PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

ESTELIONATO VIRTUAL NO DIREITO BRASILEIRO

ORIENTANDO: RUANH NERES DE ALMEIDA
ORIENTADORA: PROF.ª DR.ª FERNANDA DA SILVA BORGES

GOIÂNIA
2023

RUANH NERES DE ALMEIDA

ESTELIONATO VIRTUAL NO DIREITO BRASILEIRO

Artigo Científico apresentado à disciplina Trabalho de Curso II da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás. Prof.(a) Orientadora: Profa. Drª Fernanda da Silva Borges

GOIÂNIA-GO.

2023

RUANH NERES DE ALMEIDA

ESTELIONATO VIRTUAL NO DIREITO BRASILEIRO

Data da Defesa: ___ de _____ de _____

_____

Orientador (a): Prof. (a): Titulação e Nome Completo Nota

_____

Examinador (a) Convidado (a): Prof. (a): Titulação e Nome Completo Nota

ESTELIONATO VIRTUAL NO DIREITO BRASILEIRO

Ruanh Neres de Almeida

Com o crescente número de pessoas utilizando a internet para realizar transações financeiras, o estelionato virtual tem se tornado cada vez mais comum. O objetivo do presente artigo foi apresentar os diferentes tipos de estelionato virtual e as medidas preventivas que podem ser tomadas para evitar esse tipo de crime. Para isso, utilizou-se da pesquisa de revisão bibliográfica baseada em estudos e pesquisas sobre o tema. Os resultados desta pesquisa incluem informações importantes sobre os diferentes tipos de estelionato virtual, como phishing, engenharia social e malware. Além disso, foram apresentadas medidas preventivas que podem ser tomadas pelos usuários para evitar serem vítimas desses golpes. É importante que a sociedade digital esteja preparada para lidar com as novas formas de criminalidade que surgem no ambiente virtual para garantir a segurança e a privacidade dos indivíduos, das empresas e das instituições públicas.

INTRODUÇÃO

A sociedade contemporânea tem passado por uma grande transformação com o advento da tecnologia e a popularização da internet. Com isso, novas formas de interação social e econômica surgiram, trazendo consigo novos desafios e problemas. Um desses problemas é o aumento dos crimes virtuais, que têm se tornado cada vez mais frequentes e sofisticados.

O estelionato virtual é um desses crimes que tem ganhado destaque nos últimos anos. Ele consiste em uma fraude realizada por meio eletrônico, na qual o criminoso utiliza informações falsas ou enganosas para obter vantagens financeiras ou patrimoniais de terceiros. Essa prática criminosa pode ser realizada de diversas formas, como clonagem de cartões de crédito, *phishing,* entre outras.

Diante desse cenário, surge a problemática da pesquisa: como prevenir e combater o estelionato virtual? Essa questão se torna ainda mais relevante quando consideramos que os crimes virtuais podem afetar não apenas indivíduos, mas também empresas e instituições públicas.

Assim sendo, este trabalho tem como objetivo principal analisar as diferentes formas de estelionato virtual e apresentar medidas preventivas para evitar esse tipo de crime. Além disso, busca-se compreender a legislação

brasileira em relação aos crimes cibernéticos e avaliar sua eficácia na punição dos criminosos.

Para alcançar esses objetivos será utilizada uma metodologia de pesquisa bibliográfica exploratória. Serão consultados livros, artigos científicos e legislações relacionadas ao tema em questão. A partir dessa análise bibliográfica, serão apresentadas as principais formas de estelionato virtual e as medidas preventivas que podem ser adotadas para evitá-las.

O trabalho está estruturado em três seções. Na primeira seção, serão apresentados os conceitos básicos sobre crimes virtuais e o surgimento do estelionato virtual. Na segunda seção, serão descritas as diferentes formas de estelionato virtual, como clonagem de cartões de crédito e phishing. Por fim, na terceira seção, serão apresentadas as medidas preventivas que podem ser adotadas para evitar o estelionato virtual.

Serão abordados temas como a importância da educação digital para a prevenção dos crimes virtuais, a necessidade de verificar a autenticidade dos sites e e-mails recebidos e a importância de manter softwares atualizados.

Além disso, será realizada uma análise da legislação brasileira em relação aos crimes cibernéticos. Serão apresentadas as principais leis que tratam do assunto e avaliada sua eficácia na punição dos criminosos. Nesse sentido, acreditamos que essa pesquisa é relevante tanto do ponto de vista social quanto jurídico, pois pode ajudar na prevenção desse tipo de crime e na proteção dos direitos dos cidadãos.

1 DOS CRIMES VIRTUAIS: ASPECTOS PRINCIPAIS

De acordo com Pozzebom (2022), o aumento constante do uso da internet e da tecnologia em nossas vidas, os crimes virtuais, também conhecidos como crimes cibernéticos, se tornaram uma preocupação cada vez mais relevante. Esses crimes podem ser classificados de diversas maneiras, dependendo do tipo de crime e da abordagem utilizada para sua classificação.

Uma das principais categorias de crimes virtuais é a fraude, esse tipo de crime envolve o uso de técnicas de engenharia social para enganar as pessoas e obter informações ou dinheiro de forma ilegal (TEIXEIRA, 2022).

A autora cita os exemplos que incluem phishing, spam, golpes de pagamento adiantado e fraude de cartão de crédito. Os criminosos virtuais muitas vezes utilizam técnicas sofisticadas para criar mensagens e sites falsos que parecem autênticos, a fim de enganar as pessoas e obter informações confidenciais (POZZEBOM, 2022).

Outra categoria importante de crimes virtuais é a relacionada à propriedade, esse tipo de crime envolve o roubo ou danos a dados, software ou hardware.

Os exemplos incluem invasão de sistemas, furto de propriedade intelectual e sabotagem de sistemas, os criminosos virtuais podem utilizar técnicas de hacking para invadir sistemas e roubar informações confidenciais, ou mesmo sabotar sistemas inteiros para prejudicar empresas e indivíduos.

Os crimes virtuais também podem ser classificados de acordo com o impacto que eles têm na privacidade das pessoas, crimes contra a privacidade envolvem o acesso não autorizado a informações pessoais, como dados bancários, registros médicos e informações de identificação pessoal.

Esses crimes podem ter um grande impacto na vida das pessoas, incluindo perda financeira, comprometimento da identidade e exposição de informações pessoais, De acordo com Fia (2021, online):

> Além das questões psicológicas que atingem as vítimas, há também o impacto financeiro tanto para elas quanto para empresas ou instituições. Os usuários privados podem ter que arcar com custos de tratamento psicológico e psiquiátrico.

O crime virtual consiste em um conjunto de ações ilegais que ocorrem no contexto da utilização de tecnologias de informação e comunicação, tais como computadores, internet, redes sociais, dispositivos móveis, entre outros. Trata-se de atos que violam normas legais, cometidos por meio do processamento automatizado ou eletrônico de informações ou sua difusão (FERREIRA, 1992).

Além disso, existem crimes virtuais relacionados ao conteúdo, como a distribuição ilegal de conteúdo protegido por direitos autorais ou a criação de conteúdo prejudicial, como pornografia infantil e discurso de ódio, também existem crimes relacionados à segurança nacional, que envolvem ataques a sistemas de infraestrutura crítica, roubo de informações governamentais sensíveis e espionagem cibernética. E, finalmente, existem crimes relacionados à tecnologia, como malware, botnets e ataques de negação de serviço.

É importante lembrar que a classificação dos crimes virtuais continua a evoluir à medida que novas tecnologias e tendências surgem, à medida que as pessoas se tornam cada vez mais dependentes da tecnologia.

1.1 O SURGIMENTO DOS CRIMES VIRTUAIS E OS DESAFIOS DA SOCIEDADE DIGITAL

Os primeiros registros de delitos cibernéticos datam dos anos 60, quando indivíduos mal-intencionados manipulavam informações contidas em computadores para perpetrar atividades ilegais, tais como sabotagem, espionagem e abuso de sistemas computacionais, como aponta, Novais (200, p14):

> Os crimes cibernéticos existem desde o início da internet, e no Brasil não se tornou diferente, mas somente em 18 de junho de 1996 se tornou registrado o primeiro crime cibernético brasileiro. A notícia se tornou pública quando foi descoberta uma invasão em vários sites ligados ao governo, como o site oficial do Supremo Tribunal Federal, e partir deste evento a sociedade brasileira soube pela primeira vez o que seria o início dos crimes cibernéticos, e o governo passou a ter esta invasão cibernética como seu primeiro problema virtual, e sem qualquer plano imediato para apresentar como solução.

No entanto, naquela época, a identificação dessas práticas era bastante desafiadora devido às limitações técnicas existentes, todavia, a partir da década de 80, ocorreu uma mudança significativa no panorama, com a identificação e divulgação de várias atividades criminosas cometidas por meios virtuais, como a violação de direitos autorais, a adulteração de caixas eletrônicos e a exploração ilegal de telecomunicações, entre outras.

A intensificação desses delitos levou ao surgimento das primeiras leis que normatizavam a prática dessas ações ilícitas, desse modo, é possível afirmar que a criminalidade virtual evoluiu de forma significativa ao longo das décadas, acompanhando o desenvolvimento tecnológico e as demandas do mercado digital.

Com o avanço das tecnologias digitais, a internet e as redes sociais se tornaram ferramentas indispensáveis para a comunicação, o entretenimento, o trabalho e as compras online. No entanto, essa mesma evolução tecnológica também abriu caminho para um novo tipo de crime os crimes virtuais, Segundo Pinheiro (2000, p.20)

> Com a popularização da Internet em todo o mundo, milhares de pessoas começaram a se utilizar deste meio. Contemporaneamente se percebe que nem todos a utilizam de maneira sensata e, acreditando que a internet um espaço livre, acabam por e ceder em suas condutas e criando novas modalidades de delito.

O surgimento desses crimes é fruto da própria evolução da tecnologia e da popularização da internet, que tornaram possível a criação de ferramentas e técnicas para a prática de crimes online.

Um dos principais desafios dos crimes virtuais é a dificuldade de identificar os criminosos e coletar provas, muitos desses crimes são cometidos por pessoas que estão em outro país ou até mesmo em outra região do mundo, alguns criminosos utilizam até de meios mais sofisticados como o uso da VPN (REDE PRIVADA VIRTUAL) que consiste em ser uma técnica que visa ocultar o endereço IP do dispositivo que está sendo utilizado para cometer crimes virtuais, dificultando a identificação do autor das atividades criminosas e, consequentemente, a sua captura pelas autoridades, tornando a investigação e punição dos criminosos um processo complexo e muitas vezes frustrante.

Conforme o autor Northcutt (2022, p.156) expressa:

> VPN é uma conexão estabelecida por uma infraestrutura "pública" ou compartilhada existente, usando tecnologias de criptografia ou autenticação para proteger seu tráfego de dados. Isso cria um segmento "virtual" entre duas entidades quaisquer que têm acesso.

Outro desafio é a falta de legislação específica para crimes virtuais em muitos países principalmente no Brasil. Como os crimes virtuais são relativamente recentes, muitos países ainda estão se adaptando às novas formas de criminalidade que surgem no ambiente virtual, além disso, a cooperação internacional entre países muitas vezes é difícil, o que dificulta ainda mais a investigação e punição dos criminosos, (SIQUEIRA, 2017, p.122):

> Seria possível a identificação do criminoso obtendo o seu endereço de IP, login e senha do aparelho utilizado para a prática do crime, porém, os criminosos utilizam endereços falsos, dificultando o trabalho investigativo dos policiais.

Mas é possível adotar medidas de segurança e estabelecer leis para enfrentar essa nova forma de criminalidade.

A evolução das tecnologias digitais continua, e é importante que a sociedade esteja preparada para lidar com os novos desafios que surgem no ambiente virtual, um ponto importante a ser destacado é que os crimes virtuais não afetam apenas indivíduos e empresas, mas também governos e instituições públicas, ataques cibernéticos a sistemas governamentais e de infraestrutura crítica, como redes elétricas e sistemas de transporte, podem causar danos irreparáveis e colocar a segurança nacional em risco, por isso, é essencial que governos e instituições estejam preparados para lidar com essas ameaças, isso inclui a criação de equipes especializadas em segurança cibernética, a implementação de políticas de segurança robustas, a realização de testes de vulnerabilidade e a adoção de tecnologias avançadas de proteção, além disso, é importante destacar que os crimes virtuais não são cometidos apenas por indivíduos mal intencionados, mas também por organizações criminosas e até mesmo por governos.

Ataques cibernéticos patrocinados por Estados podem ser utilizados para fins políticos, econômicos ou militares, representando uma grave ameaça à segurança global.

Por isso, a cooperação internacional é essencial para combater os crimes virtuais e garantir a segurança cibernética. É necessário que os governos compartilhem informações e recursos, estabeleçam acordos de cooperação e atuem de forma coordenada para investigar e punir os criminosos virtuais.

O surgimento dos crimes virtuais é um fenômeno complexo e multifacetado, que representa um desafio para a sociedade digital e para a segurança global, no entanto, é possível enfrentar essa ameaça por meio da adoção de medidas de segurança, da criação de leis específicas, da cooperação internacional e do desenvolvimento de tecnologias avançadas de proteção, como aponta Fonseca (2002. pag.1):

> Não basta, para a aplicação da sanção penal, o conhecimento superficial sobre a identidade do acusado, não se trata de homonímia, mas da comprovação de que aquele que se figura como imputado realmente praticou o que lhe é imputado.

Cabe à sociedade digital estar sempre em busca de conhecimento e preparada para lidar com as novas formas de criminalidade que surgem no ambiente virtual para evitar ser uma vítima. Somente assim será possível garantir a segurança e a privacidade dos indivíduos, das empresas e das instituições públicas, e proteger a integridade da sociedade como um todo.

1.2 SUJEITOS DO CRIME

Os conceitos de sujeito ativo e sujeito passivo são importantes no direito penal para identificar quem cometeu o crime (sujeito ativo), e quem sofreu os efeitos do crime (sujeito passivo).

1.2.1 Sujeito Ativo

O sujeito ativo do estelionato virtual é aquele que pratica a fraude ou golpe por meio da internet, com o objetivo de obter vantagem financeira ou patrimonial

de forma ilícita, o sujeito ativo do estelionato virtual pode ser qualquer pessoa que tenha habilidades técnicas para realizar golpes pela internet, incluindo conhecimentos de informática, programação e segurança virtual. Em muitos casos, os golpistas atuam em quadrilhas especializadas em crimes virtuais, que utilizam técnicas avançadas para ludibriar as vítimas, seguimos com o conceito do autor Fonseca (2002, pag.1):

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

Entre os principais tipos de golpes praticados pelo sujeito ativo do estelionato virtual, estão o phishing, em que o golpista envia e-mails ou mensagens falsas para obter informações pessoais ou financeiras da vítima; o malware, em que o golpista instala programas maliciosos nos computadores das vítimas para capturar informações pessoais ou financeiras; e o ransomware, em que o golpista bloqueia o acesso aos dados do usuário e exige o pagamento de um resgate para liberá-los.

O sujeito ativo do estelionato virtual pode agir de forma anônima, utilizando técnicas de camuflagem para ocultar sua identidade e localização.

1.3.2 Sujeito Passivo

O sujeito passivo do estelionato virtual é a pessoa ou instituição que sofre prejuízo financeiro em decorrência de um golpe ou fraude realizada por meio da internet. Esse tipo de crime, conhecido como estelionato virtual ou golpe eletrônico. Conforme citado por Nabuco (s.d), o sujeito passivo do estelionato virtual pode ser qualquer pessoa ou empresa que utiliza a internet para realizar transações financeiras ou compartilhar informações pessoais. Isso inclui consumidores que realizam compras online, empresas que realizam transações comerciais pela internet, usuários de redes sociais que compartilham informações pessoais, entre outros.

O sujeito passivo do estelionato virtual muitas vezes pode ter prejuízos financeiros significativos, como a perda de dinheiro em transações fraudulentas, a cobrança de valores indevidos em cartões de crédito, ou mesmo a perda de dados pessoais e financeiros que podem ser utilizados pelos golpistas para realizar outros crimes.

2 ESTELIONATO VIRTUAL: PRINCIPAIS CARACTERÍSTICAS

O crime de estelionato é um crime que nos últimos tempos ocorre frequentemente e por isso, a sociedade necessita de maior conhecimento e de respaldo. Assim, se faz necessário compreender os aspectos deste tipo de crime, visto que são praticados em ambos os ambientes, tanto no meio virtual, quanto fora da internet, e está disposto no artigo 171, do Código Penal.
Em conformidade com a Lei nº 2.848 de 07 de dezembro de 1940, temos que:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento. Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis (BRASIL, 1940).

Estelionato é uma palavra originária do grego *stelio*, que se refere a um tipo de lagarto que modifica a cor de seu corpo para enganar suas presas. A denominação da expressão jurídica “estelionato” se deu pelo fato da relação do comportamento do lagarto para conseguir suas presas, com pessoas que utilizam de truques e artifícios para enganar alguém (RIBEIRO, 2019).

O estelionato é um crime que atenta contra o patrimônio, sendo que a legislação penal procura proteger a inviolabilidade patrimonial por meio da prevenção de atos que visam enganar a vítima para beneficiar o agente (CUNHA, 2019).

O delito em questão é caracterizado pelo ato de enganar, fraudar ou burla a vítima, que faz a vítima acreditar em uma história ou conversa que na verdade é uma farsa, como resultado, a pessoa pode sofrer prejuízos e consequências financeiras ou até mesmo atitudes criminosas que afetam sua honra muitas vezes irreparáveis.

É importante ressaltar que, no crime de estelionato, não há violência ou grave ameaça por parte do autor.

Em conformidade com a Lei nº 2.848 de 07 de dezembro de 1940, temos que:

> Art. 158 - Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa: Pena - reclusão, de quatro a dez anos, e multa (BRASIL, 1940)

Entre outros aspectos, no fato de que, no estelionato, a vítima é levada a entregar voluntariamente o objeto, enquanto na extorsão, ela é forçada a entregar contra sua vontade, por meio de violência ou grave ameaça. Em outras palavras, na extorsão, há a entrega do objeto, mesmo que o ofendido não queira entregá-lo, enquanto no estelionato, a vítima entrega conscientemente, embora iludida.

Conforme mencionado por Silva (2020):

> Diferenciam-se os crimes de extorsão e estelionato, entre outros aspectos, porque no estelionato a vítima quer entregar o objeto, pois foi induzida ou mantida em erro pelo agente mediante o emprego de fraude; enquanto na extorsão a vítima despoja-se de seu patrimônio contra a sua vontade, fazendo-o por ter sofrido violência ou grave ameaça.

O bem jurídico protegido pelo estelionato é a inviolabilidade do patrimônio, especialmente em relação aos ataques que podem ser realizados por meio de fraude. O ordenamento jurídico visa proteger tanto o interesse social, representado pela confiança recíproca que deve prevalecer em relacionamentos patrimoniais individuais e comerciais, quanto o interesse público de repelir qualquer fraude que possa causar danos a alguém.

Em síntese, é possível afirmar que o estelionato é um crime que visa enganar e prejudicar uma pessoa por meio de artimanhas e estratégias fraudulentas. A legislação penal tem como objetivo proteger a inviolabilidade patrimonial e evitar que os indivíduos caiam em golpes que possam causar prejuízos financeiros. Neste sentido, a compreensão sobre a natureza e os mecanismos do estelionato é fundamental que sejam mais rigorosas e especificas para o desenvolvimento de políticas públicas e medidas de prevenção que possam coibir este tipo de crime.

2.1 CARTÕES CLONADOS

Os carders são indivíduos que praticam atividades ilícitas relacionadas ao uso fraudulento de cartões de crédito e débito. Essas atividades podem incluir a compra de informações de cartões roubados, a venda de cartões clonados, e a realização de transações fraudulentas utilizando cartões de terceiros.

Em geral, os carders utilizam técnicas de hacking e engenharia social para obter informações sensíveis de cartões de crédito e débito, como número, data de validade, código de segurança (CVV), entre outras. Essas informações podem ser obtidas através da invasão de sistemas de empresas e instituições financeiras, do phishing (envio de e-mails e mensagens fraudulentas), do uso de skimmers (dispositivos instalados em caixas eletrônicos e máquinas de cartão), e outras técnicas.

Conforme citado por Nakamura (2007, p.22):

> A transação eletrônica segura, utilizado no comercio de eletrônico, faz com que as lojas virtuais não tenham acesso ao número do cartão de crédito, o que poderia ser aproveitado para uma base de dados de seus clientes. Essa, na realidade, é uma característica importante para a segurança, pois o maior perigo dos incidentes envolvendo cartões de crédito está relacionado ao seu armazenamento.

Com essas informações em mãos, os carders podem criar cartões clonados, que são cópias idênticas dos cartões originais, e utilizá-los para realizar transações fraudulentas em lojas físicas e online. Eles também podem vender esses cartões no mercado negro da internet, para outros criminosos que desejam usá-los para fins ilegais.

As vítimas muitas vezes só percebem que seu cartão foi clonado quando recebem as faturas do cartão de crédito com transações desconhecidas ou quando são notificadas pelo banco sobre transações suspeitas.

O cartão clonado é um dos crimes mais comuns relacionados à segurança cibernética.

2.2 PHISHING

Phishing e uma prática utilizada pelos criminosos fazendo a criação de uma réplica de um site legítimo e tentam convencer as vítimas a fornecer informações pessoais ou financeiras, phishing de acordo com Pena (2020, pag.1):

> O termo vem do inglês phishing surgiu nos anos 1990 e é uma alteração de fishing, que quer dizer pescaria, que consiste em deixar várias iscas pela internet aguardando que sejam mordidas. Podemos definir phishing como qualquer tipo de fraude por meios de telecomunicação, que usa truques de engenharia social para obter dados privados das vítimas.

Eles podem fazer isso de várias maneiras, como criar um link parecido com a do site legítimo é adicionar um certificado SSL para dar a impressão de que o site é seguro, SERASA (2021, online) é enfático ao afirmar:

> SSL é a sigla para Secure Sockets Layer, uma ferramenta de segurança digital usada para comunicar sites e navegadores de forma criptografada. É ela a responsável por modificar os endereços dos sites de HTTP para HTTPS, o que indica que oferecem comunicação segura com o servidor, o SSL é extremamente importante para proteger informações sensíveis inseridas em um site, por isso deve estar presente quando um usuário fornece dados como números de documentos, cartões de crédito ou de login, ele dificulta a captura dessas informações por hackers que buscam roubar dados de pessoas e empresas, impedindo que elas sejam interceptadas, capturadas ou visualizadas enquanto são transferidas até o servidor.

Uma vez que a vítima acessa o site falso, ela é levada a fornecer informações como nome de usuário, senha, endereço de e-mail, número de cartão de crédito ou outras informações pessoais e financeiras. Essas informações são, então, usadas pelos criminosos para cometer fraude. Clonagem de sites é uma técnica de phishing muito eficaz porque muitos usuários não verificam a URL do site que estão visitando ou não percebem a diferença entre o site real e o falso.

Além disso, os criminosos frequentemente usam táticas de engenharia social, como enviar e-mails de phishing com links para sites falsos, para atrair as vítimas a fornecerem suas informações.

Segundo Mitnick (2003), os especialistas em engenharia social buscam obter o máximo de informações sobre sua vítima, com o objetivo de criar um ambiente de conforto, familiaridade e confiança. Para isso, podem dedicar dias ou até semanas em pesquisa aprofundada, coletando dados sobre os interesses, preferências e história pessoal da pessoa que pretendem enganar.

Outro método comum de phishing é o phishing por e-mail, os criminosos enviam e-mails falsos, que parecem ser de uma empresa ou organização legítima, com o objetivo de enganar as vítimas a clicar em um link ou baixar um anexo malicioso, o link ou o anexo pode levar a um site falso ou a um arquivo infectado por malware, os e-mails de phishing geralmente contêm uma mensagem urgente ou alarmante, como um aviso de que sua conta será suspensa se você não clicar no link ou fornecer informações pessoais ou financeiras imediatamente. Eles também podem usar táticas de engenharia social, como fazer parecer que o e-mail é de uma pessoa que você conhece ou que está familiarizado com você.

O phishing por SMS é semelhante ao phishing por e-mail, mas envolve o envio de mensagens de texto em vez de e-mails. Os criminosos enviam mensagens de texto que parecem ser de uma empresa ou organização legítima e pedem que você clique em um link ou forneça informações pessoais ou financeiras, assim como no phishing por e-mail, as mensagens de texto de phishing geralmente contêm uma mensagem urgente ou alarmante e usam táticas de engenharia social para convencer as vítimas a fornecerem informações pessoais ou financeiras, eles também podem usar números de telefone falsos ou de outras pessoas para mascarar sua verdadeira identidade.

2.2.1 Bankers

Os bankers são criminosos especializados em roubar informações bancárias e financeiras, como senhas, números de contas e outros dados sigilosos, para acessar as contas bancárias de terceiros e realizar transações fraudulentas.

Assim como os carders, os bankers também utilizam técnicas de hacking e engenharia social para obter informações confidenciais de suas vítimas. Eles podem utilizar softwares maliciosos para roubar senhas e outras informações

bancárias de computadores e dispositivos móveis, ou podem enviar e-mails e mensagens fraudulentas (phishing) para enganar as pessoas e fazer com que elas forneçam suas informações bancárias sem perceber, de acordo com Rohr (2012, online):

> O objetivo principal do Banker é roubar senhas bancárias. Alguns Bankers são também programados para roubar senhas de serviços on-line, como redes sociais. Outras versões do código são capazes de roubar cartões de crédito e senhas de usuários em sites de companhias aéreas, que depois serão acessadas para o roubo de milhas de viagens acumuladas.

Com as informações bancárias em mãos, os bankers podem acessar as contas bancárias das vítimas e realizar transações fraudulentas, como transferências bancárias, pagamento de contas e compras online. Eles também podem realizar o que é conhecido como "roubo de identidade", ou seja, utilizar as informações bancárias roubadas para criar novas contas em nome das vítimas e realizar transações fraudulentas em seus nomes.

Os bankers também podem vender as informações bancárias roubadas no mercado negro da internet, para outros criminosos que desejam utilizá-las para fins ilegais.

2.2.2 Golpes em Redes Sociais

Os golpes em redes sociais são cada vez mais comuns e sofisticados, tornando-se uma ameaça crescente para os usuários de mídias sociais.

Esses golpes geralmente começam com uma mensagem ou convite de alguém que a vítima conhece ou que parece ser legítimo, eles podem ser realizados de diversas maneiras, como através da criação de perfis falsos, envio de links maliciosos, mensagens que pedem informações pessoais ou promovem produtos ou serviços falsos.

Um dos golpes mais comuns em redes sociais é a criação de perfis falsos que se passam por pessoas conhecidas, como amigos ou familiares.

Ludgero (2020, p.2) afirma que:

> 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.

Esses perfis podem ser criados para pedir dinheiro emprestado ou oferecer uma oportunidade de investimento promissora, os criminosos também podem criar perfis falsos de empresas ou organizações legítimas para obter informações pessoais dos usuários.

Outro tipo comum de golpe em redes sociais é o envio de links maliciosos ou arquivos infectados por malware. Esses links podem ser disfarçados como vídeos engraçados ou promoções tentadoras que, ao serem clicados, levam a vítima para um site malicioso que rouba informações pessoais ou instala malware em seu computador, nesse sentido. Ludgero (2020, pag.2), menciona que:

> Neste tipo de esquema, os golpistas alegam oferecer produtos grátis para as vítimas. As supostas empresas oferecem produtos ou serviços em troca likes, compartilhamentos ou divulgações. Para concluir a entrega, pedem que elas se cadastrem e enviem informações pessoais, como o endereço e um e-mail de contato. Os usuários têm, assim, suas informações roubadas. Caso cadastrem informações bancárias, eles podem até ter seu cartão "roubado”.

As mensagens que pedem informações pessoais, como senhas de conta ou números de cartão de crédito, são outro tipo de golpe em redes sociais. Os criminosos podem se passar por representantes de empresas legítimas ou mesmo enviar mensagens que parecem ser de amigos próximos, pedindo informações pessoais que podem ser usadas para fins fraudulentos.

3 ESTELIONATO E SUA APLICABILIDADE DO DIREITO BRASILEIRO

O estelionato é um tipo de delito do Código Penal Brasileiro no qual pode ser executado de diversas maneiras, conforme se depreende do artigo 171, o

criminoso induz alguém para obter vantagens indevidas, mediante artificio ou qualquer outro meio fraudulento.

O estelionatário se adapta rapidamente ao ambiente em que se encontra, agindo de modo a iludir a vítima, com suas artimanhas e a má fé, típica do perfil de quem comete tal delito, pois esse sabe disfarçar e se utiliza muitas vezes de meios virtuais para atingir seus objetivos.

O ato praticado pelo estelionatário, que agiu com nítido comportamento doloso com o foco de obter vantagem ilícita, ocasionando prejuízo à vítima, se iguala perfeitamente ao tipo penal.

Conforme nos ensina Bitencourt (2019, p.1369):

> No estelionato, há dupla relação causal: primeiro, a vítima é enganada mediante fraude, sendo está a causa e o engano o efeito; segundo, nova relação causal entre o erro, como causa, e a obtenção de vantagem ilícita e o respectivo prejuízo, como efeito.

No tipo penal, o estelionato não exige qualquer qualidade, tanto do sujeito passivo, quanto do ativo, portanto, qualquer pessoa poderá figurar como o autor do crime ou poderá ser a vítima, sendo primordiais, para a sua configuração, o preenchimento de três elementos, quais sejam: vantagem ilícita, fraude e prejuízo alheio.

Portanto, o estelionato trata-se de crime doloso, que não admite a conduta culposa, o agente por livre e consciente desejo, induz ou mantem alguém em erro, com o intuito de obter indevida vantagem, para si ou para outrem, aceitando a tentativa, caso consiga o agente o induzimento da vítima ao erro, porém, quando da obtenção da vantagem ilícita, certa vantagem não se concretiza por circunstâncias alheias à sua vontade.

Na sociedade brasileira não é considerado algo novo o crime de estelionato. Ocorre, entretanto, a observação de um aumento nesses tipos penais, mesmo que a pena e as leis, tenha ficado mais rígidas para os estelionatários.

Em 24 de dezembro de 2019, foi sancionada a “Lei anticrime” (13.964/19), ocasionou consideradas mudanças no nosso ordenamento jurídico-penal brasileiro.

O crime de estelionato, antes era processado mediante ação penal pública incondicionada, com a mudança passou a ter o seu processamento mediante ação pública condicionada à representação, salvo alguns casos específicos, tais como: casos em que o ofendido for maior de 70 anos de idade ou incapaz, seja Administração Pública, pessoa com eficiência mental, ou criança ou adolescente.

O que se pode observar dessa modalidade de crime é que se dá devido ao crescimento tecnológico, e do acesso à internet com suas facilidades, que acarreta alguns riscos à sociedade, como o crescimento dos crimes de estelionato.

Vale ressaltar, quanto mais grave for o estelionato, maior será a consequência para o estelionatário. Bem como, se for pequeno o prejuízo, será mais branda a pena e isso incentiva os criminosos a cometer pequenos delitos várias vezes.

Para a sociedade e a aplicabilidade do direito brasileiro, o Ministério Público só poderá oferecer denúncia em contra a pessoa que está sendo investigada se o ofendido, no caso a vítima, solicitar que seja feito a apuração dos fatos às autoridades (delegado de polícia, promotor ou juiz), ou se a vítima/ofendido for alguma das exceções já mencionadas. Ressalvando que, de acordo com o art. 38 do Código de Processo Penal, a representação deverá ser feita no prazo decadencial de 6 meses, contados a partir da data em que o ofendido tomar conhecimento do (s) autor (es) dos fatos.

Segundo Lima (2019, p. 262):

> Não necessita de formalidades para que se proceda com a representação, bastando apenas a vontade expressa da vítima ou de seu representante legal, indicando que deseja que aquele que cometeu o crime seja criminalmente processado.

Surge para a sociedade brasileira como uma expectativa de que a lei penal institua penas mais rigorosas para determinados crimes, como é o caso do estelionato.

3.1 IMPACTOS SOCIAIS E ECONÔMICOS DO ESTELIONATO VIRTUAL

A Lei 14.155/2021, que foi sancionada em 27/05/2021 modifica o Código Penal, criando a figura da Fraude Eletrônica, tentando tornar mais exigente a penalidade para os crimes que violam o dispositivo informático, como podemos citar as espécies de furto e estelionato realizados através de dispositivos eletrônicos pela internet.

A segurança é uma questão de bastante importante, principalmente no ambiente físico quanto no virtual. A fraude eletrônica advém, no momento em que o criminoso atinge seu objeto, enganando por meio de redes sociais, ligações telefônicas, e-mail falso ou qualquer outro meio fraudulento, ao viabilizar informações confidenciais, tais como, senhas, de bancos ou número de cartão de crédito ou débito.

De acordo com Mitnick (2003), a segurança no ambiente virtual é um jogo constante de gato e rato, no qual as empresas precisam estar um passo à frente dos invasores para minimizar os riscos. Ele destaca que a engenharia social é uma das maiores ameaças à segurança cibernética e enfatiza a importância de conscientizar os usuários sobre os riscos e ensiná-los a identificar possíveis ameaças.

Segundo o conteúdo editorial da Security Report (2023), a FortiGuard, através de seu laboratório de inteligência divulgou que o Brasil ficou em segundo lugar nos números totais de ataques cibernéticos do ano de 2022, em relação aos atingidos na América Latina, com “103,16 bilhões de tentativas de ataques cibernéticos, um aumento de 16% com relação a 2021“.

Com a percepção dos efeitos causados por um crime cibernético e o crescimento da criminalidade e seu rápido desenvolvimento nos últimos tempos motivaram aflição em escala global com o impacto que acarreta a sociedade.

Os crimes de estelionato virtual têm um impacto significativo na sociedade brasileira. Eles podem ter como vítimas: indivíduos, empresas e instituições governamentais. Tendo como consequências mais comuns: roubo de informações pessoais, ataques a empresas, propagação de malware, fraudes online, as pessoas podem se sentir menos seguras em usar a internet para realizar transações financeiras e compartilhar informações pessoais. Isso pode prejudicar a economia digital e a inovação tecnológica no país.

Os crimes realizados virtualmente são de um impacto social e psíquico devastador, com relação aos impactos econômicos estes estão relacionados aos

prejuízos financeiros causados tanto às vítimas quanto às pessoas próximas a elas. No geral, as vítimas passam por muitos momentos de tensão até conseguir recuperar as suas contas e provar que não foram elas que tiveram tais atitudes.

Por conseguinte, a segurança é fundamental, conclui-se que a prudência aliada ao bom senso deve ser adotada por todos os indivíduos que tenham acesso a meios eletrônicos, também vale destacar que é necessário um avanço tanto normativamente quanto a especialização de uma polícia investigativa para o combate o estelionato virtual.

3.2 PREVENÇÃO DO ESTELIONATO VIRTUAL NA SOCIEDADE

A proteção no mundo virtual é uma batalha contínua de estratégia, em que as empresas devem estar sempre à frente dos invasores para reduzir os perigos. É importante salientar que a engenharia social representa uma das principais ameaças à segurança cibernética e, por isso, é fundamental conscientizar os usuários sobre os riscos e ensiná-los a identificar possíveis ameaças (MITNICK, 2003).

Com o crescente número de pessoas utilizando a internet para realizar transações financeiras, o estelionato virtual tem se tornado cada vez mais comum. O crime ocorre quando alguém é enganado por um golpista que utiliza técnicas como phishing, engenharia social ou malware para obter informações pessoais e financeiras da vítima.

Para prevenir o estelionato virtual, é necessário que os usuários tomem algumas medidas preventivas. A primeira e mais importante é estar sempre atento às transações online e às informações que são fornecidas. É preciso verificar a autenticidade dos sites e dos e-mails recebidos, bem como evitar clicar em links suspeitos ou em arquivos desconhecidos.

Além disso, é importante que os usuários utilizem senhas seguras e diferentes para cada conta, evitando a utilização de informações pessoais como data de nascimento ou nome do animal de estimação. Também é recomendável que os usuários utilizem softwares antivírus e antimalware atualizados, a fim de prevenir a ação de programas maliciosos que possam comprometer a segurança do computador (MITNICK, 2017).

As empresas também têm um papel importante na prevenção do estelionato virtual. É preciso que elas invistam em medidas de segurança eficientes, como a criptografia de dados, autenticação biométrica e outras tecnologias avançadas de segurança. Além disso, as empresas devem fornecer orientações e treinamentos para seus funcionários, a fim de que estes estejam preparados para identificar e prevenir possíveis tentativas de fraude.

O poder público também pode atuar na prevenção do estelionato virtual, promovendo campanhas de conscientização e elaborando leis mais rígidas para punir os criminosos. Além disso, é importante que as autoridades competentes estejam preparadas para investigar e punir os criminosos envolvidos nesse tipo de crime.

Por fim, é importante que haja uma cultura de prevenção do estelionato virtual na sociedade como um todo. A conscientização das pessoas é fundamental para que elas possam tomar medidas preventivas e evitar serem vítimas de golpes. É preciso que as pessoas estejam sempre atentas e informadas sobre os riscos envolvidos nas transações financeiras online.

Em resumo, a prevenção do estelionato virtual é uma responsabilidade de todos. Usuários, empresas e poder público devem estar comprometidos em adotar medidas preventivas eficientes e conscientizar a população sobre os riscos envolvidos nas transações online. Dessa forma, será possível garantir um ambiente mais seguro e protegido para todos.

CONCLUSÃO

Com base nos resultados obtidos, podemos concluir que a pesquisa atingiu seus objetivos. O objetivo principal deste estudo foi analisar as principais formas de prevenção contra o estelionato virtual na sociedade. Para isso, foram realizadas pesquisas bibliográficas de especialistas na área.

Os resultados mostraram que a proteção no mundo virtual é uma batalha contínua de estratégia, em que as empresas devem estar sempre à frente dos invasores para reduzir os perigos. Além disso, a engenharia social representa uma das principais ameaças à segurança cibernética e, por isso, é fundamental

conscientizar os usuários sobre os riscos e ensiná-los a identificar possíveis ameaças.

A hipótese inicial deste estudo foi confirmada pelos resultados obtidos. Concluímos que a prudência aliada ao bom senso deve ser adotada por todos os indivíduos que tenham acesso a meios eletrônicos. É necessário um avanço tanto normativamente quanto a especialização de uma polícia investigativa para o combate ao estelionato virtual.

Em resumo, este artigo científico apresentou informações importantes sobre crimes virtuais e como se proteger deles.

REFERÊNCIAS

BITENCOURT, Cezar Roberto. **Tratado de direito penal**. Volume II São Paulo: Saraiva, 2018.

BRASIL**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal**. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 31 mar. 2023.

BRASIL. TJDFT. **Tribunal de Justiça do Distrito Federal e dos Territórios**. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/estelionato. Acesso em: 23 fev. 2023.

CUNHA, Rogério Sanches. **Lei 14.155/21 e os crimes de fraude digital - primeiras impressões e reflexos no CP e no CPP**. Meu Site Jurídico (JusPodivm), 2021. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521. Acesso em: 08 jan. 2022.

FERREIRA, Ivete Senise. **Os crimes de informática**. In: BARRA, Rubens Prestes, ANDREUCCI, Ricardo Antunes. Estudos jurídicos em homenagem a Manoel Pedro Pimentel. São Paulo: RT, 1992.

FIA. **Crimes cibernéticos: o que são, tipos, como detectar e se proteger**. São Paulo. 2021. Disponível em: https://fia.com.br/blog/crimes-ciberneticos/. Acesso em: 02 mar. 2023.

LUDGERO, Paulo Ricardo. **O que são Scammers? Entenda a fraude**. Disponível em:https://ludgeroadvocacia.jusbrasil.com.br/artigos/883306590/o-que-sao-scammers-entendaa-fraude. Acesso em: 20 mar. 2023.

MITNICK, Kevin D.; SIMON, William L. **A Arte de Enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**. 2. ed. São Paulo: Alta Books, 2003.

NABUCO, José Filho. **ESTELIONATO.** Disponível em: https://josenabucofilho.com.br/home/direito-penal/parte-especial/estelionato/. Acesso em: 18 fev. 2023.

Nakamura, E. T.; Geus, P. L. **Segurança de Redes em Ambientes Cooperativos**. 1ª ed. São Paulo: Novatec, 2007.

NORTHCUTT, S.; et al. **Desvendando segurança em redes**. Rio de Janeiro: Editora Campus, 2002.

NOVAIS, Lucas Cardozo. **CRIMES CIBERNÉTICOS E SUA EVOLUÇÃO**. 2020.

PENA, Braian Henrique; SILVA, Anderson Santos; SANTOS, Maicon. **PHISHING. SEMINÁRIO DE TECNOLOGIA GESTÃO E EDUCAÇÃO**, v. 2, n. 2. 2020.

PINHEIRO, Patrícia Peck. **Regulamentação da Web**. Cadernos Adenauer XV. Rio de Janeiro. n.4, p. 20, out/2014. Disponível em: http://www.kas.de/wf/doc/16471-1442-5-30.pdf. Acesso em: 12 fev. 2023.

POZZEBOM, Rafaela. **Diferença entre: vírus, spam, spyware, worm, phishing, botnet, rootkit.** Oficina da net (oficinadanet). 2015. Disponível em: https://www.oficinadanet.com.br/post/12991-diferenca-entre-virus-spam-spyware-worm-phishing-botnet-rootkit. Acesso em: 25 fev. 2023.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **O problema na tipificação penal dos crimes virtuais**. Jus Navigandi, Teresina, ano 7, n. 60, 1 ago. 2002. Disponível em: https://jus.com.br/artigos/3186/o-problema-na-tipificacao-penal-dos-crimes-virtuais. Acesso em: 12 fev. 2023. LIMA, Renato Brasileiro. Manual de processo penal. 7. ed. rev., atual. e ampl. Salvador: JusPodivm, 2 v. 2019.

REPORT, S. **Brasil sofreu 103,16 bilhões de tentativas de ataques cibernéticos no ano passado**. São Paulo: Editora Security Report. 2023. Disponível em: https://www.securityreport.com.br/overview/brasil-sofreu-10316-bilhoes-de-tentativas-de-ataques-ciberneticos-em-2022. Acesso em: 02 de mar. 2023.

RIBEIRO, Eliete da Silva. **Crime de Estelionato – Uma análise da evolução sob a égide da impunidade na cidade de Manaus**. 2019. Disponível em: https://semanaacademica.org.br/system/files/artigos/crime_de_estelionato_-_uma_analise_da_evolucao_sob_a_egide_da_impunidade_na_cidade_de_manaus_eliete_da_silva_ribeiro_0.pdf. Acesso em: 08 jan. 2023.

ROHR, Altieres. **Banker - Linha Defensiva.** Paraná. 2012. Disponível em: https://linhadefensiva.org/2012/04/21/banker/. Acesso em: 04 de mar. 2023.

SERASA, **O que é SSL? Entenda a importância para a segurança do seu site**. São Paulo. 2021. Disponível em: https://serasa.certificadodigital.com.br/blog/ssl/o-que-e-ssl-entenda-a-importancia-para-a-seguranca-do-seu-site/. Acesso em: 02 de mar. 2023.

SILVA, Daniel. **Diferença Entre Estelionato e Extorsão (com exemplo**). Caderno de prova (cadernodeprova), 2020. Disponível em:< https://cadernodeprova.com.br/diferenca-entre-estelionato-e-extorsao-com-exemplo/. Acesso em: 08 jan. 2023.

SIQUEIRA, Marcela Scheuer. **Crimes virtuais e a legislação brasileira.** (Re)Pensando o Direito – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13 (2017). Disponível em: http://local.cnecsan.edu.br/revista/index.php/direito/article/view/468. Acesso em: 18 fev. 2023.

SOUZA, Luciano. **Código Penal Comentado**. São Paulo: Editora Revista dos Tribunais. 2022. Disponível em: https://thomsonreuters.jusbrasil.com.br/doutrina/secao/1728397420/art-157-roubo-codigo-penal-comentado-ed-2022. Acesso em: 26 fev. 2023.

TEIXEIRA, Tarcisio. **Direito Digital e Processo Eletrônico**. Saraivajur. 6. Ed. 2022.

WENDT, Emersson. JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos: Ameaçase procedimentos de investigação**. 2 ed. Rio de Janeiro. Editora Brasport, 2013.