FACULDADE EVANGÉLICA DE RUBIATABA

CURSO DE DIREITO

DAYANE MACIEL GONÇALVES

O CANTO DA SEREIA – DA CAPTAÇÃO DE VÍTIMAS DE ESTELIONATO VIRTUAL POR MEIO DAS REDES SOCIAIS

RUBIATABA/GO
2021

DAYANE MACIEL GONÇALVES

O CANTO DA SEREIA - DA CAPTAÇÃO DE VÍTIMAS DE ESTELIONATO VIRTUAL POR MEIO DAS REDES SOCIAIS

Monografia apresentado como requisito parcial para a obtenção do título de Bacharel em Direito pela Faculdade Evangélica de Rubiataba, sob orientação da professora Mestra Leidiane de Morais e Silva Mariano.

RUBIATABA/GO
2022

DAYANE MACIEL GONÇALVES

O CANTO DA SEREIA – DA CAPTAÇÃO DE VÍTIMAS DE ESTELIONATO VIRTUAL POR MEIO DAS REDES SOCIAIS

Monografia apresentado como requisito parcial para a obtenção do título de Bacharel em Direito pela Faculdade Evangélica de Rubiataba, sob orientação da professora Mestra Leidiane de Morais e Silva Mariano.

MONOGRAFIA APROVADA PELA BANCA EXAMINADORA EM __ / ___ / ____

Escreva a titulação e o nome completo do seu orientador
Orientador
Professor da Faculdade Evangélica de Rubiataba

Escreva a titulação e o nome completo do Examinador 1
Examinador
Professor da Faculdade Evangélica de Rubiataba

Escreva a titulação e o nome completo do Examinador 2
Examinador
Professor da Faculdade Evangélica de Rubiataba

Dedico esta monografia para toda minha família, amigos e professores, que contribuíram muito com a minha caminhada.

AGRADECIMENTOS

Primeiramente a Deus que me deu a oportunidade de me formar e conseguir realizar este sonho.

Gostaria de agradecer e dedicar esta monografia às seguintes pessoas

Minha família, minha mãe Luceny, meu padrasto Genino, minha vovó Lazara, minha irmã Danyele, meu pai Roberto.

Aos meus tios Lucimar e Luciene.

As minhas amigas Isabella, Daiane Rodrigues, Fabiano e Gabrielle.

Em especial, à minha orientadora Leidiane Morais, que nunca desistiu de mim e me ajudou bastante, por fim, gratidão a todos que me ajudaram a concluir esta faculdade.

RESUMO

O objetivo da monografia em epígrafe é abordar o crime de estelionato virtual, em especial, a variante conhecida como “golpe do amor”, sendo as redes sociais como o principal instrumento de captação de vítimas. E, ainda, emergir políticas preventivas voltadas às vitimas, para reduzir e inibir a prática desse delito. Nesse sentido, foram abordados os aspectos legais dos crimes virtuais, entre outras condutas ainda não tipificadas; flertando com as fraudes empregadas na internet; bem como, analisando os efeitos das alterações inseridas pela Lei 14.155 de 2021, no tipo penal abordado, e as ações de prevenção e punição dos crimes virtuais, especialmente no estelionato sentimental – golpe do amor. A abordagem é qualitativa, com pesquisa sustentada na legislação, em artigos, doutrinas, revistas, e demais fontes de pesquisa disponíveis em meio eletrônico, principalmente aqueles que tratem do tema, e suporte no método dedutivo. Finalizado o estudo, a conclusão é que as práticas de variáveis formas de estelionatos virtuais necessitam de regulamentação jurídica específica, e ações de conscientização e orientação aos usuários das redes sociais, bem como, aplicação efetiva da LGPD, especialmente quanto ao tratamento e o ciclo de vida dos dados coletados nas redes sociais.

Palavras-chave: atração; estelionato virtual; golpe do amor; redes sociais.

ABSTRACT

The purpose of this monograph in question is to address the crime of virtual fraud, in particular, the variant known as "love scam", with social networks as the main instrument for capturing victims. And, still, to emerge preventive policies aimed at victims, to reduce and inhibit the practice of this crime. In this sense, the legal aspects of virtual crimes were addressed, among other conducts not yet typified; flirting with the frauds employed on the internet; as well as, analyzing the effects of the changes inserted by Law 14.155 of 2021, in the criminal type addressed, and the actions for prevention and punishment of cybercrime, especially in the sentimental fraud - the love scam. The approach is qualitative, with research supported by legislation, articles, doctrines, magazines, and other research sources available in electronic media, especially those dealing with the subject, and support in the deductive method. Finishing the study, the conclusion is that the practice of various forms of virtual fraud requires specific legal regulation, and actions to raise awareness and provide guidance to users of social networks, as well as the effective application of the General Data Protection Law, especially regarding the treatment and life cycle of the data collected on social networks.

Keywords: attraction; virtual fraud; love scam; social networks.

Traduzido por Marise de Melo Lemes, licenciada em Letras: Língua Portuguesa/Inglês, pelo Centro Universitário de Anápolis - UniEvangélica – Unidade Ceres-GO.

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AP	Apelação
ART.	Artigo
CAP.	Capítulo
CRFB	Constituição da República Federativa do Brasil
CP	Código Penal
CPP	Código de Processo Penal
INC.	Inciso
LGPD	Lei Geral de Proteção de Dados
N.	Número
P./pag.	Página
STJ	Superior Tribunal de Justiça
STF	Supremo Tribunal Federal

LISTA DE SÍMBOLOS

§ Parágrafo
§§ Parágrafos
@ Arroba

SUMÁRIO

1 INTRODUÇÃO

Em razão das medidas urgentes impostas pela pandemia da Covid-19, a inserção da tecnologia na vida das pessoas foi impreterível, com um aumento exponencial de serviços *home Office*, estudos, eventos, inclusive festas '*online'*, reinventando as relações sociais, transmutando-se para uma realidade virtual. O crescimento do uso de aplicativos de redes sociais, como meio alternativo de manutenção da vida cotidiana favoreceu também o cenário do submundo dos crimes, em especial as práticas de crimes virtuais.

Crimes virtuais, de forma preliminar, se apresentam por meio fraudulento que conduz a vítima a erro. A apuração dessa incursão criminosa é que muitas vezes altera a tipificação legal, a depender do bem que foi atingido. A caracterização do estelionato exige a obtenção de uma vantagem ilícita em detrimento de outra pessoa, uso de meio ardil ou fraudulento de enganar alguém.

O estelionato está previsto no Código Penal desde 1940, e teve um desdobramento em maio de 2021, quando entrou em vigor a Lei n.º 14.155/2021, que acrescentou o art. 154-A, e os parágrafos 2º-A e 2º-B no art. 171 do Código Penal, para punir o chamado estelionato virtual ou fraude eletrônica, majorando a pena quando o ato criminoso é cometido no ambiente virtual, bem como criando tipo penal específico quando existir invasão de dispositivo eletrônico.

Dentre os vários crimes virtuais, o golpe do amor, também conhecido como estelionato sentimental (*scammer* sentimental), ganhou volume durante o isolamento social, onde o estelionatário constrói uma relação afetiva com a vítima para ganhar confiança e, depois, tirar proveito financeiro.

Não obstante o avanço tecnológico e especialmente da internet, a legislação e a estrutura dos órgãos de prevenção e repressão penal, não acompanham seu desenvolvimento, dificultando a apuração e repressão dos criminosos que atuam nesse ambiente virtual. No contexto abordado no presente trabalho, destaca-se o ato de utilizar das redes sociais para atrair, enganar e extorquir as vítimas, entre outros pontos atrativos, o namoro, à promessa de casamento, a exploração da libido, com o intuito e consequente aferimento de vantagem ilícita.

Cabe salientar que o 'golpe do amor' se distingue do "boa noite cinderela", especialmente em razão do multimodos *operandi;* no primeiro caso é formado um vínculo entre o agente criminoso e a vitima, com ações a longo prazo, inclusive se relacionando e

criando vínculo com a família e os amigos da vítima; por outro lado o golpe "boa noite cinderela" é aplicado a curto prazo, com ação imediata no primeiro encontro via de regra.

A temática definida - o canto da sereia[1], a captação de vítimas de estelionato virtual por meio das redes sociais, teve como inspiração no sentido figurado a expressão "o canto da sereia", que significa o discurso ou ação para atrair alguém em regra para uma armadilha[2]. – foi escolhia por analogia ao recurso de sedução para atrair o alvo ao golpe.

E, quando se trata de estelionato, especialmente na modalidade virtual, a atração pelo perfil é uma das ferramentas mais eficientes. Assim, o trabalho aborda as seguintes problemáticas: Os dados coletados nas redes sociais favorecem a captação de alvos em potencial? Quais as medidas preventivas do estelionato virtual voltadas às vitimas para reduzir e inibir a prática desse delito?

Em razão desses problemas, surgem algumas hipóteses: não, os dados coletados nas mídias e redes sociais não possibilitam a captação de vítimas de estelionato virtual; ou, sim, os dados coletados nas mídias e redes sociais possibilitam a captação de vítimas de estelionato virtual; e ainda, o tratamento e ciclo de vida de dados nos termos da LGPD – Lei Geral de Proteção de Dados previne e inibe a prática desse delito.

Nesse sentido, o objetivo geral do trabalho é abordar o crime de estelionato virtual, especialmente na modalidade estelionato sentimental, e de forma específica as redes sociais como instrumento de captação e atração das vítimas.

Ao final do estudo, a conclusão é que a forma mais eficaz são ações de conscientização e orientação aos usuários, bem como, aplicação efetiva da LGPD, especialmente quanto ao tratamento e o ciclo de vida dos dados coletados nas redes sociais.

Trata-se de um estudo de abordagem qualitativa; método de referência é dedutivo, o que oportunizou um panorama do tema que partiu do seu aspecto geral para o particular, e do emprego de pesquisa nas legislações aplicáveis, nos artigos, doutrinas, revistas, e demais fontes de pesquisa disponíveis em meio eletrônico.

A estrutura do trabalho foi distribuída em capítulos e subtítulos. Os capítulos iniciais abordam o avanço da internet e das redes sociais nas comunicações da sociedade, e a sua relevância no contexto mundial; e, o reflexo dessa demanda na prática do estelionato virtual, através do uso de perfil falso nas redes sociais, e o crime de falsa identidade, absorvido por um crime maior.

---

[1] "utiliza-se ainda a expressão "canto da sereia" que designa algo que tem grande poder de atração em que as pessoas caem sem resistência" (RIBEIRO JR., W.A.).

[2] Significado tirado do dicionário Priberam. https://dicionario.priberam.org/canto%20da%20sereia

O trabalho discorre acerca das disposições gerais acerca do estelionato, o ardil do autor e a torpeza da vítima, e as inserções trazidas pela Lei n° 14.155 de 27 de maio de 2021. Na segunda parte da pesquisa, pautam-se acerca da abordagem do uso redes sociais que reverberam na prática do crime de estelionato virtual, especialmente atraídos por perfil falso, e outros estímulos da libido, considerando que no caso de golpes como sedução as vítimas tem uma parcela de participação. E nesse sentido, as considerações finais são voltadas às ações de prevenção aos usuários, à obrigatoriedade de tratamento e estipulação de ciclo de vida dos dados coletados nas redes sociais, conforme determinação legal.

2 ESTELIONATO VIRTUAL

Desde sempre, o ser humano tem necessidade de se relacionar uns com os outros, buscando os mais variados recursos de comunicação. E, durante a pandemia as relações sociais foram reformuladas para uma realidade virtual, que já era ativa, mas que foi expandida em massa. A internet sempre foi um grande aliado na busca pela interação social e o é, nesse momento de isolamento social, o único meio de entrosamento. Contudo, também ampliou o cenário do submundo do crime, e propiciou a expansão das práticas e acesso a alvos em potencial, especialmente por meio das redes sociais.

Nesse sentido, cabe a necessidade de explanar acerca dos crimes virtuais, destacando o ardil do autor e a torpeza da vítima. Abordar o uso a internet e das redes sociais como ferramenta de comunicação e integração social, mas também como cenário para prática de crimes virtuais. Apontar as modificações trazidas pela Lei 14.155/2021, criada com o intuito de combater e inibir as práticas de crimes virtuais.

2.2 Crimes Virtuais

Atuais são as palavras de Pinochet (2014) ao dizer:

> Estamos em uma realidade em que hoje seria impensável viver sem a tecnologia, uma vez que está presente em todos os espaços do nosso desenvolvimento cotidiano comum. A tecnologia está presente em todas as atividades da nossa vida: no lar, nos veículos e nos transportes, em nossos locais de trabalho e de estudo, assim, fazendo parte ativa da revolução digital. Em suma, não se deve esquecer que a tecnologia existe para servir ao homem, para proporcionar uma vida mais fácil e agradável por meio de inovações tecnológicas que a melhore e a simplifique. (PINOCHET, 2014).

O fato é que a internet oportunizou expandir a interação social, independe da sua localização, a alta adesão de internautas em um espaço cibernético, como consequência de desvio à funcionalidade, aflorou os “agressores que atacam as máquinas através de máquinas e iniciaram ataques aos seres humanos reais através das máquinas” (JAISHANKAR, 2010, p. 01)

É necessário compreender essa questão e explorar mais profundamente os perfis e comportamentos criminosos, no intuito de implantar ações para prevenir e reprimir os crimes virtuais, que acarretam danos à sociedade e impactam na segurança a toda e qualquer navegação na rede; especialmente pela vulnerabilidade da maioria dos usuários cibernautas, e a nebulosidade existente no mundo virtual. A incompreensão total da internet e dos recursos

tecnológicos, evidencia que a internet é uma fonte/meio que propicia a criminalidade divergente.

Nesse ponto, aborda-se suscintamente, a composição da internet, considerando a *Surface Web* (a internet na superfície, é onde as páginas indexadas estão disponíveis aos usuários) e a *Deepe Web* (a internet profunda, o conteúdo não é indexado e não pode ser encontrado). O que todos conhecem por internet convencional é a *Surface Web*, ou seja, é o termo utilizado para definir as páginas que podem ser facilmente encontradas, podendo-se localizar uma máquina ou servidor de acesso a partir de uma *Internet Protocol (IP*[3]*).* Já a *Deep Web* é formada por páginas não encontras na *Superface Web;* também conhecida como submundo virtual ou internet secreta, usada para se referir a um conjunto de sites, fóruns e comunidades que não são identificados de forma precisa por navegador, o que em tese, torna impossível o rastreamento do IP do usuário, e uma comunicação segura e privada (ANDRADE, 2015).

Cabe esclarecer, que a *Deep Web* é usada para armazenar conteúdos secretos e de forma sigilosa, sobretudo pelo aumento exponencial de usuários da internet e surgimento de várias empresas especializadas, indivíduos e estruturas governamentais dos países com acesso amplo e irrestrito à rede mundial (ANDRADE, 2015).

O fato é que os crimes materializados na *Supeface web* são cogitados e preparados na *Deep web*, em decorrência dos recursos que ela possibilita, como levantamento dos dados pessoais das vítimas em potencial.

Parte sombria do mundo virtual é chamada de *Deep Web* ou *Dark Web*, onde se encontram informações e materiais proibidos entre outros diversos conteúdos ilegais, como também propicia a prática de falsificações, contrabando, comércio ilegal de armas de fogo, crimes bancários, invasões de privacidade, lavagem de dinheiro, comércio de loterias, tortura real de animais, tráfico, terrorismo, contratação de assassinos, divulgação e contratação de sexo e pornografia, turismo sexual, crimes contra a liberdade sexual, entre tantas outras possibilidades tratadas via sites, chats e/ou fóruns (ANDRADE, 2015; VIGNOLI; MONTEIRO, 2016).

São inúmeros os crimes virtuais, seja de natureza material financeira e contra a honra, contudo, sem abrir a discussão para outras vertentes, mas atendo-se ao tema do presente estudo, tratemos acerca do estelionato.

---

[3] "O IP (ou Internet Protocol) é uma identificação única para cada computador conectado a uma rede. Podemos imaginá-lo como um documento de identificação único, como o CPF, por exemplo. Descobrir este número é bastante fácil e pode ser útil para diversas situações, como veremos neste artigo". (Edivaldo Brito, 2013)

O Código Penal no artigo 171 prevê sete modalidades de estelionato, entretanto o tipo aberto do *caput* concede multimodos *operandi,* a depender do autor do crime, considerando sua criatividade e nível intelectual.

Conforme se extrai do dispositivo legal, o estelionato pode ser praticado mediante artifício, ardil ou qualquer outro meio fraudulento, e nesse sentido ensina Júlio Fabbrini Mirabete:

> (...) o artifício existe quando o agente se utilizar de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos de luz etc. (MIRABETE, 2021, pag. 325).

O artificio, a encenação material mediante uso de objetos ou aparatos aptos a enganar; e, o ardil é a astúcia, a conversa enganosa; e por fim, o silêncio (estelionato por omissão), para manter a vítima em erro. Cabe aqui reafirmar, que tudo isso, tanto pode ser realizado presencialmente ou virtualmente.

Postos no rol dos crimes patrimoniais, o estelionato se caracteriza com a premissa de três elementos: vantagem ilícita, prejuízo alheio e fraude. A fraude nesse sentido é utilizada pelo autor para induzir (criar falsa percepção da realidade) ou manter (aproveitamento o engano espontâneo) a vítima em erro.

Não é novidade o uso da internet para práticas de crimes virtuais, o que chamou a atenção foi o aumento de usuários da internet, e a deliberada aceitação e adesão aos recursos tecnológicos, não apenas para comunicação usual, como também para trabalho, estudo, e relacionamentos amorosos. Obviamente relacionado, e digo até uma consequência, da pandemia pela COVID-19, que obrigou e propiciou o cenário e a integração nas redes sociais.

2.2 Estelionato Sentimental – Golpe do Amor

Como visto no crime de estelionato, a conduta típica é induzir a vítima ao erro, por meio de artifícios para alcançar seu objetivo, que é obter vantagem ilícita para si ou para outrem. Considera-se um crime patrimonial, onde não há uso de violência ou grave ameaça, mas, sim, de meios fraudulentos para obtenção da vantagem ilícita, especialmente financeira.

O golpe do amor, também conhecido como estelionato sentimental (*scammer* sentimental), ganhou volume durante o isolamento social, onde o estelionatário constrói uma relação afetiva com a vítima para ganhar confiança e, depois, tirar proveito financeiro.

S*cammer* é uma palavra de origem inglesa e descreve o conjunto de golpistas virtuais inseridos em grupos organizados por intermédio da internet, com o objetivo de enganar e extorquir suas vítimas (FILHO; KHALIL, 2021).

Apura-se que o alvo predominante são mulheres, especialmente aquelas com um nível de carência afetivo abalado, com recurso ao convencimento e acalentamento através de conversas. Cabe ressaltar que o contato iniciado não se limita a conversas promíscuas ou de conteúdo meramente sexual e/ou pornográfico, mas, primeiramente, trabalham a questão emocional e identificam o estado frágil das vítimas para, ao final, aplicar um golpe financeiro; por meio da confiança alheia de forma intencional para obter vantagem, inclusive dos familiares e amigos da vítima.

O objetivo do golpe do amor é obter vantagem financeira por meio da afeição e atenção dedicada, de até promessa de casamento ou namoro, auferindo vantagem ilícita em prejuízo da vítima; agem de forma atenciosa, sendo certo que o relacionamento pode se estender até meses para que se estabeleçam laços de confiança. O idealizador consegue convencer sua vítima a lhe doar dinheiro, presentes, e até mesmo *criptomoedas*, que é principal ‘moeda’ na *Deep Web.*

Cabe dizer que a boa-fé objetiva, conduta leal e correta esperada nas negociações comerciais, também se esperam nos relacionamentos estabelecidos no ambiente virtual; e a garantia é reforçada pelas trocas de narrativas e fotos, geralmente *fakes*, o que faz com que as vítimas, em fragilidade emocional, acabam desenvolvendo confiança e laços afetivos.

Para Robert Greene (2004) em “A arte da sedução”, “As pessoas estão morrendo de vontade de ser conquistadas, de abandonar a sua costumeira teimosia. Quem entra em suas vidas oferecendo aventura e prazer é irresistível. Os sedutores sabem que a possibilidade de prazer fará uma pessoa segui-los, e que a experiência desse prazer fará com que ela se abra, suscetível ao toque”.

E, a partir desse comentário, aborda-se uma questão a possibilidade da caracterização do estelionato quando a vítima, inconscientemente e/ou involuntariamente, também age de ‘má-fé’, pretendendo obter uma ‘vantagem indevida’. Nessa hipótese, a doutrina denomina de Torpeza Bilateral, ou seja, quando há uma fraude recíproca, seja em prejuízo da outra parte ou não.

Os posicionamentos se dividem na corrente seguida por Nelson Hungria, a qual defende que não há crime quando a vítima não está de boa-fé, pois a lei não pode amparar a má-fé da vítima. Por outro lado, a corrente majoritária, defendida por Fernando Capez, diz que a boa-fé não constitui elemento subjetivo do tipo, sendo que o dolo do agente não guarda

dependência com a intenção da vítima, restando caracterizado o estelionato; , devendo ser punido o sujeito ativo e, se for ocaso, também a vítima, quando praticada a conduta ilícita; “não há possibilidade de compensação de condutas no direito penal” (CAPEZ, 2020).

Quanto ao aspecto formal, segundo Rogério Greco (2018, p. 198) crime seria toda conduta que atentasse ou que colidisse com a lei penal editada pelo Estado, enquanto o conceito material do crime seria considerado toda conduta que viola os bens jurídicos mais importantes.

Nesse sentido, o Direito Penal encontra inúmeras dificuldades para se adequar ao avanço tecnológico, principalmente em relação à internet como instrumento de captação de vítimas.

Com um *scammer* age conforme dispõe Ludgero (2020):

> O "scam romance" (também conhecido como "Catfish") é quando o criminoso estabelece um relacionamento com a vítima. Ele também pode ser chamado de "Golpe da Nigéria", por ser comumente praticado por pessoas desse país onde o governo não tem como rastrear os criminosos. Após aplicar os golpes, os pretendentes desaparecem e criam novos perfis, aplicando novos golpes em outras vítimas.

A fundamentação legal do crime de estelionato na internet não está precisamente tipificada na legislação brasileira, por essa razão se aplica o artigo 171 do Código Penal de forma análoga, inclusive o estelionato sentimental.

Quanto à autoria no estelionato virtual, Biasoli (2010) afirma que:

> Uma problemática que envolve o estelionato praticado na Internet diz respeito o da autoria, ou seja, a identificação do autor desta infração penal. Estando este criminoso muito mais protegido por trás de uma rede virtual do que o próprio estelionatário comum, ou seja, aquele que se expõe.

O cenário perfeito seria que o estelionato praticado na internet fosse tipificado em instrumento normativo específico, que proporcionaria uma proteção mais eficaz ao cidadão, além de possibilitar a punição dos agentes causadores dos danos.

Importa salientar, a legislação que regulamenta os crimes cibernéticos não é suficiente para abranger todas as condutas irregulares praticadas no mundo virtual. A ausência de lei específica beneficia as condutas reprovadas, lembrando que várias dessas condutas podem ser consideradas atípicas, o que resulta na não punição do sujeito, por falta de tipicidade e do princípio da reserva legal e da legalidade vigorante no direito penal (ALVES, 2018).

Como dizem a internet é um mundo sem fronteiras, está disponível no mundo todo, e através dela se torna mais fácil o encontro da vítima com criminoso, que propicia a falsa

identidade, e no caso do estelionato sentimental, o grau de facilidade é imenso, se for comparado ao crime de estelionato comum. Através das redes sociais, especialmente aquelas de relacionamentos, é possível adquirir confiança por parte da vítima, e consequentemente o criminoso, pode usufruir de filtros, avatares e criptografia, uma comunicação direta, e atingir seu objetivo, podendo o agente se passar por quem entender conveniente, conforme o perfil de cada vítima.

Como dito anteriormente, a boa fé é um comportamento que perdura em todas as relações sociais, transações financeiras, negócios empresariais, mas no caso do estelionato sentimental é ardiloso e falso do lado do idealizador do crime, contudo a vítima acredita e demonstra evidente existência de sentimento e relacionamento estável, com a finalidade de formação familiar.

Brenoff (2017) destaca que os *scammers* são indivíduos que usam perfis falsos na internet, usam perfis falsos em sites de namoro e redes sociais, com fotos de homens ou mulheres atraentes para despertar e alimentar paixões à distância, também utilizam informações como ser estrangeiro, financeiramente estável, um drama familiar que demonstra carência e desejo de ser amado, tudo para ser um perfil ardilosamente atrativo para ‘fisgar’ sua ‘presa’; visando o locupletamento ilícito ao ‘capturar’ suas vítimas, que acreditam na relação desenvolvida e no sentimento declarado, que prometem amor e casamento, algo que, para a vítima, constitui um relacionamento real.

O que ocorre é que a pessoa se encanta pelo perfil, se apaixona e confia no sentimento construindo e em todo o contexto fático que o *scammer* lhe repassa, o golpe do estelionato sentimental se concretiza com a remessa de quantias de dinheiro para o estelionatário, as vezes continuamente a longo prazo.

E, conforme Ann Brenoff salienta, além dos prejuízos financeiros, as vítimas saem com graves feridas psicológicas e se sentem deploravelmente envergonhadas (BENOFF, 2017).

Ainda não há um levantamento exato, mas presume-se que as vítimas são inúmeras, porém, o medo e a vergonha as impedem de denunciar ou, até mesmo, de falar com a família e tão pouco em público sobre o ocorrido, permanecendo no anonimato. O que descarta a possibilidade de reembolso do prejuízo financeiro e impede a divulgação dos perfis falsos que podem ser reutilizados para cativar novas vítimas.

Nesse sentido, evidente a vulnerabilidade da vítima usuária da internet em razão da boa-fé e expectativas dispensadas ao *scammer* sem a cautela necessária exigida no ambiente virtual, e após a consumação do crime, a vergonha e/ou a reprovação social. A estrutura de

controle e repressão estatal deve oferecer além da repressão qualificada, o apoio moral e psicológico para que a vítima necessitada ante os graves prejuízos sofridos.

Por fim, cabe lembrar, que os *scammers* são punidos pela prática delitiva do crime capitulado no artigo 171 do Código Penal Brasileiro. Contudo, as ações de prevenção devem também possuir caráter pedagógico e indicar medidas de proteção e, em caso de concretização do delito, o procedimento a ser seguido pela vítima junto aos órgãos responsáveis. Os crimes virtuais necessitam de um aparato legislativo específico, especialmente o estelionato sentimental praticado por *scammers* na internet, também em razão e favor das vítimas não identificadas, que saem lesadas desse ato e sem punição do agente causador.

2.3 As alterações inseridas pela Lei nº 14.155, de 27 de Maio de 2021.

O Código Penal dispõe no artigo 171 acerca do crime de estelionato, teve uma considerável alteração, ou melhor, um acréscimo, com a Lei n° 14.155, de 27 de maio de 2021, dentre as alterações destacam-se os §§ 2°-A e 2°-B, que tratam da 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 (BRASIL, 2021).

A inserção do § 2°-A atribuiu uma qualificadora ao crime de estelionato, quando este é praticado de forma não presencial, na situação em que o agente se utiliza de informações constantes de redes sociais, contatos telefônicos, e envio de e-mail a vítima. E, ainda, o dispositivo legal abre a possibilidade da prática do crime de estelionato virtual por qualquer outro meio fraudulento análogo.

Já o §2°-B inseriu o aumento de pena de 1/3 a 2/3, quando o crime é praticado mediante a utilização de servidor estrangeiro, ou seja, a pena deve ser maior, considerando a relevância do resultado gravoso para dosar a fração de aumento, tendo em vista que há uma grande dificuldade de localização e punição do agente, quando o crime é cometido a partir de um servidor ou equipamento localizado fora do território brasileiro.

Cabe destacar o §4° do artigo 171 também foi inserido pela lei n°14.155/2021, com a seguinte redação: “§ 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" (BRASIL, 2021). Nesse caso, a redação anterior do referido dispositivo legal previa a aplicação de pena em dobro, no caso de estelionato praticado contra idoso (pessoa com idade igual ou superior a 60 anos). Assim, em relação ao crime cometido contra o idoso é mais favorável ao agente, visto que a fração a ser aplicada obedecerá ao critério da gravidade do resultado, em contrapartida ao texto anterior, no qual, em qualquer caso, a fração de aumento de pena seria o dobro.

Nesse sentido, a alteração da lei poderá retroagir em benefício do acusado ou condenado, anteriormente à alteração do referido dispositivo legal, a conduta do agente para a prática do crime de estelionato não tenha sido de grande relevância.

Tratando-se de crimes cometidos contra vulnerável, haverá o mesmo aumento de pena para o agente, ou seja, de 1/3 até o dobro. O juiz, ao fixar a pena base, deverá observar o critério da relevância do resultado.

Cumpre salientar, que não há uma definição legal do termo "vulnerável" quando se trata estelionato cometido mediante fraude, assim deve ser utilizado o conceito trazido pelo artigo 217-A, §1°, do Código Penal, que dispõe o seguinte:

> Artigo 217-A § 1° - Incorre na mesma pena quem pratica as ações descritas no caput com alguém que, por enfermidade ou deficiência mental, não tem o necessário discernimento para a prática do ato, ou que, por qualquer outra causa, não pode oferecer resistência (BRASIL, 2021).

Há de ser feita uma interpretação sistemática e, para que seja compreendida como vulnerável, a vítima deve sofrer de enfermidade, ou algum tipo de deficiência mental, que retire ou diminua o discernimento para a realização de seus atos. A Lei 13.964/2019 (Pacote Anticrime) também modificou a natureza da ação penal no crime de estelionato, incluindo o § 5º no artigo 171, com a seguinte redação:

> § 5º Somente se procede mediante representação, salvo se a vítima for: I - a Administração Pública, direta ou indireta; II - criança ou adolescente; III - pessoa com deficiência mental; ou IV - maior de 70 (setenta) anos de idade ou incapaz (BRASIL, 2019).

A ação penal seria, em regra, pública incondicionada, sendo ressalvadas as exceções trazidas no artigo 182 do Código Penal. A partir da supracitada alteração, tem-se a representação como condição de procedibilidade para instauração da ação penal, ressalvadas as hipóteses dos incisos I a IV.

Dentre as alterações a Lei n°14.155/2021 modificou também o artigo 70 do Código de Processo Penal, tratando da competência para o julgamento de algumas das modalidades do crime de estelionato, o §4° do referido artigo foi incluído com a seguinte redação:

> § 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 (BRASIL, 2021).

Assim, o critério para definir a competência se tornou o domicílio da vítima, sendo a competência determinada pela prevenção em caso de pluralidade de vítimas. Entretanto, em caso de estelionato mediante falsificação de cheque, a competência para processamento e julgamento do crime será do juízo do local da obtenção da vantagem ilícita, conforme dispõe a sumula 48 do STJ.

Assim, com as alterações inseridas pela Lei n° 14.155/2021, acrescentou outros parágrafos ao artigo 171, do Código Penal, e também algumas regras de competência para o julgamento, sendo possível fazer um panorama sobre o crime de estelionato; restando demonstrado que a prática do estelionato virtual tem sido muito frequente e, em razão da pandemia do Covid-19, o número de vítimas elevou consideravelmente. A reforma trazida pela supramencionada Lei, foi de essencial no combate a crimes virtuais, mas ainda não produz eficiência e expressivos resultados.

3 DA ABORDAGEM DE CAPTAÇÃO DE VÍTIMAS DE ESTELIONATO POR MEIO DAS REDES SOCIAIS

Nesse capítulo, discorre-se acerca do alcance e uso das redes sociais, a internet como instrumento de comunicação da sociedade atual, a sua importância no contexto mundial, mas também a sua relação com os crimes virtuais.

As pessoas possuem a necessidade de se relacionarem uns com os outros. E viver em sociedade é uma característica comum a cada pessoa; diante disso, o homem sempre procurou formas de interagir com o próximo, buscando os mais diversos meios de comunicação. E, a internet sempre foi um grande aliado na busca pela interação social; e através das redes sociais, essa ferramenta revolucionou a comunicação e a forma de convivência da sociedade.

3.1 Do Uso das Redes Sociais como Instrumento de Captação

Oportuno dizer que o termo “rede social” refere-se a uma plataforma digital, onde a pessoa cria uma identidade virtual, com a finalidade de interagir com outras pessoas. O processo de criação do perfil virtual é rápido e prático, e possibilita que o usuário insira informações a seu respeito, que poderão ser compartilhadas com outros usuários.

A maioria dessas plataformas é inspirada no perfil virtual, onde os usuários possam publicar e compartilhar informações, mensagens, fotos, vídeos, e interagir com as publicações de outros usuários, podendo estabelecer diálogos e transações.

O estudo realizado pelo “We Are Social e Hootsuite” apresentou o relatório Digital 2021, inclusive com um panorama sobre as redes sociais mais usadas no Brasil. A pesquisa realizada em janeiro de 2021, apontou que existem cerca de 150 milhões de usuários de redes sociais no Brasil, o que corresponde a 70,3% da população do país. Entre as redes mais utilizadas no Brasil estão Youtube, WhatsApp, Twitter, Facebook e Instagram (WE ARE SOCIAL E HOOTSUITE - DIGITAL 2021).

As redes sociais estão presentes em todo o país e no mundo, interligando as pessoas e diminuindo as distâncias, criando lações e relações entre povos e culturas.

Ocorre que tem sido também muito comum à criação de perfis que não condizem com a verdadeira identidade da pessoa usuária, com informações que dizem respeito à outra pessoal real ou até fictícia.

3.1.1 *Dos Perfis Falsos*

Cumpre destacar que a criação de um perfil falso referente a uma pessoa inexistente não configura um crime necessariamente. Isso se justifica, pelo fato de que muitos internautas criam perfis falsos com o fim de buscar o anonimato, passando-se por uma pessoa fictícia, ao se relacionar e estabelecer diálogos inofensivos com um terceiro.

Os indivíduos escolhem imagens de pessoas desconhecidas, para atribuí-las ao seu perfil falso. Inclusive, existem sites que tem a finalidade de ofertar fotos nesse sentido, com pessoas que disponibilizaram o uso de sua imagem para esse fim. Tal prática não é crime, estando o criador sujeito a infringir apenas alguma regra dos Termos de Serviço da rede social. Evidentemente, identificado abuso ou uso indevido de imagens ou informações, será punido com a exclusão da conta.

Deve-se ressaltar que, ainda que o perfil falso criado seja referente a uma pessoa que não exista, um animal ou um objeto, é possível que haja responsabilização dos criadores, visto que, em alguns casos, a conduta se adequa a outros delitos previstos na legislação penal.

Por outro lado, a criação de um perfil referente a uma pessoa real, viva ou falecida, pode ser adequada ao crime de falsa identidade previsto no artigo 307, do Código Penal, com a seguinte redação: “Art. 307 - Atribuir-se ou atribuir a terceiro, falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem: Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave”.

Nesse caso, o dispositivo traz a possibilidade de elementos que tornam criminosa a conduta. E, para tanto, é necessário estabelecer o conceito de identidade, que, segundo Nelson Hungria (1958), é:

> [...] o conjunto de caracteres próprios de uma pessoa, que permite identificá-la e distingui-la das demais, a exemplo do nome, idade, profissão, sexo, estado civil etc. A lei pune a auto atribuição falsa, ou a atribuição falsa a terceiro, isto é, o agente se identifica incorretamente, com dados que não lhe são próprios, ou atuam, da mesma forma, atribuindo esses dados falsos a terceira pessoa (HUNGRIA, 1958).

A identidade se refere à qualificação do indivíduo, de modo a distingui-lo dos demais, sendo que é reprovável a conduta do agente que atribui a si mesmo uma qualificação que não lhe pertence.

E, quanto ao crime de falsa identidade, Fernando Capez (2020) ensina que, para a sua configuração, “exige-se também o chamado elemento subjetivo do tipo, consistente no fim especial de obter vantagem, em proveito próprio ou alheio, ou de causar dano a outrem”.

Assim, faz-se necessário a comprovação de que há dolo na conduta, com a intenção de obter vantagem ou causar dano a alguém, quando da criação do perfil falso na internet.

Há de se considerar o fato de que há um enorme número de usuários que cria perfis falsos ou, até mesmo, perfis de artistas, por ter um apreço por tais pessoas. O direito civil brasileiro prevê uma proteção à imagem de cada indivíduo, de forma com que cada atitude pode ter uma implicação, seja em âmbito penal ou civil.

Conforme ensina Fernando Capez: “Consuma-se o crime com o ato de atribuir-se ou atribuir a outrem falsa identidade. Trata-se de crime formal, de maneira que o delito se perfaz independentemente da obtenção da vantagem ou da produção de dano à terceiro” (CAPEZ, 2020, s.p.).

Ludgero (2020) destacou:

> O número de esquemas tem crescido tanto que o Instagram, em novembro de 2018, se posicionou contra os perfis criminosos. O ambiente online acaba facilitando ações ilegais, por conta da dificuldade de rastrear o criminoso e a falta de informação dos internautas de como denunciar. Esses perfis são mais difíceis de identificar que do um Fake comum, pois eles agem como se fossem reais — postam fotos, legendas, Stories e informações que conferem legitimidade para o perfil, que pode ser pessoal ou institucional. Estima-se que o Instagram pode ter até 95 milhões de perfis falsos.

Assim, se a pessoa cria uma rede social, com intuito de obter alguma vantagem ou causar dano a alguém, responde pelo crime de falsa identidade, não sendo necessário que a vantagem seja alcançada ou o dano concretizado, pois se trata de crime formal.

Esse crime pode ser absorvido por um delito mais grave, a depender da conduta do agente, conforme ensina Nelson Hungria (1958), “a vantagem pretendida pelo agente não poderá ter natureza econômica, pois, se assim fosse, tal conduta seria tipificada como estelionato, delito previsto no artigo 171, do Código Penal”.

Por outro lado, caso o agente incorpore a personalidade de outra pessoa, agindo como se ela fosse, por meio de uma rede social, inserindo declaração falsa ou diversa da que devia ser escrita, com a finalidade de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante, essa conduta será considerada crime de falsidade ideológica.

Nesse prisma, como já salientado, a criação de perfil falso em uma rede social não é necessariamente considerada crime, sendo preciso verificar a real intenção de obter algum proveito com essa conduta. Podendo o indivíduo buscar o anonimato, a fim de estabelecer diálogo com outros usuários ou, simplesmente, por apreço a uma figura pública. Ademais,

quando a conduta se adequar ao crime de falsa identidade, esse delito pode ser absorvido por um crime mais grave.

3.2 Repercussão de alguns casos noticiados

O golpe do amor – estelionato sentimental ganhou volume na pandemia por meio das redes sociais, mas ele já era praticado também presencialmente, a expansão do uso dos ambientes virtuais só propiciou o alcance de vítimas, especialmente em razão da maior carência manifestada no isolamento social.

Cabe abordar alguns casos de repercussão nacional divulgados pela mídia.

3.2.1 *"Belas, Sedutoras e Perigosas"* (FISCHER, 2016).

A TV Globo apresentou no programa Conexão Repórter em junho 2016, um documentário apresentado pelo repórter Roberto Cabrini, que mostrou a intrigante história de três mulheres que usavam de seus atributos para enganar pessoas e aplicar golpes.

As mulheres consideradas belas e sedutoras, na reportagem, destacaram algumas características marcantes: rosto delicado, corpo escultural, conversa envolvente, poder de atração arrebatador; conhecida como ‘Barbie do crime’. Entre as entrevistadas uma promovia encontros secretos para negociar acertos fraudulentos e subornos; outra foi acusada de enganar, mentir, falsificar, extorquir, inventar doenças e de se passarem por representantes de organizações humanitárias; e outra, de sequestro, latrocínio, extorsão, ocultação de cadáver e formação de quadrilha.

3.2.2 *“Mulheres Bonitas eram Usadas por Quadrilha para Golpes em Prefeituras”* (NETO; LACERDA. 2013)

Em 2013, o programa do Fantástico, transmitido na TV Globo, e replicado no portal do g1, noticiou o golpe aplicado em fundos de pensão de prefeitura, onde mulheres bonitas convenciam os prefeitos a ‘aplicar’ o dinheiro dos fundos de pensão. A quadrilha tinha uma vida de luxo; carros, lanchas; e montava empresas de fachada para lavar dinheiro; movimentando cerca de R$300.000.000,00 (trezentos milhões de reais) em um ano em meio.

Na investigação, foram presas 22 pessoas, entre elas quatro mulheres, consideradas fundamentais na ação criminosa, elas eram chamadas de “pastinhas”, usadas para aliciar os

prefeitos e convencê-los de usar o dinheiro de fundos de pensão em investimentos criados para dar prejuízo, e em trocas eles receberiam propinas.

Na reportagem uma das abordadas, conta que “foi criado um sensacionalismo em cima das meninas que eram contratadas. Foram quatro meninas que trabalhavam, todas bonitas, bem apessoadas”. E ressalta que a beleza facilitava o contato dessas com os prefeitos, mas que nessas reuniões só apresentavam propostas de investimentos financeiros da empresa comandada pelo doleiro preso.

3.2.3 *“Brasileira acha que namora músico grego e perde R$880 mil”* (SÓTER. 2021).

Em dezembro 2021, o Correio Braziliense noticiou um golpe que resultou em um prejuízo de R$880.000,00 (oitocentos e oitenta mil reais) para uma mulher brasileira de 59 anos de idade, que conheceu um estelionatário pelas redes sociais. Acreditava que namorava um músico grego, até combinou casamento com suposto *affair*. O fato se tornou de conhecimento público após ter ‘viralizado’ uma história de um italiano que pensava namorar Alessandra Ambrósio.

Evidente que a historia que envolvia uma pessoa ‘famosa’ nacional e internacionalmente chamou atenção para casos de anônimos que sofreram inúmeras situações até mais prejudiciais.

A denúncia do Ministério Público do Estado de São Paulo, acusou um homem nigeriano de se apropriar de cerca de R$880 mil reais, que se passava pelo músico grego Yanni; o “Yanni fake” através das redes sociais iniciou um ‘relacionamento’ com a vítima, comprometeram-se em casar, e a brasileira efetuou inúmeras transferências bancárias para o homem, que na verdade morava no Brasil.

Cabe destacar que não foi a vítima que noticiou o fato à polícia, pois acreditava no relacionamento, e foi pedir R$10.000.000,00 (dez milhões de reais) à sua família para pagamente de um suposto resgate de seu amado. E, a partir daí a família noticiou o fato à polícia que iniciou as investigações.

A matéria informou que, segundo Ministério Público, o individuo fazia parte de uma quadrilha internacional conhecida como “Yahoo Boys” e tem mais de 200 membros no Brasil; e que esse grupo é especializado em praticar o assim chamado estelionato sentimental.

Na reportagem, também foi destacado que a polícia já contabilizou mais de 400 vítimas em todo o país, isso considerando os casos informados/noticiados por meio dos

registros de ocorrências, ou seja, a estimativa real é bem superior; e que a captação das vítimas se dá por meio de perfis falsos nas redes sociais.

3.2.4 *"Italiano cai em golpe e passa 15 anos achando que namorava Alessandra Ambrósio"* (Redação – Isto é Gente. 2021)

Recentemente, viralizou nas mídias televisionadas, virtuais e impressas, a inconcebível história do jogador de vôlei italiano, Roberto Cazzaniga, que acreditou namorar uma modelo brasileira por quase 15 anos. As informações do jornal O Globo e replicada pelos sites da revista *Isto é Gente*, *Extra e Correio Brasiliense* entre outros sites de noticia (2021).

A vítima informou que foi enganado após conhecer uma pessoa pela internet que usava fotos da modelo Alessandra Ambrósio, mas se identificava como Maya, e após vários anos de farsa, a família do jogador e jornalistas reuniram provas para revelar o golpe milionário que ele havia caído.

Que no curso do 'relacionamento', o jogador italiano já havia entregado à 'namorada' cerca de 700 mil euros (R$4,3 milhões de reais), para custear supostos tratamentos cardíacos que ela necessitava.

Assim, como nos demais casos, o convencimento da vítima era tanto que o golpe só foi revelado pela intervenção da família que, desconfiados dos altos valores envolvidos nas transações financeiras, e com a ajuda de jornalistas reuniram provas para convencê-lo de que estava sendo enganado.

3.3 A Lei nº 13.709/2018 – LGPD como Instrumento de Prevenção às Práticas de Estelionato Virtual

A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A internet acompanhou o fenômeno da globalização e cresce o número de usuários adeptos; proporcionando a interação de pessoas de diferentes lugares, bem como, compartilhamentos de informações, sendo, também, uma grande ferramenta para fomentar o comércio. E, como dito, atrai também a atenção dos criminosos, que usam dos meios tecnológicos para a prática de crimes; onde usam a internet para coletar informações e dados

de indivíduos que serão suas possíveis vítimas; salientando que no mundo inteiro, pessoas compartilham e guardam suas informações digitalmente.

A LGPD (Lei 13.709/18) faz o Brasil fazer parte dos 120 países que contam com uma regulamentação específica para proteção de dados pessoais. A LGDP teve como influência o GDPR (General Data Protection Regulation), que entrou em vigor em 25 de maio de 2018 e regulamenta esta questão para os países da Área Econômica Europeia (AEE). O GDPR é a legislação mais relevante sobre privacidade de dados e passou a servir de base para muitos outros países criarem as suas leis relacionadas a este tema (PINHEIRO, 2020).

Aos olhos da LGPD, todo e qualquer dado pessoal deve ser protegido, independentemente do meio pelo qual o mesmo seja obtido ou processado. Isto significa que os dados obtidos e/ou processados de forma manual ou mecânica também estão sujeitos à mesma regulamentação. Por exemplo: quando você entra em um restaurante, e se conecta ao *wifi* gratuito do mesmo, mediante fornecimento de usuário e senha de um serviço de rede social, como Facebook, Google, etc., está fornecendo dados pessoais ao restaurante, que deve ser responsável pelo tratamento dos mesmos, nos termos da lei.

A lei busca um equilíbrio entre os novos modelos de negócio, baseados no uso de dados pessoais e a proteção à privacidade. Esse valor cada vez mais alto na pauta dos cidadãos a partir da divulgação de casos de uso indevido de tais informações.

A LGPD dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, inclusive por meio digital.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
> (...)
> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2019)

E nesse sentido, de acordo com LGPD o compartilhamento dos dados deve ser consentido pelos seus titulares, bem como, as informações devem ser eliminados após o término do seu tratamento. O que proporciona maior segurança quanto ao uso dos dados fornecidos aos contratantes.

Mesmo tendo toda a preocupação do mundo em proteger dados pessoais e estando em absoluta *compliance* com a LGPD, a empresa seguirá tendo riscos de que possa haver um vazamento de dados, ou um incidente específico com algum dado de titular. Se isto acontecer, a empresa deve estar preparada para conter o vazamento, reagir de forma a tratar de solucionar as causas, e comunicar aos titulares de dados e à Autoridade Nacional de Proteção de Dados sobre o ocorrido.

Como já mencionado os golpes na internet crescem de maneira exponencial, principalmente com o estado de calamidade causado pela pandemia do COVID 19. O universo virtual já fazia parte do cotidiano de muitas pessoas, mas, uma parcela considerável da população ainda tinha aversão à tecnologia. No entanto, as medidas de afastamento os obrigaram às adaptações, de todas as formas: uso de máscaras, comprar pela *internet*, pagar uma conta pelo aplicativo do banco e até mesmo a realizar consultas por videoconferência, recebendo a receita do remédio via e-mail e já enviando à farmácia, sem nem mesmo ter que sair de casa para receber os medicamentos.

Diariamente, as pessoas negociam objetos e serviços, cadastram senhas, fornecem dados, trocam mensagens, participam de grupos, acessam redes sociais e se utilizam de vários meios que, de alguma forma, armazenam suas informações pessoais. As inúmeras formas de utilização da internet podem parecer inofensivas, mas também oferecem riscos aos usuários, quando ‘caem’ nas graças de pessoas mal-intencionadas.

Com a acessibilidade aos serviços rotineiros (contas bancárias, entidades governamentais e prestadoras de serviços), sem ter que sair de casa, tem sido bastante comum e propicia a prática de crimes virtuais. Nessas condutas criminosas, os agentes invadem os dispositivos eletrônicos com o fim de obter dados pessoais da vítima como números de CPF, cartão de crédito e senhas, utilizando-se de links, mensagens e anúncios atrativos, que levam ao acesso de páginas falsas, mas que levam às ações fraudulentas.

Assim, a LGPD ao disciplinar a proteção de dados pessoais (meio físico e virtual) visou alcançar respaldo para todo cidadão que carece de transmitir seus dados a quem quer que seja. Pois, o que leva o criminoso a conseguir sucesso em ação, é o fato de estar em posse das informações pessoais da vítima, e ao entrar em contato, obter vantagem e convence-la de que se trata de pessoa idônea.

Abordamos alguns casos nesse capítulo, contudo, muitos outros brasileiros, são vítimas diárias de golpes. Apenas uma pequena ilustração diante das inúmeras acusações de cibercrime, e a maioria desses crimes começam com o acesso e utilização ilegal aos bancos de dados pessoais de empresas, de redes sociais, de cadastros públicos.

O Brasil está entre os países com mais ataques de *phishing* (mensagens fraudulentas) do mundo, segundo um levantamento feito pela companhia de segurança digital Kaspersky (VELASCO e MANCINI, 2022). Nesse sentido, ainda carece de mais ações e medidas de proteção aos usuários, além do dever de cautela e cuidados essenciais.

Embora a LGPD não incidir para atividades de investigação e repressão de infrações penais, a lei impõe que as empresas responsáveis por tratar dados pessoais deverão possuir boas práticas de governança e cultura em proteção de dados, inibindo que os dados pessoais sejam acessados por terceiros não autorizados e/ou com más intenções.

A princípio houve uma resistência das empresas e órgãos para adequação de seus sistemas, arguindo as despesas que essa formatação imposta pela LGPD acarretariam, contudo, é evidente que as sanções, em decorrência do seu descumprimento, como multas e indenizações, podem ser mais problemáticos e o prejuízo maior. Assim se as boas práticas de tratamento de dados já eram recomendadas antes da entrada em vigor da LGPC, atualmente é uma exigência que deve ser cobrada pelos próprios consumidores, e fiscalizada pelas autoridades competentes.

CONSIDERAÇÕES FINAIS

O debate acerca da interação entre a legislação brasileira e a internet, ainda exige muito aprofundamento legal, especialmente quando consideramos o grande volume de Fakes, os perfis falsos da internet.

Como destacamos no tema abordado nesse trabalho, um dos principais objetivos com a conta de perfil falso é sustentar uma prática de *catfish*, em que alguém cria um perfil com o objetivo de namorar *online*. Alguns ficam meses ou até mesmo anos acreditando que estão em um relacionamento com a pessoa que veem nas fotos, quando, na verdade, estão sendo vítimas de um golpe.

Depois de ganhar sua confiança, o indivíduo começa a pedir dinheiro ou presentes para o seu namorado virtual e, em outros, apenas mantém um relacionamento à distância encoberto por mentiras e desculpas.

O isolamento social favoreceu os golpes na internet, como exemplo, clonagem de WhatsApp e redes sociais; uso indevido de imagens de terceiros em perfis falsos, etc. Em razão da disponibilidade de dados pessoais disponíveis na internet e/ou decorrentes de vazamentos de ataques às bases de dados de empresas e instituições.

As recentes alterações na legislação penal quanto à tipificação do estelionato por meio virtual, e a implantação de legislação específica de proteção de dados, ampliou a possibilidade de prevenção e punição. Mas, ainda é um pequeno passo num vasto universo; e cada caso deve ser analisado, mas de forma geral, as vítimas de estelionato sentimental podem, no mínimo, solicitar reparação por Danos Materiais e Morais, se tiverem tido sua dignidade prejudicada de alguma forma por conta das ações de quem estava por trás do *Fake*.

REFERÊNCIAS

ANDRADE, Leonardo. **Cybercrimes na deep web: as dificuldades de determinação de autoria nos crimes virtuais.** 2015. Disponível em: <https://jus.com.br/artigos/39754/cybercrimes-na-deep-web-as-dificuldades-juridicasde-determinacao-de-autoria-nos-crimes-virtuais/2>. Acesso em: fevereiro de 2022.

ANDREUCCI, Ricardo Antonio. **Manual de Direito Penal**. 10 ed. São Paulo: Saraiva, 2014.

ALVES, Maria Hionara dos Santos. **A evolução dos crimes cibernéticos e o companhamento das leis específicas no Brasil**. 2018. Disponível em: <https://jus.com.br/artigos/64854/a-evolucao-dos-crimes-ciberneticos-e-oacompanhamento-das-leis-especificas-no-brasil>. Acesso em: janeiro de 2022.

ATAIDE, Amanda Albuquerque. **Crimes Virtuais: Uma Análise Da Impunidade E Dos Danos Causados Às Vítimas**. Disponível em: <http://www.faaiesa.edu.br/aluno/arquivos/tcc/tcc_amanda_ataide.pdf>. Acesso em 23/10/2021.

BIASOLI, Luiz Carlos de Sales. **Da necessidade de tipificação do crime de estelionato praticado na internet**. 2010. Disponível em: <http://www.conteudojuridico.com.br/?Artigos& ver=1055.25896&seo=1>. Acesso em: março de 2022.

BLUM, Renato Opice. **LGPD – Lei Geral de Proteção de Dados - Comentada**. São Paulo: Revista dos Tribunais, 2019.

BLUM, Renato Opice. **Data Protection Officer (Encarregado).** São Paulo: Revista dos Tribunais, 2020.

BRASIL**. Código Penal.** DECRETO-LEI Nº 2.848, DE 7 DE DEZEMBRO DE 1940**.**

BRASIL**. Código de Processo Penal**. DECRETO-LEI Nº 3.689, DE 3 DE OUTUBRO DE 1941**.**

BRASIL. LEI N 12.737, DE 30 DE NOVEMBRO DE 2012.

BRASIL. LEI N 13.709, DE 14 DE AGOSTO DE 2018.

BRASIL. LEI N 13.853, DE 08 DE JULHO DE 2019.

BRASIL. LEI N 13.964, DE 24 DE DEZEMBRO DE 2019.

BRASIL. LEI N° 14.155 DE 27 DE MAIO DE 2021.

BRENOF, Ann. **Como um golpe bilionário na internet está partindo corações e esvaziando contas bancárias.** 2017. Disponível em: <https://www.huffpostbrasil.com/2017/08/04/como-um-golpe-bilionario-na-internet-esta-partindo-coracoes-e-s_a_23063731/>. Acesso em: março de 2022.

BRITO, Edivaldo. **O que é o ip? descubra para que serve e qual é seu número? o ip (ou internet protocol) é uma identificação única para cada computador conectado a uma rede. descobrir este número é bastante fácil e pode ser úteis para diversas situações**. 2013. Disponível em: <https://www.techtudo.com.br/noticias/2013/05/o-que-e-o-ip-descubra-para-o-que-serve-e-qual-e-seu-numero.ghtml>. Acesso em: Março de 2022.

CABETTE, Eduardo Luiz Santos. **Furto mediante fraude e estelionato no uso de cartões de crédito e/ou débito subtraídos ou clonados**. 2012. Disponível em: <https://egov.ufsc.br/portal/conteudo/furto-mediante-fraude-e-estelionato-no-uso-de-cart%C3%b5es-de-cr%C3%a9dito-eou-d%C3%a9bito-subtra%C3%addos-ou->. Acesso em 04/11/2021.

CAPEZ, Fernando. **Parte especial arts. 121 a 212 / Fernando Capez. Coleção Curso de direito penal**. V. 2 – 20. Ed. – São Paulo: Saraiva Educação, 2020.

CAPEZ, Fernando. **Parte especial arts. 213 a 359-h / Fernando Capez. Coleção Curso de direito penal.** V. 3 – 18. Ed. – São Paulo: Saraiva Educação, 2020.

CARCARÁ, Thiago. **Estelionato virtual: a reinvenção de uma prática criminosa secular**. Disponível em: <https://procon.pmt.pi.gov.br/estelionato-virtual-a-reinvencao-de-uma-pratica-criminosa-secular/. Acesso em: 30/04/2022.

CARDOSO, Letycia. **Golpe do amor: estelionatários seduzem vítimas pela internet para pedir dinheiro**. 2020. Disponível em: <https://extra.globo.com/economia-e-financas/golpe-do-amor-estelionatarios-seduzem-vitimas-pela-internet-para-pedir-dinheiro-24612535.html?versao=amp>. Acesso em: novembro de 2021.

CASTELLS, Manuel. **A sociedade em rede**. 6. Ed. São Paulo: Paz e terra, 1999.

CAVALIERI FILHO, S. **Programa de responsabilidade civil**. 12. Ed. São Paulo: Atlas, 2014.

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

Dicionário Priberam. Disponível em: <https://dicionario.priberam.org/canto%20da%20sereia>. Acesso em janeiro de 2022.

Estelionato. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/ campanhas-e-produtos/direito-facil/edicao-semanal/estelionato>. Acesso em 29/10/2021 as 17:15

FEITOZA, Luís Guilherme De Matos. **Crimes Cibernéticos: O Estelionato Virtual.** Disponível em: <https://egov.ufsc.br/portal/sites/default/files/crimes_ciberneticos_o_estelionato_virtual.pdf>.Acesso em 04/11/2021 às 17.39.

FILHO. Edson Benedito Rondon; KHALIL, Karina Pimentel. **Scammers: Estelionato Sentimental Na Internet**. Disponível em: < file:///D:/Users/DELL/Downloads/397-Texto%20do%20Artigo-1169-1-10-20210524.pdf>. Acesso em março de 2022.

FISCHER, Neuber. **Conexão Repórter investiga a história de três mulheres sedutoras e perigosas.** 2016. Disponível em: <https://observatoriodatv.uol.com.br/noticias/conexao-

reporter-investiga-a-historia-de-tres-mulheres-sedutoras-e-perigosas>. Acesso em novembro de 2021.

GOMES, Luiz Flávio. **Direito penal: parte geral**: volume 2. – São Paulo: Editora Revista dos Tribunais, 2007.

GONÇALVES, Victor Eduardo Rios. **Direito penal esquematizado: parte especial do Código Penal**. - 8. Ed. – São Paulo: Saraiva Educação, 2018.

GONÇALVES, Nelson. **Como age o estelionatário sedutor?** 2014. Disponível em: <https://www.jcnet.com.br/noticias/policia/2014/08/415740-como-age-o-estelionatario-sedutor.html>. Acesso em 01/11/2021 as 16:41.

GRECO, Rogério. **Código Penal Comentado**. 5 ed. Rio de Janeiro: Impetus, 2011.

GRECO, Rogério. **Curso de Direito Penal**. 20. Ed. Rio de Janeiro: Impetus, 2018.

Greene, Robert. **A arte da sedução / Robert Greene: tradução de Talita M. Rodrigues**. – Rio de Janeiro: Rocco, 2004.

HUNGRIA, Nelson. **Comentários ao Código Penal** – Vol. IX. Rio de Janeiro: Forense, 1958.

INTERNET. **Conceito de virtual**. 2013. Disponível em: <https://conceito.de/virtual >. Acesso em: janeiro de 2021

INTERNET. **O significado de criptografia.** 2016. Disponível em: <https://www.significados.com.br/criptografia/ >. Acesso em: janeiro de 2021.

JAISHANKAR, K. **The Future of Cyber Criminology: Challenges and Opportunities. International Journal of Criminology Cyber (IJCC)**. v.4, issue 1,2, p.26-31. 2010. Disponível em: <http://www.cybercrimejournal.com/editorialjai2010ijcc.pdf >. Acesso em: março de 2022.

LOPES, ALAN MOREIRA; TEIXEIRA, TARCISIO. **Direito das Novas Tecnologias: Legislação eletrônica comentada, mobile law e segurança digital**. RT, 2015.

LOPES, ALAN MOREIRA; TEIXEIRA, TARCISIO. **Startups e Inovação. Direito no Empreendedorismo**. Editora Manole, 2017.

LUDGERO, Paulo Ricardo. **O que são Scammers? Entenda a fraude.** Disponivel em: <https://ludgeroadvocacia.jusbrasil.com.br/artigos/883306590/o-que-sao-scammers-entenda-a-fraude>. Acesso em: março de 2022.

MIRABETE, Júlio Fabbrini e FABBRINI, Renato N. **Manual de direito penal: parte especial: arts. 121 a 234-B do CP** – volume 2, 36° edição, São Paulo, Atlas, 2021.

MONTEIRO, Renato Leite. **Crimes eletrônicos: uma análise econômica e constitucional.** Fortaleza, 2010. Disponível em:< http://www.dominiopublico.gov.br/download/teste/arqs/cp142465.pdf>. Acesso em: 20 abr. 2020.

MOREIRA, Rômulo de Andrade. **Conflito negativo de atribuições entre os membros do MP**. 2010. Disponível em:< https://www.migalhas.com.br/depeso/ 107045/conflito-negativo-de-atribuicoes-entre-membros-do-mp >. Acesso em: 22 fev. 2020.

MOURA, Grégore Moreira de**. O Direito Penal enganador, a Lei Anticrime e o crime de estelionato.** 2021. Disponível em: <https://congressoemfoco.uol.com.br/blogs-e-opiniao/forum/o-direito-penal-enganador-a-pacote-anticrime-e-o-crime-de-estelionato/>. Acesso em 16/12/2021.

NAUATA, Felipe Machado. **Crimes virtuais: estelionato**. 2018. Disponível em:< https://jus.com.br/artigos/65242/crimes-virtuais-estelionato>. Acesso em: 19 fev. 2020.

NETO, Vladimir; LACERDA, Denise. **Mulheres bonitas eram usadas por quadrilha para golpes em prefeituras.** Ed. 29/09/2013. Disponível em: < https://g1.globo.com/fantastico/noticia/2013/09/mulheres-bonitas-eram-usadas-por-quadrilha-para-golpes-em-prefeituras.html>. Acesso em: novembro de 2021.

OLIVEIRA, Hesron Cesar. **Cibercrimes: Do Estelionato Virtual.** Disponível em: http://repositorio.aee.edu.br/bitstream/aee/17815/1/2020%20-TCC%20-HESROM%20C%C3%89SAR%20DE%20OLIVEIRA.pdf>. Acesso em: 22/09/2021.

OLIVEIRA, Ricardo Alexandre de. **O legítimo interesse e a LGPD**. São Paulo: Revista Dos Tribunais, 2020.

PACHECO, francisco. **Conexão repórter investiga a história de três mulheres sedutoras e perigosas.** Disponível em: https://www.noticiasdatvbrasileira.com.br/2016/06/conexao-reporter-investiga-historia-de.html?m=1. Acesso em: março de 2022.

PAGNOZZI, Isadora Marina Catelan de Almeida. **Crimes Virtuais: uma abordagem jurídica acerca das limitações no combate aos crimes cibernéticos**. Curitiba, 2018.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: Comentários à Lei 13.709/2018 - LGPD.** São Paulo: Saraiva, 2020.

PINHEIRO, Patricia Peck. **Direito Digital**. São Paulo: Saraiva,2010, 4 ed. Rev. Atual e Ampl.

PINOCHET, L. **Tecnologia da Informação e Comunicação**. Rio de Janeiro: Grupo GEN, 2014. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788595153196/>. Acesso em: 24 de setembro de 2021.

Redação. Isto é Gente. 25/11/2021. **Italiano cai em golpe e passa 15 anos achando que namorava Alessandra Ambrosio**. Disponível em: <https://istoe.com.br/italiano-cai-em-golpe-e-passa-15-anos-achando-que-namorava-alessandra-ambrosio/>. Acesso em: março de 2022.

RELATÓRIO ESPECIAL DIGITAL 2021. **Seu Guia Definitivo Para O Mundo Digital Em Evolução**. Disponível em: <https://wearesocial.com/uk/blog/2021/01/digital-2021-uk/>. Acesso em: Abril de 2022.

RIBEIRO JR., W.A. As sereias. Portal Graecia Antiqua, São Carlos. Disponível em: <https://pt.wikipedia.org/wiki/Sereia>. Acesso em: Fevereiro de 2022.

SANTOS, RAFA. **"Lei Anticrime" torna estelionato crime de ação condicionada e divide opiniões.** 2020. Disponível em: <https://www.conjur.com.br/2020-jan-02/lei-anticrime-torna-estelionato-crime-acao-condicionada>. Acesso em 04/11/2021 as 15.37

SILVA, Beronalda Messias da, ASSIS, Mariana Redondo de. **Phishing de internet, como criminalizar? Aspectos técnicos e jurídicos dessa ameaça virtual**. Disponível em: http://www.publicadireito.com.br/artigos/?Cod=6840f4a1c1d 16484. Acesso em 03/11/2021.

SÓTER, Cecília. **De novo? Brasileira acha que namora músico grego e perde R$ 880 mil**. Correio Braziliense, 2021. Disponível em: < https://www.correiobraziliense.com.br/diversao-e-arte/2021/12/4967705-de-novo-brasileira-acha-que-namora-musico-grego-e-perde-rs-880-mil.html>. Acesso em 16/12/2021.

TEIXEIRA, Filipe Silva; CHAVES, Fábio Barbosa. **Os crimes de fraude e estelionato cibernéticos e a proteção ao consumidor no e-commerce.** 2019. Disponível em: <https://jus.com.br/artigos/73480/os-crimes-de-fraude-e-estelionato-ciberneticos-e-a-protecao-ao-consumidor-no-e-commerce>. Acesso em 22/10/2021.

VELASCO, Clara; MANCINI, Fernando. **Golpes em Redes Sociais crescem no Brasil; veja como não cair.** G1 E TV GLOBO. 2022. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2022/03/09/golpes-em-redes-sociais-crescem-no-brasil-veja-como-nao-cair.ghtml>. Acesso em 11/04/2022.

VIGNOLI, Richele Grenge; MONTEIRO, Silvana Drumond. **A dark web e seu conteúdo informacional. In: VI SECIN, Seminário em Ciência e Informação**. UEL: Londrina – PR, 3 a 5 de agosto de 2016. Disponível em: <http://www.uel.br/eventos/cinf/index.php/secin2016/secin2016/paper/viewfile/266/186> Acesso em: março de 2022.

WE ARE SOCIAL E HOOTSUITE - Digital 2021 [Resumo E Relatório Completo]. **Digital 2021: Os Mais Recentes Insights Sobre O 'Mundo Do Digital'.** Disponível em: <https://www.amper.ag/post/we-are-social-e-hootsuite-digital-2021-resumo-e-relat%c3%b3rio-completo>. Acesso em: Abril de 2022.