e disposição para a prática dos cuidados indispensáveis com a segurança virtual no cotidiano, seja profissionalmente ou na vida pessoal.

3 A CONFIGURAÇÃO DO CRIME DE ESTELIONATO VIRTUAL – LEGISLAÇÕES VIGENTES E CLASSIFICAÇÕES DOUTRINÁRIAS

Como depreende-se, o crime de estelionato está tipificado no Código Penal Brasileiro (1940), no Capítulo VI – Do Estelionato e Outras Fraudes, art. 171, caput, que aduz: "Obter, para si ou para outrem, vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer meio fraudulento: Pena – reclusão, de um a cinco anos, e multa". Destaca-se, porém, que, recentemente o crime de estelionato previsto no art. 171 do CP, foi alterado pela lei n° 14.155/2021, a qual introduziu nos §§ 2°- A[3] e 2°- B[4] a figura da "fraude eletrônica" e trouxe maior severidade na punição quando se tratar de crimes de violação de dispositivo informático, furto e estelionato quando cometidos por meio eletrônico ou pela internet (ANDREUCCI, 2021).

Outro marco jurídico importante foi a nova lei sancionada, conhecida como "Lei do Pacote Anticrimes" n° 13.964/2019, que alterou substancialmente a natureza

[3] § 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.

[4] § 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.

da ação penal do crime de estelionato, o qual em relação ao seu processamento era mediante ação penal pública incondicionada e a partir de então será por meio de ação pública condicionada à representação, ou seja, passou-se a exigir representação da vítima para tramitação da ação penal, porém, com algumas exceções evidenciadas no § 5° do art. 171, da lei supracitada, a saber: a administração pública quando for o ofendido, criança ou adolescente, pessoas com deficiência mental ou maior de 70 anos de idade ou incapaz. Entretanto, essa mudança tem provocado muita divergência no meio jurídico, principalmente entre as turmas do Superior Tribunal de Justiça (STJ). O cerne da questão está em até que ponto a nova lei pode retroagir, para beneficiar o réu em processos cuja denúncia já foi oferecida pelo Ministério Público (ANDREUCCI, 2021).

O bem jurídico a ser tutelado pelo art. 171 do Código Penal é a inviolabilidade do patrimônio da vítima. Pode-se dizer que outros bens também são objetos de proteção como a boa-fé, quando dos relacionamentos tanto no interesse social quanto no interesse público. De outro giro, observa-se que a Constituição da República Federativa do Brasil de 1988 (CF/88), também estabeleceu diretrizes em defesa do patrimônio do cidadão. São instrumentos legais aptos para garantir a proteção desse patrimônio, conforme observa-se:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: XXII – é garantido o direito de propriedade; XXIII – a propriedade atenderá a sua função social;

É também dever do Estado manter a ordem pública e transmitir segurança, mesmo que em alguns casos seja necessário o uso da força e de seu poder de coação, por meio da autoridade policial e judiciária, promovendo a convivência social harmoniosa e pacífica. A ocorrência desse tipo de crime contra a pessoa ou seu patrimônio coloca em risco a harmonia e a paz social, como também fere os direitos fundamentais do indivíduo.

Em síntese, outro diploma legal sancionado, com importante destaque no campo jurídico foi a lei n° 12.965/2014, conhecida como o "Marco Civil da Internet". Tal lei prevê princípios que regulam a utilização da internet no Brasil, a exemplo dos princípios da proteção da privacidade e dos dados pessoais. Mesmo sendo considerada de caráter "civil", tem sua influência na investigação e atuação contra os crimes virtuais (NUCCI, 2017).

Por seu turno, outra lei de destaque no combate aos crimes virtuais segundo este autor foi a criação da lei n° 12.737/2012, popularmente conhecida como "Lei Carolina Dieckmann", em que a atriz, no ano de 2012, sofreu uma invasão em seu celular e teve suas fotos íntimas publicadas na internet. Destaca-se que houve alterações no Código Penal por causa desta lei, alterações essas que foram verificadas com a inserção dos arts. 154-A[5] e 154-B[6] identificando o crime de invasão de dispositivo informático.

De mais a mais, para Nucci (2017, p. 794), existem várias formas de se cometer o crime de estelionato, porém destaca-se em sua forma genérica "o que está disposto no caput do artigo 171, que trata do indivíduo quando o mesmo obtém determinado proveito indevido de outra pessoa ao persuadi-la a erro, ou até mesmo, fazer com que permaneça nele". O autor do crime pode provocar a situação de armadilha ou simplesmente fazer que a vítima permaneça no engano, usando de meios fraudulentos ou qualquer outra forma de fraude.

Embora difícil de catalogar as inúmeras formas de estelionato virtual, a fraude é considerada a causa do erro, uma forma maliciosa de enganar, que se refere a uma maneira de enriquecimento injusta. É a motivação do ato da vítima em dispor o patrimônio, permitindo assim o proveito ilegal em dano impensável. Se por um lado a fraude pode ser considerada qualquer meio embuste para alcançar um fim ilícito, por outro lado, em um formato mais amplo trata-se de um engano dolosamente provocado, em que a vítima é induzida a erro. Nesse momento, importante trazer a ideia do que é fraude. Segundo Venosa (2011, p. 213), "a fraude nada mais é do que o uso de meio enganoso ou ardiloso com o objetivo de envolver a lei ou um contrato, seja ele antecedente ou futuro".

De outro giro, Rogério Grecco (2020, p. 850-853) traz o entendimento da relação do estelionato com a fraude, destacando que há duas modalidades de estelionato: "a comissiva e a omissiva, como também, entende que ambas condutas implicam em fraude, seja quem de forma ativa causa o erro para um fim ilegal, quanto quem de maneira passiva deixa a vítima perseverar no erro e dele se utiliza". Por fim, Grecco (2020, p. 850-853) apresenta a classificação do crime de estelionato trazendo-a de forma resumida, conforme segue:

> Na verdade, conforme se verifica pela interpretação analógica determinada pelo caput do art. 171 do Código Penal, artifício e ardil fazem parte do gênero fraude, isto é, o engano, a artimanha do agente, no sentido de fazer com que a vítima incorra em erro ou, pelo menos, nele permaneça…A indução pressupõe um comportamento comissivo, vale dizer, o agente faz alguma coisa para que a vítima incorra em erro. Por outro lado, a conduta de manter a vítima em erro pode ser praticada omissivamente, isto é, o agente, sabedor do erro em que está incorrendo a vítima, aproveita-se dessa oportunidade, silenciando-se, a fim de obter a vantagem ilícita em prejuízo dela… Analisando a figura típica fundamental, podemos concluir que o estelionato é um crime comum tanto com relação ao sujeito ativo quanto ao sujeito passivo; doloso; material; comissivo e omissivo (tendo em vista ser possível esse raciocínio através da conduta de manter a vítima em erro); de forma livre (pois qualquer fraude pode ser usada como meio para a prática do crime); instantâneo (podendo, ocasionalmente, ser

[5] Art. 154-A. Invadir dispositivo informático alheio, 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: Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

[6] Art. 154-B. Invadir dispositivo informático alheio, 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: Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

> reconhecido como instantâneo de efeitos permanentes, quando houver, por exemplo, a perda ou destruição da coisa obtida por meio de fraude); de dano; monossubjetivo; plurissubsistente; transeunte ou não transeunte (dependendo da forma como o delito é praticado).

Esse resumo traz a ideia de que o tipo penal descreve uma atitude ou ação do criminoso que trará um resultado, como também é necessário a existência desse resultado para que o crime de estelionato seja consumado, considerando que o momento consumativo deste tipo de delito é quando a vítima sofre o prejuízo, ou seja, a perda patrimonial. Dessa forma, sobre os elementos objetivos do tipo, ensina Nucci (2020, p. 702) quando ressalta que:

> Há várias formas de cometimento de estelionato, prevendo-se a genérica no caput. Obter vantagem (benefício, ganho ou lucro) indevida induzindo ou mantendo alguém em erro. Significa conseguir um benefício ou um lucro ilícito em razão do engano provocado na vítima. Esta colabora com o agente sem perceber que está se despojando de seus pertences. Induzir quer dizer incutir ou persuadir e manter significa fazer permanecer ou conservar. Portanto, a obtenção da vantagem indevida deve-se ao fato de o agente conduzir o ofendido ao engano ou quando deixa que a vítima permaneça na situação de erro na qual se envolveu sozinha. É possível, pois que o autor do estelionato provoque a situação de engano ou apenas dela se aproveite. De qualquer modo, comete a conduta proibida.

A partir dessa informação, é feita uma análise dos métodos utilizados pelo criminoso, em que ele cita o artifício como astúcia, o ardil como cilada ou estratagema, e, o outro meio fraudulento como interpretação analógica. O autor também procurou explicar que "a utilização de mecanismos grosseiros de engodo não configura o crime, pois é exigível que o artifício, ardil ou outro meio fraudulento seja apto a ludibriar alguém". Como se vê a prática desse tipo de delito é muito vantajosa em várias situações pois sua engenhosidade é desde os primórdios entranhada nos seres humanos que pendem para essa prática e sua evolução cada vez mais eficiente, em muitos casos sem se quer deixar rastros, dificultando sua descoberta pelas autoridades policiais (NUCCI, 2020).

Quanto aos sujeitos envolvidos nesse delito, temos o sujeito ativo e o sujeito passivo. Cleber Masson (2020, p. 526) aduz essa diferenciação começando pelo sujeito ativo, onde explica que: "Pode ser qualquer pessoa (crime comum), tanto a responsável pelo emprego da fraude como aquela beneficiada pela vantagem ilícita. Vale frisar que normalmente tais condições reúnem-se na mesma pessoa." Já quanto ao sujeito passivo do delito, Masson afirma que: "Pode ser qualquer pessoa, física ou jurídica (de direito público ou de direito privado), seja quem for enganado pela fraude, seja quem suporta o prejuízo patrimonial." Ainda concluiu que: "Em regra, tais condições estão presentes em uma só pessoa." E que "a vítima deve ser pessoa certa e determinada, pois o tipo penal fala em prejuízo alheio, induzindo ou mantendo alguém em erro."

Segundo o explanado, não existe uma pessoa específica, nem tampouco definida para praticar tal crime. E ainda nem sempre o criminoso age sozinho, podendo contar com coautores ou partícipes, o que torna sua prática mais facilitada e sua descoberta mais árdua. Diante dessa afirmação, Masson (2020, p. 527) indica que é possível uma análise muito interessante ao exemplificar situações envolvendo incertezas quanto ao sujeito passivo na prática delituosa. Assim aduz:

> Consequentemente, as condutas voltadas a pessoas incertas e indeterminadas (exemplo: adulteração de bomba de posto de combustíveis ou de balança de supermercado), ainda que sirvam de fraude para obter vantagem ilícita em prejuízo alheio, configuram crime contra a economia popular, nos termos do art. 2°, inciso XI, da Lei 1.521/1951. Se contido alguém vier a ser efetivamente lesado, haverá concurso formal entre o crime contra a economia popular (contra as vítimas incertas e indeterminadas) e o estelionato (contra a vítima certa e determinada).

Dessa forma, há de se considerar que para a tipificação do crime de estelionato a vítima precisa ser alguém que sofre um dano, além é claro dos outros elementos já identificados anteriormente. Importante ressaltar que, a situação de engano transcende para o mundo dos negócios, mais especificamente, nas relações comerciais. Trata-se de uma linha muito tênue entre o engano de um simples ilícito civil e o engano de um crime capaz de privar o atroz de sua liberdade. Tal situação é ainda mais explicitada na abordagem de Grecco (2020, p. 847) quando afirma que:

> Na verdade, quem determina a gravidade da fraude e, consequentemente, a necessidade de criação da figura típica é o legislador, que atua movido por questões de política-criminal, que variam de acordo com cada momento pelo qual atravessa a sociedade. Assim, não há, na verdade, qualquer critério predeterminado que tenha o condão de traçar, com precisão, a diferença entre fraude civil e fraude penal, pois até a valoração de sua intensidade é levada a efeito de acordo com o sentimento político de cada época. Dessa forma, o que antes poderia ser entendido como fraude de natureza civil, amanhã já poderá receber a valoração exigida pelo Direito Penal.

Em contrapartida, mesmo com essa situação de imprecisão na diferenciação das fraudes civil e penal, as cortes superiores dispõem de duas posições sobre essa matéria. No primeiro posicionamento o STJ afirma que inexiste diferença ontológica entre fraude penal e fraude civil (STJ, HC 76106, Fischer, 5ª T., u., 14.6.2007), já a segunda posição permeia na diferença que reside no inadimplemento preordenado ou preconcebido que denota a fraude penal, a ser examinada após a instrução criminal (STF, RHC 59100, Muñoz, 1ª T., u., 25.8.1981).

Assim, o mero fato de a matéria estar sendo discutida no âmbito civil não afasta o estelionato." Portanto, há de se considerar que a ilicitude na prática do crime de estelionato deve ser analisada com rigor e apurada concretamente, pois é uma conduta amplamente discutida em nossa jurisprudência pátria (BALTAZAR JÚNIOR, 2017).

4 PRÁTICA E EVOLUÇÃO DO CRIME DE ESTELIONATO NA CIDADE DE MACAPÁ E A CRIAÇÃO DA DR-CCIBER

Por meio de entrevista semiestruturada, com perguntas abertas, respondidas por meio de formulário, encaminhado via e-mail, o delegado-geral da Polícia Civil de Macapá, o Sr. Antônio Uberlândio de Azevedo Gomes, ressaltou que as facilidades trazidas com a conexão da internet em âmbito mundial, certamente ensejou o aumento exponencial da prática do crime de estelionato. Aqui no Estado do Amapá, as autoridades policiais acreditam que a possibilidade de maior exposição da população nas redes sociais, bem como o crescente uso das plataformas digitais de compra e venda fizeram com que a criminalidade migrasse, paulatinamente para o meio digital.

Ademais, Uberlândio informa que do ponto de vista do criminoso, há diminuição dos riscos inerentes à sua atividade, pois agindo por meio digital, evita a possibilidade de eventual confronto direto com as forças policiais de segurança pública e, por vezes, seu único instrumento para a prática delitiva consiste em um mero aparelho celular. Além disso, os crimes são cometidos à distância, em várias ocasiões, em outras unidades federativas, distantes da residência da vítima, o que dificulta tanto na notificação à Polícia Judiciária pela crença da vítima na impunidade, quanto à própria atividade investigativa, que demanda cooperação interestadual.

Ainda de acordo com o delegado, outro ponto que merece destaque, é o acesso a telefones celulares por parte de criminosos que já estão cumprindo pena em presídios. Não raro, esses celulares são compartilhados entre vários detentos na mesma cela, o que também torna difícil a elucidação da autoria delitiva. Já, para a equipe da Polícia Civil de Macapá, o aumento do acesso à internet e a maior exposição da população nas redes sociais, bem como o crescente uso de plataformas digitais de compra e venda, tais como OLX, Facebook, Instagram,WhatssApp fizeram com que a criminalidade migrasse, paulatinamente, para o meio digital. A PC ressalta ainda que todas as modalidades de estelionato são praticadas na cidade de Macapá, sendo o mais comum, todavia, a utilização de meios digitais.

O Gabinete da Delegacia Geral da Polícia Civil do Amapá – DGPC/GAB, por meio do Ofício n° 350101.0076.21580127/2021, que pode ser verificado pelo link[7] disponibilizado da DGPC/GAB, encaminhou as informações de que o sistema de registro de ocorrências utilizado para a realização da pesquisa solicitada, começou a ser implantado no ano de 2017 e que os números podem sofrer alterações em virtude dos aditamentos de ocorrências, especialmente dos fatos que ainda estão sob investigação, como também, dos registros posteriores à data da pesquisa de fatos ocorridos no período solicitado. A priori, informa-se que os números a seguir referem-se aos fatos registrados como consumados.

No ano de 2018 foram registrados em torno de 66 crimes de estelionatos, em 2019 saltou para 181, quase 300% acima do registro do ano anterior. E em 2020, a tendência de aumento permaneceu, sendo que foi registrado 206 delitos de estelionato. Registra-se que todos esses crimes foram em ambiente virtual (internet). Lembrando também que existe um grande número de vítimas que não registram a ocorrência, por não acreditarem na justiça ou por medo de vingança do criminoso. E conclui que "tamanha é a astúcia desses criminosos, que utilizam-se da ingenuidade e confiança do usuário para obter informações que podem ser utilizadas para acessar desde os domínios não autorizados pelos usuários, quanto promover roubos de dinheiro, bens ou serviços de várias formas."

4.1 A ATUAÇÃO DA POLÍCIA, POR MEIO DA DR-CIBER DE MACAPÁ-AP COMO FORMA DE REPRESSÃO AO CRIME DE ESTELIONATO VIRTUAL

O crime de estelionato virtual é extremamente complexo, seja pelos inúmeros elementos constitutivos, seja pela árdua tarefa de diferenciar o crime de estelionato de um simples ilícito civil. Acompanhando a demanda social decorrente do aumento do crime de estelionato virtual, na cidade de Macapá-AP, foi criada, por intermédio da lei estadual n° 2.507, de 13 de agosto de 2020, a Delegacia de Repressão aos Crimes Cibernéticos (DR-CCiber). Sua criação se justifica pela própria evolução da criminalidade que vem aperfeiçoando seus métodos e se aproveitando das vulnerabilidades do ambiente virtual. Além disso, a ocorrência de cibercrimes cada vez mais complexos exige o trabalho de uma equipe melhor qualificada e capacitada para enfrentar os obstáculos da investigação em busca de vestígios virtuais.

Também como resposta ao questionário desenvolvido para análise da atuação da DR-CCiber, os profissionais qualificados para atuação na repressão ao crime de estelionato virtual, informaram que a delegacia em si, não atua por mera abstração, mas trata-se de uma capacidade desenvolvida por eles, os quais estão designados para tal trabalho e atuação, com conhecimento e precisão na busca incansável pela resolução dos crimes cometidos, e assim proporcionar a correta punição aos criminosos. Ressaltam que, pode haver delegacias, por exemplo, que não possuam nenhum profissional capacitado para atuar neste tipo de investigação, o que poderá culminar em procedimentos que não chegará à correta autoria.

Por isso, normalmente, cada delegacia conta com, pelo menos, um profissional que tenha certa experiência nesse ramo e que acumula também esta função, auxiliando na medida do possível a esperada conclusão das investigações. Esta é a maior vantagem de uma delegacia especializada neste tipo de ocorrência, pois conta com uma equipe de profissionais com expertise, dispostos a atuar exclusivamente na investigação destes crimes, e assim conferirá maior aproveitamento aos

[7]Site:https://sigdoc.ap.gov.br/public/autenticadorDocumento/index.jsf. Verificador: 35795318 Código CRC: FBD7E6E. Fonte: DGPC/GAB (2021)

procedimentos.

4.2 FORMA DE UTILIZAÇÃO DESSE SERVIÇO ESPECIALIZADO E SEUS RESULTADOS

A Delegacia especializada de combate aos crimes virtuais de Macapá foi criada com o intuito de especialização no apoio e na atuação da polícia civil, para inovação do atendimento à população trazendo respostas mais céleres e efetivas. Ainda como resposta ao questionário, o profissional atuante na DR-CCiber informa que a vantagem da criação desta delegacia é vista no semblante da população. A população após cair num golpe dessa natureza, clama para que sua ocorrência seja apurada, gerando assim, uma resposta positiva à população, de que não há impunidade no ambiente virtual, mas sim uma busca pela punição aos responsáveis pelo cometimento do crime.

Concluindo, ressalta que a principal vantagem é disponibilizar à população uma equipe de profissionais com qualificação necessária para investigar cibercrimes cada vez mais complexos, cujos autores costumam estar em outro estado da Federação e adotando ferramentas cada vez mais modernas para ocultar sua identidade, garantindo à sociedade o combate adequado dos crimes desta espécie, de modo a impedir que os autores destas práticas fiquem impunes.

Como todo início de projeto, a atuação da DR-CCiber, também apresenta algumas desvantagens que foram identificadas por seus profissionais em atuação. Por se tratar de uma delegacia com equipe reduzida, o ideal seria a designação específica para o combate aos crimes cibernéticos, porém, o problema é que a sede da DR-CCiber foi instalada em área aeroportuária, no Aeroporto Internacional de Macapá-AP, o que em muitas situações desvia o foco principal de investigação e solução de crimes, para atendimentos de atribuições que fogem do escopo da polícia civil.

Um exemplo é a equipe que poderia focar em solucionar casos que requerem uma atenção e tempo diferenciado, estão recebendo atribuições como apoio ao turista que a procura, ou outras situações que possam surgir devido a sua localização, podendo tirá-la do seu objetivo, foco e finalidade. Em vários momentos, a equipe de profissionais qualificados fica impossibilitada de se dedicar ao propósito para o qual foi designada.

Em vez disso, o profissional divide sua atenção com questões administrativas do aeroporto, muitas vezes adotando atribuições de polícia aeroportuária, deixando a investigação em segundo plano. Enfim, uma equipe ainda que diminuta, porém inteiramente voltada à investigação, certamente entregaria um resultado mais satisfatório à sociedade. Outra desvantagem é porque a maioria dos crimes são interestaduais, o que dificulta a prisão em flagrante.

Independente das desvantagens apontadas, a população tem à disposição um apoio no combate ao crime de estelionato virtual, o qual pode ser acionado em atendimento presencial, diretamente no Aeroporto Internacional de Macapá, com atendimento presencial de segunda a domingo, das 7h30 às 18h00. Se preferir, o cidadão pode registrar a ocorrência de forma virtual, acessando o link8, onde o registro da ocorrência é feito com base nas declarações da vítima, dispensando a apresentação de qualquer documento específico.

Porém recomenda-se que no momento do registro também sejam apresentados quaisquer documentos úteis à investigação, ou seja, o máximo de informação que possua, como registros de conversas, por qual meio encontrou ou foi encontrada pelo suposto infrator, comprovantes de pagamento, ou transferência, quando houver. E, por fim, documentos ou indícios que possam permitir a comprovação dos fatos alegados, e consequentemente do crime sofrido.

4.3 COMO EVITAR SER UMA VÍTIMA DO CRIME DE ESTELIONATO VIRTUAL

A maioria das plataformas digitais de maior relevo possuem sistemas de segurança consideráveis, tais como autenticação em dois fatores, que acrescentam uma camada adicional de segurança para o processo de login da conta, exigindo que o usuário forneça duas formas de autenticação. Para além do aumento da segurança das plataformas digitais, é preciso que as pessoas se conscientizem que o uso da tecnologia deve ser feito com as mesmas cautelas adotadas na vida em geral, desconfiando de preços atrativos, bem como redobrando o cuidado em relação aos golpes relacionados com a chamada engenharia social, que pode tornar qualquer pessoa vítima com o uso da persuasão.

A engenharia social utiliza da fragilidade emocional humana como tática de convencimento, fazendo com que as vítimas ou pessoas de seu relacionamento caiam em ardis que a levem a prejuízo. Ainda, segundo o delegado-geral Sr. Antônio Uberlândio, “dentre as várias modalidades de utilização dessa tática criminosa, podemos citar o Phishing, o Pretexting, o Quid pro quo, a Sextorsão, o Dumpster Diving, o Shoulder Surfing e o Tailgating, entre tantos outros golpes possíveis.”

De todo modo, é necessário que a população fique atenta e seja bem informada, desconfiando de ofertas de produtos com valor muito abaixo ao de mercado; envio de fotos íntimas a desconhecidos; solicitação de empréstimos por meio de ligações ou mensagens em aplicativos. Enfim, a cautela sempre será a melhor medida contra o crime de estelionato virtual, vez que é intrínseco dessa modalidade criminosa a utilização de ardil ou meio fraudulento capaz de induzir a própria vítima a auxiliar o criminoso na obtenção da vantagem ilícita.

4.4 TIPOS DE CRIMES DE ESTELIONATO COMETIDOS NO AMBIENTE VIRTUAL EM MACAPÁ

De acordo com o Ofício nº 350101.0076.21580127/2021, encaminhado pelo DGPC/GAB descreve-se abaixo algumas situações comuns registradas em ocorrências policiais na cidade de Macapá, entre os anos de 2018 a 2020:

1 – Golpe da casa própria – nesse tipo de golpe os estelionatários usam vários disfarces, alguns se passam por casal, outros por corretores de imóveis. Até facilitam a falsa venda, proporcionando parcelamento com uma

entrada de 50% do valor combinado, tudo para dar mais segurança ao comprador.

2 – Golpe do amigo – é o crime em que os golpistas clonam um aplicativo de conversas e a partir deste perfil replicado tentam conseguir dinheiro de amigos da vítima. Eles se passam pelo dono do perfil e usam as mais criativas justificativas para simular a necessidade da ajuda.

3 – Golpe da sedução – nesse tipo de delito os bandidos usam perfis falsos nas redes sociais de homens e mulheres para seduzir amorosamente as vítimas. Durante as conversas há troca de nudes (fotos íntimas) que posteriormente serão utilizadas para extorquir valores de quem foi enganado. Sendo nesse caso os alvos, em sua maioria homens casados, que para não serem descobertos pagam os valores solicitados pelos criminosos.

4 – Golpe do falso depósito – o líder da associação criminosa, que está preso, entra em contato com a vítima pelo WhatsApp e manifesta interesse na compra do que foi anunciado. Na sequência, outra pessoa vai buscar o bem adquirido e entrega para outro integrante do grupo. Após a vítima descobrir que não tem valor algum na conta bancária, não consegue mais contato com o suposto comprador.

5 – Golpe do anúncio falso – o estelionatário clona um anúncio real de um vendedor da plataforma (a exemplo da OLX) e entra em contato com o anunciante oferecendo um valor maior do que o anunciado, porém com a contrapartida de que o vendedor exclua o anúncio. A partir daí, sem o real vendedor saber, o criminoso anuncia o bem como sendo seu, com seu contato e com valor mais baixo do que o vendedor anunciou. Quando uma vítima interessada na compra entra em contato com o criminoso, também sem saber, conversa e realiza toda a negociação.

É claro que o estelionatário já está munido das informações do bem que será vendido e apresenta uma história inventada convencendo a vítima que o item é seu. É tão real a artimanha, que as vítimas só descobrem o golpe quando o comprador (maior prejudicado) já depositou o dinheiro na conta do suposto vendedor (criminoso) e o vendedor quando percebe que não recebeu nada para a venda, isso porque o dinheiro depositado para o comprador foi na do estelionatário.

5 CONSIDERAÇÕES FINAIS

Assim, conclui-se que os danos causados às vítimas de estelionato virtual podem ser de ordem física, material ou psíquica, que produz angústia moral e psicológica quando da consumação do delito. Ao concentrar a análise no domínio deste estudo, é possível identificar uma crescente na prática do crime de estelionato virtual, porém, apesar de alguns percalços também é visível o comprometimento das autoridades em atuar com ímpeto na busca pela resposta célere e elucidativa para a sociedade, por intermédio da Delegacia de Repressão aos Crimes Cibernéticos.

Todavia, mesmo com todos os esforços dispensados na busca de resultados concretos da atuação da DR-CCiber, ainda é prematuro definir o resultado de modo geral, visto que a delegacia conta com menos de 6 (seis) meses de existência, desde a sua criação. Porém, conclui-se que a alta procura diária para registro de ocorrências, reflete a aceitação e credibilidade da sociedade no trabalho que está sendo desenvolvido por ela. É certo que, o Poder Judiciário também é peça fundamental nesse combate, aplicando métodos punitivos e repressivos em relação ao agente criminoso, para que não venha cometer novamente a prática delitiva.

Sabe-se que, é dever constitucional do Estado proteger o patrimônio do cidadão, como também manter através da tutela estatal a ordem pública transmitindo segurança aos indivíduos, seja pela interferência policial ou judicial, garantindo assim condições favoráveis para a convivência pacífica da sociedade em geral. Por isso foi criada a DR-CCiber, que além de outros benefícios também tem promovido a conscientização da população amapaense, com informações e orientações para o combate ao crime de estelionato virtual, e assim tal prevenção não seja apenas esforço dos agentes policiais, mas de toda a sociedade, pois a Polícia Civil quando recebe os boletins de ocorrência, na maioria dos casos, o crime já foi consumado.

Diante do exposto, considera-se que a hipótese inicialmente formulada foi parcialmente confirmada. No que diz respeito ao engajamento da equipe especializada que atua na Delegacia de Repressão aos Crimes Cibernéticos, no combate aos crimes de estelionato virtual, os resultados foram positivos e a expectativa dos profissionais é que cada dia mais esse trabalho seja conhecido por toda a sociedade. Já no questionamento quanto à efetividade comparada com as outras delegacias, não foi possível mensurar pelo curto espaço de tempo da atuação da DR-CCiber. Assim, é cauteloso descrever que não houve possibilidade de mensuração entre as delegacias, deixando oportunidade para novas pesquisas.

REFERÊNCIAS

ABSY, Cindy. **O que são sistemas de segurança digital? 4 opções para se proteger.** 2021. Disponível em https://maplink.global/blog/sistema-seguranca-digital/. Acesso em: 19 out. 2021.

ALECRIM, Emerson. **Dicas de segurança na internet.** Atualizado 2019. Disponível em https://www.infowester.com/dicaseguranca.php. Acesso em: 19 out. 2021.

ANDREUCCI, Ricardo Antônio. **O crime de estelionato cibernético ou virtual.** 2021. Disponível em https://emporiododireito.com.br/leitura/o-crime-de-estelionato- cibernetico-ou-virtual. Acesso em: 19 out. 2021.

AMAPÁ. ASSEMBLEIA LEGISLATIVA DO ESTADO DO AMAPÁ. **LEI N° 2.507 DE 13 DE AGOSTO DE 2020. Criação da DR-CCiber**. Disponível em http://www.al.ap.gov.br/pagina.php?pg=buscar_legislacao&n_leiB=2507,%20DE%2013/08/20. Acesso em: 19 out. 2021.

BALTAZAR JUNIOR, José Paulo. **Crimes Federais.** 11. ed. São Paulo: Saraiva, 2017.

BARROS, Aidil Jesus da Silveira et al. **Fundamentos da Metodologia Científica.** 3. ed. São Paulo: Pearson Prentice Hall, 2007.

BOTO, Olho de. **Delegado escapa de golpes, e agora procura criminosos.** 2021. Disponível em https://selesnafes.com/2021/04/delegado-escapa-de-golpe-e-agora- procura-criminosos/. Acesso em: 03 jun. 2021.

BRASIL. **CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988 – CF/88**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 19 de nov. 2021.

BRASIL. DECRETO-LEI N° 2.848, DE 7 DE DEZEMBRO DE 1940. **CP**. Disponível Em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 19 nov. 2021.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. **Alteração CP**. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 19 nov. 2021.

BRASIL. LEI Nº 13.964, DE 24 DE DEZEMBRO DE 2019. **Lei Pacote Anticrimes**. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em: 19 nov. 2021.

BRASIL. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. **Lei Carolina Dieckman**. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 19 nov. 2021.

BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. **Marco Civil da Internet de 2014**. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 19 nov. 2021.

COMPUGRAF, Blog. **Quais os principais tipos de ataque de Engenharia Social**. 2020. Disponível em https://www.compugraf.com.br/quais-os-principais-tipos-de-ataque-de-engenharia-social/. Acesso em: 20 nov.2021.

COSTA, Paloma. **Análise do art. 171 do Código Penal.** 2016. Disponível em https://palomacosta.jusbrasil.com.br/artigos/225471133/analise-do-art-171-do- codigo-penal. Acesso em: 21 maio 2021.

CRESPO, Marcelo. **Crimes digitais: do que estamos falando?** 2016. Disponível em https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/. Acesso em: 19 nov. 2021.

FARAH, Danilo Morais. **A adequada tipificação criminal do saque em caixa eletrônico com a utilização de cartão clonado: um confronto entre os postulados clássicos dos delitos de estelionato e furto qualificado mediante fraude com a realidade contemporânea.** 2017. Disponível em: https://repositorio.uniceub.br/jspui/handle/235/11958. Acesso em: 21 maio 2021**.**

GIL, Antônio Carlos. **Métodos e Técnicas de Pesquisa Social.** 7. ed. São Paulo: Saraiva, 2019.

GOMES, Antônio Uberlândio de Azevedo, **Ofício n° 350101.0076.2158.0127/2021 Delegado Geral (DGPC/GAB – Delegacia Geral de Polícia Civil/Gabinete)**, em 17/05/2021. https://sigdoc.ap.gov.br/public/autenticadorDocumento/index.jsf. Verificador: 35795318 Código CRC: FBD7E6E

GRECCO, Rogério. **Curso de Direito Penal: Parte Especial (arts. 121 a 212).** 17. ed. vol 2. Rio de Janeiro: Impetus, 2020.

JESUS, Damásio. **Direito Penal. Parte especial: dos crimes contra a pessoa e dos crimes contra o patrimônio**. 28. ed. rev. e atual. São Paulo: Saraiva, 2007.

LOUREIRO, Marcelo. **Governador do Amapá sanciona lei anticorrupção e contra crimes organizados e cibernéticos.** 2020. Disponível em: https://www.portal.ap.gov.br/noticia/1408/governador-do-amapa-sanciona-lei-anticorrupcao-e-contra-crimes-organizados-e-ciberneticos. Acesso em: 21 out. 2021.

MARCONI, Marina de Andrade et al. **Metodologia Científica .** 7. ed. São Paulo: Atlas, 2017.

MASSON, Cleber. **Direito Penal: Parte Especial (arts. 121 a 212).** 13. ed. São Paulo: Método, 2020.

MORAES, Alexandre de. **Direito Constitucional.** 25. ed. São Paulo: Atlas, 2010.

NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** 2018. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso em: 24 out. 2021.

NETWORKS, Telium. **Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação**. 2018. Disponível em https://www.telium.com.br/blog/confidencialidade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao. Acesso em: 19 nov. 2021.

NUCCI, Guilherme de Souza. **Manual de Direito Penal.** 13. ed. Rio de Janeiro: Forense, 2017.

NUCCI, Guilherme de Souza. **Manual de Direito Penal.** 16. ed. Rio de Janeiro: Forense, 2020.

PEREIRA, Ana Carolina dos Santos. **O estelionato virtual.** 2021. Disponível em: https://anacarolinasantospereira.jusbrasil.com.br/artigos/667046774/o-estelionato- virtual. Acesso em: 19 out. 2021.

PEREIRA, Jeferson Botelho. **Aspectos jurídicos da novíssima Lei n° 14.155, de 27 de maio de 2021.** Disponível em: https://jus.com.br/artigos/90857/aspectos-juridicos-da-novissima-lei-n-14-155-de-27-de-maio-de-2021. Acesso em: 19 out. 2021.

ROLFINI, Fabiana. **Cibercrime: ataques no Brasil aumentam mais de 300% com a pandemia**. 2020. Disponível em: https://olhardigital.com.br/2020/07/03/seguranca/cibercrime-ataques-no-brasil-aumentam-mais-de-300-com-a-pandemia/. Acesso em: 25 nov. 2021.

ROQUE, Sérgio Marcos. **Criminalidade informática: crimes e criminosos do computador**. São Paulo: ADPESP Cultural, 2007.

VENOSA, Sílvio de Salvo. **Direito Civil: parte geral.** 11. ed. São Paulo: Atlas, 2011.

VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013.

VITAL, Danilo. **Mudança do crime de estelionato no pacote "anticrime" abre divergência no STJ**. 2020. Disponível em: https://www.conjur.com.br/2020-out-21/mudanca-crime-estelionato-gera-divergencia-stj. Acesso em: 28 maio 2021.

XAVIER, Fábio Correa. **Segurança digital: Responsabilidade de todos**. 2021. Disponível em: https://www.tce.sp.gov.br/6524-artigo-seguranca-digital-responsabilidade-todos. Acesso em: 17 nov. 2021.