PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

PROJETO DE TRABALHO DE CURSO I

ESTELIONATO VIRTUAL

ORIENTANDO: ARTHUR SIQUEIRA LOPES

ORIENTADORA: PROFA. DRA. CLAUDIA LUIZ LOURENÇO

GOIÂNIA-GO

2023

ARTHUR SIQUEIRA LOPES

ESTELIONATO VIRTUAL

Artigo Jurídico apresentado à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).

Orientadora: Dra. Cláudia Luiz Lourenço

GOIÂNIA-GO

2023

ARTHUR SIQUEIRA LOPES

ESTELIONATO VIRTUAL

Data da Defesa: 07 de junho de 2023

BANCA EXAMINADORA

_____

Orientador (a): Prof. (a): Dra. Claudia Luiz Lourenço Nota

_____

Examinador (a) Convidado (a): Prof. (a): Ms. Silvia Maria G. S. de L. S. Curvo Nota

SUMÁRIO

ESTELIONATO VIRTUAL

Arthur Siqueira Lopes[1]

RESUMO

Este artigo científico é um estudo sobre os crimes praticados em ambientes virtuais, com destaque para o crime de estelionato, abordando suas formas de punição e prevenção. O objetivo principal é compreender as principais características do crime virtual de estelionato, suas formas de atuação e como o direito brasileiro tem tratado essa questão. Para alcançar esse objetivo, foi utilizado o método de revisão bibliográfica, a partir de uma análise sistemática de artigos científicos, livros e legislações relacionadas ao tema. O estudo apontou que o estelionato virtual tem se tornado cada vez mais comum, principalmente por conta do aumento do uso da internet e da tecnologia, que possibilita que os criminosos ajam de forma mais sofisticada e discreta. No entanto, existem formas de punição e prevenção, previstas pelo direito brasileiro, para coibir essas práticas ilegais. Entre as formas de prevenção, destaca-se a educação e a conscientização da população sobre os riscos do uso da internet e a importância de proteger informações pessoais. As empresas também podem implementar medidas de segurança para garantir a privacidade de seus clientes e usuários. No âmbito da punição, existem leis que preveem penas para os criminosos virtuais, bem como a possibilidade de responsabilização das empresas que não adotarem medidas de segurança adequadas. Assim, é fundamental que as empresas, governo e sociedade civil estejam engajados na prevenção e combate aos crimes virtuais, por meio de investimentos em tecnologia e segurança, além da conscientização da população sobre os riscos e formas de prevenção. A pesquisa conclui que a revisão bibliográfica foi fundamental para entender as características do estelionato virtual e as formas de punição e prevenção previstas pelo direito brasileiro.

PALAVRAS-CHAVE: Crimes virtuais; Estelionato; Prevenção e punição;

ABSTRACT

This scientific article is a study on crimes committed in virtual environments, with a focus on the crime of fraud, addressing its forms of punishment and prevention. The main objective is to understand the main characteristics of virtual fraud, its forms of operation and how Brazilian law has dealt with this issue. To achieve this goal, the method of literature review was used, based on a systematic analysis of scientific articles, books, and legislation related to the topic. The study pointed out that virtual fraud has become increasingly common, mainly due to the increased use of the internet and technology, which allows criminals to act in a more sophisticated and discreet manner. However, there are forms of punishment and prevention, provided for by Brazilian law, to curb these illegal practices. Among the forms of prevention,

[1] Acadêmico do Curso de Direito da Pontifícia Universidade Católica de Goiás. Email:

education and awareness of the population about the risks of internet use and the importance of protecting personal information stand out. Companies can also implement security measures to ensure the privacy of their customers and users. In terms of punishment, there are laws that provide for penalties for virtual criminals, as well as the possibility of holding companies accountable that do not adopt adequate security measures. Thus, it is essential that companies, government, and civil society are engaged in the prevention and combat of virtual crimes, through investments in technology and security, as well as raising awareness of the population about the risks and forms of prevention. The research concludes that the literature review was essential to understand the characteristics of virtual fraud and the forms of punishment and prevention provided for by Brazilian law.

Keywords: Virtual crimes; Fraud; Prevention and punishment.

INTRODUÇÃO

A rápida e crescente evolução da tecnologia nos trouxe inúmeras vantagens como, por exemplo, o fácil acesso aos meios de comunicações, ferramentas para trabalho, estudos, ouvir músicas e até para fazer compras. Atualmente a internet está presente e se faz indispensável no cotidiano de grande parte da população mundial, o que acabou fazendo com que nos tornássemos reféns de máquinas e programas.

Fato é que esta evolução tecnológica que proporcionou muitos avanços positivos para a sociedade, também propiciou a utilização destes meios para a prática de condutas ilícitas denominadas em crimes cibernéticos.

Atualmente, é inúmera a quantidade de crimes praticados no ambiente virtual, tais como fraudes de cartões de crédito, desvio em contas bancárias, injúria, pedofilia, favorecimento a prostituição, dentre outros.

Um dos grandes problemas encontrados pelos operadores do direito consiste na adequação da legislação aos caracteres que diferenciam os crimes virtuais dos crimes presenciais, levando-se em conta as peculiaridades referentes à autoria, à materialidade e à tipificação de seus institutos.

Combater os crimes virtuais não é tarefa das mais fáceis quando a polícia tem à mão um Código Penal escrito em 1940, sendo assim, infelizmente, o Brasil necessitava de uma legislação eficaz que reprima estes crimes e de um aperfeiçoamento da polícia científica para identificar os indivíduos que atuam na obscuridade da internet.

Nesse sentido e objetivando adequar o direito às mudanças tecnológicas que transformam continuamente a sociedade, foi editada a Lei nº 12.737/2012, apelidada de Lei Carolina Dieckmann, que dispõe sobre a tipificação criminal de delitos informáticos, visando suprir o vácuo legislativo que anteriormente havia sobre o tema. Entretanto, a referida lei não resolveu todos os problemas. Os debates sobre crimes cibernéticos, reacendidos por meio de sua edição, devem ser retomados em busca de uma solução eficaz, tendo em vista que muitas condutas ainda não estão tipificadas na Lei, acarretando na impunidade dos criminosos.

Essa falta de impunidade tem sido o grande atrativo para os hackers. De acordo com um relatório da Norton Cyber Security, em 2017 o Brasil passou a ser o segundo país com maior número de casos de crimes cibernéticos, afetando cerca de 62 milhões de pessoas e causando um prejuízo de US$ 22 bilhões.

No ano anterior, o Brasil era o quarto colocado na lista, mas agora fica atrás apenas da China, que em 2017 teve um prejuízo de US$ 66,3 bilhões.

A grande maioria dos usuários da internet desconhece procedimentos de segurança, utilizam sistemas operacionais piratas, não atualizam o antivírus e deixam informações pessoais gravadas no HD. De posse destas informações, o hacker pode aproveitar-se delas para adquirir produtos via cartão de crédito, transferência bancária, chantagem e outras formas ilícitas de extorsão.

O interesse por esse assunto surgiu por se tratar de um tema atual e cada vez mais presente no cotidiano da sociedade, considerando que os crimes virtuais são cada vez mais comuns e as pessoas cultivam a sensação de que o ambiente virtual é uma terra sem Leis.

1 CONCEITOS DE CRIMES CIBERNÉTICOS

Segundo Ivete Senise Ferreira, crime de informática é “toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão” (apud ROSSINI, 2004, p. 104). A autora utiliza o conceito analítico de crime, mas com o foco voltado para a informática, verificando-se que o conceito seria o que já é conhecido mudando apenas o meio de praticar o crime.

Neil Barret, citado por Queiroz, apresenta uma definição de crimes digitais (Apud QUEIROZ, 2008, p. 173):

> Crimes digitais seriam todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados acessados ilicitamente ou utilizados para ameaçar ou fraudar; e para tais práticas sendo indispensável à utilização de um meio eletrônico.

Segundo Sérgio Marcos Roque (apud ROSSINI, 2004, p. 109): “Crime informático é conduta definida em lei como crime em que o computador tiver sido utilizado como instrumento para a sua perpetração ou consistir em seu objeto material”.

Na concepção de André Queiroz (QUEIROZ, 2008, p.174):

> […] Um delito típico de internet seria quando uma pessoa se utiliza de um computador acessando a rede, invade outro computador e obtém, destrói, ou altera um arquivo pertencente ao sistema, ainda que não havendo qualquer obtenção de vantagem patrimonial, mas tão somente a obtenção, destruição ou alteração de dados daquele sistema restrito – circunstância esta que já caracterizaria o tipo penal específico.

Nos conceitos acima citados de diversos doutrinadores é notável a variedade de definições para conceituar o crime informático. Alguns têm uma visão fechada e dizem que o crime cibernético é cometido por meio do computador, outros doutrinadores demonstram que o crime cibernético pode ser cometido por algum outro meio tecnológico, e formularam uma definição mais coerente.

Destarte, Crime informático, Crime cibernético, e-crime, Cibercrime, crime eletrônico ou crime digital são termos utilizados para se referir a toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, uma base de ataque ou como meio de crime. Referem-se a todos os delitos cometidos utilizando computadores ou internet, por

meio de uma rede pública, privada ou doméstica. Os objetivos desses crimes são diversos e variam de acordo com os interesses do infrator. Além disso, as formas de cometer também são diversas e podem atingir apenas um usuário, vários usuários ou inclusive um sistema de redes completo.

Assim, crimes cibernéticos possuem uma definição ampla e podem buscar atingir diretamente uma pessoa por meio da internet ou apenas o próprio computador do usuário. O criminoso, além disso, pode cometer vários crimes ao mesmo tempo e em diversos lugares ao mesmo tempo, utilizando diversos computadores.

Os crimes virtuais assemelham-se muito ao crime comum, ou definição de crime, tendo somente a diferença que o objeto utilizado para o êxito foi um computador ou algum sistema informatizado, onde essas características é que alguns autores classificam os crimes informáticos em subgrupos.

2 DA CLASSIFICAÇÃO E TIPICIDADE DOS CRIMES CIBERNÉTICOS

Existem várias classificações doutrinarias sobre a natureza jurídica dos crimes cibernéticos. Adotaremos, neste artigo, a vertente que divide os crimes em crimes cibernéticos próprios, impróprio, mistos e mediatos ou indiretos, por ser a vertente mais abrangente e detalhada.

2.1 Crimes cibernéticos próprios

Os crimes cibernéticos próprios são aqueles em que o agente, para cometer um delito, necessita do computador, ou seja, o computador é o meio de execução essencial. Nesse sentido:

> Ao contrário dos crimes cibernéticos impróprios, que envolvem o uso da tecnologia como instrumento para a prática de crimes tradicionais, os crimes cibernéticos próprios têm como objeto a infração direta a bens jurídicos relacionados à tecnologia, tais como dados eletrônicos, sistemas informatizados e outros recursos tecnológicos (SOUZA; OLIVEIRA, 2021, p. 10).

Nessa categoria de crimes está, não só a invasão de dispositivo informático, mas também os exemplos que segue:

A) São considerados crimes cibernéticos próprios a interferência em dados informatizados quando praticada por funcionário público no exercício de suas funções, conforme reza os artigos 313-A e 313-B do Código Penal Brasileiro (BRASIL, 1940):

> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:
> Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
> Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.
> Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.

B) Também é um crime cibernético próprio à interceptação ilegal, no qual os dados são capturados durante sua transferência de um dispositivo informático para outro. A conduta está tipificada na Lei nº 9.296/1996, que, em seu art. 10, dispõe:

> Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
> Pena: reclusão, de 2 (dois) a 4 (quatro) anos, e multa (BRASIL, 1940).

C) A criação e divulgação de programas de computadores destrutivos, que tem como principal representante os vírus informáticos. Esta conduta foi criminalizada, o que se deu no §1º do art. 154-A do CPB, “in verbis”:

> [...] §1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput (BRASIL, 1940).

2.2 Crimes cibernéticos impróprios

Os crimes informáticos impróprios são aqueles já puníveis em nossa legislação penal, cometidos através de meios informáticos, sem lesar dados ou informações, ou seja, a máquina em si é utilizada como instrumento para a realização das condutas ilícitas. Nesse sentido:

> Os crimes cibernéticos impróprios, também chamados de tradicionais em ambiente virtual, são aqueles em que a tecnologia é utilizada como instrumento para a prática de crimes já tipificados na legislação penal, tais como estelionato, falsidade ideológica, pornografia infantil, entre outros (ROSA, 2017, p. 67)

Não é raro a prática deste delito, tendo em vista que, na maioria das vezes, não é necessário que o autor tenha grande conhecimentos técnicos do uso de computadores para praticá-lo.

Exemplo clássico é o simples envio de um e-mail que permite não só a execução de delitos contra a honra (Calúnia - art. 138 do CPB, difamação - art. 139 do CPB, injúria - art. 140 do CPB), mas também o empreendimento dos crimes de induzimento, instigação ou auxílio ao suicídio (art. 122 do CPB), ameaça (art. 147 do CPB), violação de segredo profissional (art. 154 do CPB), incitação ao crime (art. 286 do CPB) e apologia de crime ou criminoso (art. 287 do CPB), entre outros.

Estes crimes também poderiam ser cometidos em salas de "bate papos", whatsapp, através de criação de página na Web, ou redes sociais.

Essa simplicidade de acesso à internet, junto com a facilidade de se criar publicações anônimas nas páginas criadas em servidores gratuitos, é responsável por uma grande quantidade de casos de publicação de fotos pornográficas de crianças na Internet, o que em nossa legislação é crime de pedofilia, previsto no art. 241-A do Estatuto da Criança e do Adolescente (ECA – Lei nº 8.069/1990).

Dentre os crimes informáticos impróprios previstos na legislação penal extravagante, que podem ser cometidos através da simples publicação de uma página na Internet, há ainda os de concorrência desleal (art. 195, da Lei nº 9.279/1996), violação de direito autoral (art. 12, da Lei nº 9.609/1998) e uma série de crimes eleitorais (art. 337, da Lei nº 4.737/1965).

Dentre os crimes informáticos impróprios praticados na Internet, destaca-se também o crime de estelionato (art. 171, do CPB), como exemplo as falsas páginas de lojas online, nas quais o agente efetua o pagamento, mas nunca recebe a mercadoria.

A prostituição também é muito explorada através de páginas na Internet, no qual há sites de anúncios oferecendo os serviços e disponibilizado foto de profissionais do sexo. Os visitantes das páginas podem contratar os serviços on-line o que, em tese, pode caracterizar os delitos de favorecimento da prostituição (art. 228, do CPB) já que as páginas facilitam o contato com os “clientes”, ou rufianismo (art. 230, do CPB), uma vez que o responsável pela página possivelmente receba comissão pelos contatos bem-sucedidos.

Esses crimes em sua maioria são cometidos por meio da internet, mas não necessariamente, conseqüentemente, a legislação brasileira em sua maioria não os trata como

crimes virtuais e sim como crime penal ao qual independente do meio utilizado para sua consumação, se for realizado, será enquadrado na lei penal em questão.

2.3 Crimes cibernéticos mistos

Já os crimes cibernéticos mistos “são aqueles em que o uso da internet ou sistema informático é condição sine qua non para a efetivação da conduta, embora o bem jurídico visado seja diverso ao informático”.

Conforme ROSSINI, 2002, p. 139 “Delitos informáticos mistos são aqueles “em que o computador é mera ferramenta para a ofensa a outros bens jurídicos que não exclusivamente os do sistema informático”.

Aqui o agente não visa o sistema de informática e seus componentes, mas a informática é instrumento indispensável para consumação da ação criminosa. Ocorre, por exemplo, nas transferências ilícitas de valores através do internet banking.

2.4 Crimes cibernéticos mediatos ou indiretos

Crime informático mediato ou indireto ocorre quando são praticados dois tipos penais distintos, sendo um com a finalidade de atingir o sistema informático (crime próprio) e o outro de natureza diversa. O crime com o intuito de atingir o sistema informático denomina-se como “delito-meio”, uma vez serviu como forma de consumar o “delito-fim” que, no caso, é o crime de natureza diversa.

Conforme Vianna, 2013, p. 35 “é o delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação.”

Vale ressaltar que esta classificação não se confunde com crime informático impróprio, visto que este apenas utiliza o sistema informático para a prática de um crime já tipificado no ordenamento jurídico, ou seja, não é necessário um crime-meio para consumação do delito.

Se alguém invade um dispositivo informático de um banco e transfere indevidamente dinheiro para sua conta, estará cometendo dois delitos distintos: o de invasão de dispositivo informático e o furto; o primeiro, crime informático, o segundo, patrimonial.

O delito de invasão de dispositivo informático será executado como crime-meio para que se possa executar o delito-fim que consiste na subtração da coisa alheia móvel. Desta forma, o agente só será punido pelo furto, aplicando-se ao caso o princípio da consunção. O crime-fim será classificado como informático mediato ou indireto quando, pela aplicação do principio da consunção, um crime-meio informático não for punido em razão da sua consumação.

Pode-se citar ainda como exemplo de delito informático mediato a invasão a dispositivo informático no qual conste um banco de dados de uma empresa de comércio eletrônico para a aquisição dos números de cartões de crédito dos clientes. O uso posterior destes números de cartões de crédito para a realização de compras na Internet constituiria um estelionato. Aplicar-se-ia o princípio da consunção e o agente seria punido tão somente pelo delito patrimonial.

3 O ESTELIONATO EM AMBIENTE VIRTUAL

O estelionato, também conhecido como fraude, é uma prática criminosa que envolve o engano e a obtenção de vantagens ilícitas por meio de informações falsas ou manipuladas. Com a crescente popularização da internet e das transações comerciais online, o estelionato realizado em ambientes virtuais tem se tornado cada vez mais comum e preocupante.

Os golpes virtuais podem ser realizados de diversas maneiras, como através de e-mails falsos, sites clonados, redes sociais, mensagens instantâneas e aplicativos de mensagens. Em geral, o criminoso utiliza técnicas de engenharia social para induzir a vítima a fornecer informações pessoais, como senhas, números de cartão de crédito e dados bancários.

> O engenheiro social procura obter informações da vítima ou empresa como, por exemplo, agenda de compromissos, dados de conta bancária, número de cartão de crédito a serem usados para o ataque. Nesse tipo de "crime", as pessoas podem aplicar protocolos de segurança recomendadas por especialistas; podem adquirir e instalar produtos de segurança e efetuar as configurações e atualizações indicadas para cada versão do hardware e/ou software destinadas às correções e aplicações dos devidos módulos de segurança. Vale ressaltar que, ainda assim, essas vítimas estarão suscetíveis às ameaças advindas da engenharia social (PEDROSO, 2019, p. 15).

Um dos golpes mais comuns é o phishing, que consiste em enviar e-mails falsos com links para sites falsos que se parecem com sites legítimos, como de bancos, lojas online ou empresas de serviços. A vítima, ao inserir seus dados pessoais, acaba fornecendo informações sensíveis para os golpistas, que podem utilizá-las para realizar compras fraudulentas, fazer saques em contas bancárias e até mesmo cometer crimes de identidade.

Nesse sentido:

> A engenharia social, de modo simples, tem como ênfase explorar as fragilidades do ser humano; ou seja, consiste na habilidade de obter informações ou o acesso indevido a determinados ambientes e/ou sistemas, utilizando para isso técnicas de convencimento e/ou espionagem. As técnicas de ataque são as mais variadas, sempre explorando a fragilidade e ingenuidade das pessoas. Nenhum artigo sobre ataques de engenharia social estaria completo sem citar o famoso e um dos maiores hackers de todos os tempos, Kevin Mitnick. Iguais a ele, atualmente existem muitos e as táticas utilizadas são basicamente as mesmas (PEDROSO, 2019, p. 37).

Outro golpe bastante comum é o do falso suporte técnico, onde o criminoso entra em contato com a vítima alegando que seu computador ou dispositivo está infectado com vírus ou com problemas técnicos, e oferece ajuda para solucionar o problema. Ao permitir o acesso

remoto ao seu dispositivo, a vítima acaba permitindo que o criminoso tenha acesso a suas informações e dados pessoais.

Para evitar cair em golpes virtuais, é importante adotar algumas medidas de segurança, como não fornecer informações pessoais para fontes desconhecidas, verificar a autenticidade de sites e e-mails recebidos, não clicar em links suspeitos e manter o sistema de segurança de seu dispositivo sempre atualizado.

Além disso, em caso de suspeita de fraude, é fundamental denunciar o crime às autoridades competentes e tomar medidas imediatas para evitar prejuízos maiores. A segurança na internet é uma responsabilidade de todos, e é importante estar sempre atento e informado para evitar cair em golpes e fraudes virtuais.

3.1 A CRIMINALIDADE VIABILIZADA PELAS NOVAS TECNOLOGIAS

As novas tecnologias têm transformado a forma como as pessoas se comunicam, trabalham e se relacionam, mas também têm possibilitado novas formas de criminalidade. Com a internet e a conectividade em alta velocidade, as oportunidades para crimes virtuais se multiplicaram, tornando-se cada vez mais sofisticados e difíceis de serem detectados. Nesse sentido:

> A Internet possibilitou que indivíduos situados em diferentes pontos do globo se comuniquem instantaneamente e efetuem transações comerciais e financeiras sem a necessidade de contato físico, o que tornou o ambiente virtual propício ao cometimento de fraudes, crimes cibernéticos e ataques a sistemas e informações. (MARTINS, 2018, p. 43)

Nesse mesmo sentido:

> A internet é um espaço aberto e sem fronteiras, no qual é possível a realização de diversos tipos de atividades ilícitas sem a necessidade de um espaço físico para sua concretização. Esse ambiente virtual propicia a criação de redes de criminosos que atuam globalmente, dificultando a investigação e a repressão dos crimes cibernéticos (SCARPELINI; MARÇAL, 2018, p. 23).

Entre as principais formas de criminalidade viabilizadas pelas novas tecnologias estão os ataques virtuais, como o phishing, a clonagem de cartões de crédito, a invasão de sistemas e o roubo de dados pessoais. Esses crimes podem ser cometidos por indivíduos ou grupos

organizados que utilizam técnicas avançadas de engenharia social para enganar suas vítimas e obter informações sensíveis (SCARPELINI; MARÇAL, 2018)

Além disso, as redes sociais também têm sido utilizadas para a prática de crimes, como a divulgação de conteúdo ilegal, o assédio virtual, o cyberbullying e a disseminação de notícias falsas. A facilidade de disseminação de informações na internet também tem permitido que criminosos se organizem para a prática de crimes em grupo, como o tráfico de drogas e armas, a lavagem de dinheiro e o terrorismo.

As novas tecnologias também têm possibilitado a criação de novos tipos de crimes, como o cibercrime, que inclui a invasão de sistemas e o roubo de informações, e o crime digital, que abrange a violação de direitos autorais, a pirataria e o acesso ilegal a conteúdos protegidos por lei.

Para combater a criminalidade viabilizada pelas novas tecnologias, é preciso investir em tecnologias e políticas de segurança, além de conscientizar a população sobre os riscos da internet e a importância de proteger suas informações pessoais. As empresas também precisam adotar medidas de segurança para proteger seus dados e informações confidenciais, além de treinar seus funcionários para evitar que informações sensíveis sejam divulgadas.

Em resumo, a criminalidade viabilizada pelas novas tecnologias é uma realidade que precisa ser enfrentada de forma urgente e eficaz. A tecnologia pode ser uma ferramenta poderosa para a prevenção e a investigação de crimes, mas também pode ser utilizada para a prática de crimes graves. Cabe a todos nós, como cidadãos e usuários da internet, fazer nossa parte para garantir um ambiente digital mais seguro e confiável.

3.2 O *MODUS OPERANDI* DO CRIMINOSO VIRTUAL

A internet se tornou um campo fértil para a atuação de criminosos, que utilizam as tecnologias para cometer fraudes, invadir sistemas e roubar informações. Os criminosos na internet são conhecidos como cibercriminosos e agem de diversas formas para obter vantagens ilícitas. Nesse sentido:

> Os criminosos virtuais são indivíduos perspicazes, dotados de grande habilidade técnica e de capacidade para explorar as vulnerabilidades existentes nos sistemas de segurança da informação, bem como as fragilidades das pessoas, tais como a

> confiança excessiva e a falta de conhecimento sobre os riscos da internet. (MILAGRE, 2016, p. 31)

Uma das principais formas de atuação dos criminosos na internet é através do *phishing*, que consiste em enviar e-mails que aparentam ser de empresas ou instituições conhecidas, como bancos, redes sociais ou serviços de comércio eletrônico. Esses e-mails possuem links que levam a páginas falsas que imitam as páginas originais, e o objetivo é obter informações pessoais e senhas dos usuários, que são utilizados posteriormente para realizar compras fraudulentas ou até mesmo cometer crimes de identidade.

Outra forma de atuação dos criminosos na internet é através de malwares, que são softwares maliciosos que podem ser instalados em computadores ou dispositivos móveis. Esses malwares podem roubar informações, controlar a câmera e o microfone do dispositivo, ou até mesmo criptografar os dados do usuário, exigindo o pagamento de um resgate para liberá-los.

Os criminosos também utilizam técnicas de engenharia social para persuadir as pessoas a fornecer informações sensíveis ou instalar softwares maliciosos em seus dispositivos. Eles podem se passar por amigos, familiares ou instituições de confiança, utilizando informações pessoais disponíveis na internet para parecerem mais convincentes.

Para se proteger dos criminosos na internet, é fundamental adotar medidas de segurança, como utilizar antivírus e softwares de proteção em todos os dispositivos, verificar a autenticidade dos sites e e-mails recebidos, e nunca fornecer informações pessoais ou senhas para fontes desconhecidas.

CONCLUSÃO

Os crimes cometidos em ambientes virtuais, especialmente o estelionato, têm se mostrado cada vez mais frequentes e sofisticados, representando uma ameaça crescente à segurança das pessoas e das empresas. O estelionato virtual é caracterizado pela obtenção fraudulenta de informações pessoais e financeiras, com o objetivo de realizar transações indevidas em nome da vítima.

No âmbito do direito brasileiro, existem diversas formas de prevenção e combate ao estelionato virtual. Uma das principais medidas é a conscientização da população sobre os riscos e cuidados a serem tomados ao navegar na internet, evitando compartilhar informações pessoais e financeiras com terceiros ou em sites suspeitos.

Além disso, a legislação brasileira prevê penas severas para os crimes virtuais, como o estelionato, com a aplicação de multas e até mesmo a prisão dos envolvidos. O poder público tem atuado de forma proativa no combate a esses crimes, por meio de ações de fiscalização, investigação e punição dos infratores.

Uma das medidas adotadas pelo poder público é a criação de unidades especializadas em crimes virtuais, como a Delegacia de Repressão aos Crimes de Informática (DRCI) e a Divisão de Crimes Cibernéticos da Polícia Federal. Essas unidades têm como objetivo investigar e coibir a prática de crimes virtuais, como o estelionato, além de orientar a população sobre as melhores práticas de segurança na internet.

Em conclusão, o estelionato virtual é um crime grave que pode causar prejuízos financeiros e emocionais para as vítimas. No entanto, existem medidas de prevenção e combate eficazes que podem ser adotadas, tanto pela população quanto pelo poder público. É fundamental que todos estejam atentos aos riscos e adotem medidas de proteção para garantir a segurança no ambiente virtual.

Além das medidas de prevenção e combate já mencionadas, o direito brasileiro também prevê a responsabilidade civil das empresas e provedores de serviços que não tomarem medidas para garantir a segurança dos dados de seus usuários. Isso significa que as empresas podem ser responsabilizadas judicialmente caso não adotem medidas de segurança eficazes e ocorram crimes virtuais contra seus usuários.

Dessa forma, é importante que as empresas e provedores de serviços invistam em tecnologias e processos que garantam a segurança das informações de seus usuários, bem como

que ofereçam orientação e suporte para que seus usuários possam utilizar seus serviços de forma segura.

Por fim, é fundamental que a sociedade como um todo esteja engajada no combate aos crimes virtuais, por meio da denúncia de suspeitas de atividades ilegais e da conscientização sobre a importância da segurança na internet. Com a atuação conjunta de governo, empresas e sociedade civil, é possível reduzir os casos de estelionato virtual e garantir um ambiente digital mais seguro e confiável para todos.

REFERÊNCIAS

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Diário Oficial da União, Brasília, DF, 31 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 04 abr. 2023

_____. Lei nº 9.296, de 24 de julho de 1996. **Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal**. Diário Oficial da União, Brasília, DF, 25 jul. 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9296.htm. Acesso em: 04 abr. 2023.

DE AZEVEDO NUNES, Mário Vinicius; MADRID, Fernanda de Matos Lima. CRIMES VIRTUAIS: O DESAFIO DO CÓDIGO PENAL NA ATUALIDADE E A IMPUNIDADE DOS AGENTES. **ETIC-ENCONTRO DE INICIAÇÃO CIENTÍFICA-ISSN 21-76-8498**, v. 15, n. 15, 2019. Disponível em: <http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7895>. Acesso em: 26 set 2022.

HOFFELDER, Juliana Toffolo; DE CASTRO, Matheus Felipe. ESTELIONATO ELETRÔNICO: Necessidade de Tipificação Legal?. **Anuário Pesquisa e Extensão Unoesc São Miguel do Oeste**, v. 3, p. e19789-e19789, 2018. Disponível em: <https://unoesc.emnuvens.com.br/apeusmo/article/view/19789>. Acesso em: 26 set 2022.

MACHADO, Daniela Regina Gabriel; GROTT, Sérgio. Estelionato virtual. **Revista Científica Multidisciplinar do CEAP**, v. 4, n. 1, p. 10-10, 2022. Disponível em: <http://periodicos.ceap.br/index.php/rcmc/article/view/149>. Acesso em: 26 set 2022.

MILAGRE, José Antonio. **Crime Digital**: Investigação e Prova no Processo Penal. São Paulo: Atlas, 2016.

OLIVEIRA, Hesrom César de. **Cybercrimes:** do Estelionato Virtual. 2020. Disponível em: <http://45.4.96.19/handle/aee/17815>. Acesso em: 26 set 2022.

ROSA, F. S. **Crimes Cibernéticos**: Aspectos Penais e Processuais. São Paulo: JH Mizuno, 2017.

SCARPELINI, João Pedro; MARÇAL, Vinícius. **Direito Penal na Era Digital**. São Paulo: Thomson Reuters Brasil, 2018.

SOUZA, L. R.; OLIVEIRA, J. R. **Crimes cibernéticos**: análise de casos e desafios para a investigação policial. Revista de Direito, Tecnologia e Inovação, São Paulo, v. 8, n. 2, p. 5-22, jul./dez. 2021.