PREVENÇÃO AOS CRIMES CIBERNÉTICOS: ESTELIONATO ELETRÔNICO

Andressa Kelle Alves
UniProcessus – Centro Universitário Processus, DF, Brasil
E-mail: kelledf@gmail.com
Cláudia Cristina Caixeta de Sousa
UniProcessus – Centro Universitário Processus, DF, Brasil
E-mail: claudiacaixeta@gmail.com
Elisabeth Cristiane de Medeiros Alves Silva
UniProcessus – Centro Universitário Processus, DF, Brasil
E-mail: bethvet24@yahoo.com.br
Emile Carla Ribeiro da Silva
UniProcessus – Centro Universitário Processus, DF, Brasil
E-mail: emilecarla605@gmail.com
João de Souza Santos
UniProcessus – Centro Universitário Processus, DF, Brasil
E-mail: joaoss.direito@gmail.com
Maria Amélia Mazzola
UniProcessus – Centro Universitário Processus, DF, Brasil
E-mail: mariaameliamazzola09@gmail.com
Milena de Souza Coutinho
UniProcessus – Centro Universitário Processus, DF, Brasil
E-mail: milena.coutinho@outlook.com.br

Resumo

A presente pesquisa teórica foi realizada com o objetivo de embasar a atividade extensionista que será realizada no âmbito da disciplina "Direito Digital", sob a orientação do Prof. Dr. Henrique Savonitti Miranda.

O presente estudo buscará abordar a temática do estelionato eletrônico, realizado via meios digitais.

O uso das novas tecnologias traz uma série de facilidades, porém, ela vem acompanhada de alguns inconvenientes, no caso aqui tratado, uma espécie de crime digital, que utiliza esse meio para o cometimento de ilícitos. Então, o grupo tomou como importante aclarar e conscientizar a comunidade a respeito do crime de estelionato eletrônico e apresentar medidas preventivas que ajudam os cidadãos a serem mais conhecedores de como usar o meio digital com mais cautela e, por conseguinte, previdência, para que possam perceber certas formas de simulação de negociações que na verdade se revelam maliciosas, levando a prejuízos financeiros dos cidadãos.

Essa pesquisa servirá de referencial teórico para a execução de material informativo, na modalidade de panfletos, para a comunidade externa à Uniprocessus, com um olhar mais direcionado ao público mais vulnerável, quais sejam, as mulheres, os idosos e os adolescentes. A maior suscetibilidade de tais grupos encontra-se

registrada no Anuário Brasileiro de Segurança Pública de 2023, a partir de levantamento feito entre 2018 e 2022.

Por fim, entende-se, dessa forma, poder despertar na população que acessa os mais diversos meios digitais, a adoção de medidas preventivas simples, porém eficazes, evitando-se, assim, tornar-se vítima de crimes de estelionato digital.

1. Introdução

O estelionato eletrônico, também conhecido como golpe ou fraude eletrônica, é uma forma de crime cibernético que envolve a obtenção fraudulenta de informações pessoais, financeiras ou confidenciais de indivíduos ou organizações por meios eletrônicos. A crescente dependência da sociedade em relação à tecnologia e à internet tem facilitado o aumento da ocorrência desse tipo de fraude, cada vez mais sofisticada e ampla.

A relevância do tema, atualmente, explica-se em razão do papel crescente que a tecnologia desempenha em nossas vidas, tanto pessoal, quanto profissional. A dependência tecnológica vivenciada em uma era altamente digitalizada, na qual muitas transações e interações ocorrem online. Isso torna as pessoas e as organizações mais suscetíveis a ameaças cibernéticas, incluindo o estelionato eletrônico.

O aumento das transações online cria oportunidades para criminosos explorarem vulnerabilidades e enganarem as vítimas. A natureza globalizada da internet permite que criminosos operem virtualmente em qualquer lugar do mundo, tornando a identificação e a punição mais complexas. Falhas na proteção de dados pessoais expõem os indivíduos e as organizações, tornando-os alvos fáceis para as mais diversas modalidades de golpe digital. (BIASOLI, Luiz Carlos. Da necessidade de tipificação do crime de estelionato praticado na internet. Conteúdo Jurídico. 23 jan. 2010. Disponível em: https://conteudojuridico.com.br/consulta/Monografias-TCC-Teses-E-Book/19147/da-necessidade-de-tipificacao-do-crime-de-estelionato-praticado-na-internet. Acesso em: 28, ago. 2023)

Buscando atender aos anseios da sociedade diante no novo delito, o Código Penal teve seu texto alterado pela Lei nº 14.155 de 2021, para que houvesse o acréscimo ao art. 171 que trata do crime de estelionato, o §2º-A, o §2º-B e o §4º, que

trouxeram a tipificação do crime de Fraude Eletrônica na referida norma, identificando-o como sendo “(...) a fraude 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 (...)”, além de trazer as majorantes a serem aplicadas nos mais diversos casos e a preocupação com as vítimas idosas ou vulneráveis, visando coibir crimes virtuais. (BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1851-1899/d847.htm. Acesso em: 28, ago. 2023)

As táticas utilizadas no estelionato eletrônico são variadas e evoluem constantemente. Isso pode envolver o envio de e-mails de phishing convincentes, criação de sites falsos, uso de malware para capturar informações ou até mesmo manipulação psicológica das vítimas por meio de engenharia social. Os criminosos frequentemente se fazem passar por entidades legítimas, como bancos, empresas ou até mesmo conhecidos, para enganar as vítimas e obter acesso a informações sensíveis. Isso pode incluir dados bancários, senhas, números de cartão de crédito, informações de identificação pessoal e outros dados que possam ser usados para obter vantagens financeiras ilícitas. (Lei endurece penas para crimes eletrônicos, como clonagem do WhatsApp e outros golpes via internet. 28, mai. 2021. Disponível em: https://portal.febraban.org.br/noticia/3631/pt-br. Acesso em: 28, ago. 2023)

As consequências do estelionato eletrônico são significativas, resultando não apenas em perdas financeiras para as vítimas, mas também em danos à privacidade, à confiança nas transações online e ao sentimento de segurança digital. Para combater esse tipo de crime, é essencial que os indivíduos estejam cientes das táticas utilizadas pelos golpistas, adotem medidas de segurança cibernética e reportem atividades suspeitas às autoridades competentes.

O impacto financeiro e emocional causado nas vítimas de estelionato eletrônico pode ser avassalador, refletindo-se em perdas financeiras significativas, além de estresse emocional e psicológico decorrentes da violação da privacidade e da confiança. Por essa razão, o presente trabalho tem por objetivo apresentar a prevenção como medida crucial no combate ao estelionato eletrônico. Educar as pessoas sobre como identificar golpes, proteger suas informações e adotar práticas

seguras é fundamental. A conscientização sobre o crime, a adoção de práticas de segurança cibernética e a colaboração entre indivíduos, empresas e governos são essenciais para mitigar os riscos e proteger nossos ativos digitais e informações pessoais. (MOREIRA, Paulo. Estelionato praticado por meio da internet: Uma visão acerca dos crimes digitais. 16, fev. 2022. Migalhas. Disponível em: https://www.migalhas.com.br/depeso/359821/estelionato-praticado-por-meio-da-internet. Acesso em: 28, ago. 2023)

Dentre as boas práticas de segurança cibernética amplamente reconhecidas, formuladas por organizações de segurança cibernética, especialistas em tecnologia e governos, que promovem a conscientização e a proteção contra ameaças online, que podem ser adotadas estão:

- a educação e a conscientização da população acerca dos tipos comuns de golpes eletrônicos e das táticas utilizadas pelos criminosos;
- o uso de senhas únicas e fortes para suas contas online, evitando as senhas óbvias;
- ativação da autenticação de dois fatores sempre que possível, adicionando, assim, uma camada extra de segurança, exigindo uma segunda forma de verificação além da senha;
- a verificação da legitimidade de e-mails, mensagens ou sites antes de fornecer informações pessoais ou financeiras, sempre devendo desconfiar de solicitações urgentes ou mensagens não solicitadas que peçam informações confidenciais;
- atentar-se para links de e-mails suspeitos ou desconhecidos, protegendo-se contra Phishing;
- manter sistema operacional, navegadores e programas atualizados com as últimas correções de segurança;
- instalar e manter atualizados programas de antivírus e firewalls para proteger seu dispositivo contra malware;
- evitar fazer transações financeiras ou inserir informações confidenciais em redes Wi-Fi públicas ou não seguras;
- não compartilhar informações pessoais ou financeiras por e-mail, mensagem ou telefone, a menos que tenha certeza da legitimidade da solicitação;

- monitorar suas contas bancárias, cartões de crédito e atividades online regularmente em busca de atividades suspeitas e realizar backups regulares de seus dados importantes e mantenha-os em locais seguros. (Segurança em primeiro lugar: Como se proteger contra fraudes na internet. Autentify. 20, mai. 2023. (Disponível em: https://www.autentify.com.br/antifraude/seguranca-em-primeiro-lugar-como-se-proteger-contra-fraudes-na-internet/ Acesso em: 28, ago. 2023)

Vale destacar que a prevenção é uma prática contínua e permitirá o melhor preparado para se proteger contra o estelionato eletrônico e outras ameaças cibernéticas.

2. Estelionato Eletrônico: Formas de Prevenção

Nas palavras de Ataíde (2017): “ocorre crime de estelionato virtual quando os infratores criam links, e-mails, etc., falsos, com o objetivo de não ser identificado e consequentemente prometem fazer algo que sabem não ser possível fazer, mas fazem a promessa em troca de alguma vantagem que em grande parte das vezes é pecuniária”.

Conforme Freitas (2009), “o mundo virtual oferece inúmeras vantagens aos usuários no momento de realizar uma compra. É possível comprar os mais diversos produtos, sem sair de casa, apenas com poucos cliques e a preços mais baixos. Em razão disso comprar pela internet se torna bem conveniente para o comprador, contudo nem sempre isso ocorre”. Nos dias atuais a internet tem proporcionado a simplificação de tarefas, o ato de comprar algo, por exemplo, hoje pode ser executado em poucos cliques e com valores menores, como assevera a autora, contudo a mesma alerta que o espaço não é tão segura como se espera, pois, pessoas mal-intencionadas podem se valer dessas facilidades para causar dano ao próximo.

Uma das formas mais frequentes de estelionato virtual é a invasão do correio eletrônico da vítima, especialmente aquelas que têm o costume de consultar saldos e extratos bancários pelo computador. Nesse caso em específico, o estelionatário encontra uma maneira de clonar a página da internet banking e fazer com que a vítima tente fazer o acesso a conta, sem saber que o dano inserido na dita página será interceptado por um terceiro de má-fé.

Outro tipo bem comum é praticado por pessoas de menor saber informático, os quais se utilizam de crenças populares ou correntes de sorte, para que ao final a vítima deposite determinada importância em dinheiro para que obtenha aquilo que foi veiculado, sendo garantido a esta que ao adquirir o almejado a importância lhe será devolvida, fato que não ocorre (FEITOZA, 2012).

Forma típica de estelionato no ciberespaço, é, portanto, conforme a citação acima, aquela que se dá quando a pessoa invade o correio eletrônico da vítima, em especial aquelas que costumam consultar saldos e extratos bancários pelo computador. No caso em questão o estelionatário se vale de medidas para clonar a página legítima do usuário e fazê-lo acreditar que se encontra no local correto, e acreditando nisso inserir os dados de acesso. Outra forma bem comum, como salienta o autor é executado por pessoas de menor conhecimento de informática, e que vêm a se utilizar de corrente de sorte e de crenças populares encaminhando diversos e-mails para as pessoas que tem a possibilidade de serem persuadidas por aquilo, neste momento eles contam uma história breve e pedem depósitos prévios em dinheiro, para que algo lhes seja realizado, além de garantir o reembolso do dinheiro acaso o prometido não ocorra.

Aliás, tem sido bem comum que pessoas sejam vítimas de golpes de estelionatários na internet (FREITAS, 2009). Percebe-se, pois, que cada vez é mais frequente a prática de estelionato virtual, o que se deve principalmente como já analisado, ao avanço da tecnologia e popularização da internet.

De acordo com Junior (2008), “comete crime de estelionato aquele que cria página em ambiente virtual ou faz anúncios em sites, simulando por exemplo, a venda de produtos com o objetivo de induzia a vítima em erro para que essa efetue pagamento antecipado para a compra de produtos, na ilusão de que irá recebe-los posteriormente, quando, em verdade, se trata de um golpe empregado pelo agente para obter vantagem indevida, aproveitando-se da boa-fé de pessoas para enganá-las e provocar prejuízo patrimonial a elas”.

> 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 1 (um) a 5 (cinco) anos, e multa. 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. Estelionato contra idoso ou vulnerável § 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).

O caput do artigo 171 do Código Penal Brasileiro dispõe que o crime de estelionato é praticado através de meio ardil, artifícios, meios fraudulentos, manter o sujeito passivo em erro para assim conseguir vantagem ilícita.

Cezar Roberto Bitencourt, interpreta o crime de estelionato desta forma: “A característica fundamental do estelionato é a fraude, utilizada pelo agente para induzir ou manter a vítima em erro, com a finalidade de obter vantagem patrimonial ilícita. No estelionato, há dupla relação causal: primeiro, a vítima é enganada mediante fraude, sendo esta 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. (BITENCOURT, 2015, p. 836)”.

E ainda menciona os requisitos fundamentais para a configuração do crime de estelionato: “1) emprego de artifício, ardil ou qualquer outro meio fraudulento; 2) induzimento ou manutenção da vítima em erro; 3) obtenção de vantagem patrimonial ilícita em prejuízo alheio (do enganado ou de terceiros).” (BITENCOURT 2015, p. 836).

De acordo com Júlio Fabbrini Mirabete, “o emprego meio artifício, é quando o sujeito passivo muda o aspecto material da coisa. O artifício existente quando o agente se utiliza de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes efeitos de luz, etc. (MIRABETE, 2003, p. 1348)”.

> O meio artifício de uma forma mais simples, “é toda simulação ou dissimulação idônea para induzir uma pessoa em erro, levando-a à percepção de uma falsa aparência da realidade;”. No que tange ao meio ardil o mesmo autor, conceitua este como “a trama, o estratagema, a astúcia; qualquer outro meio fraudulento é uma fórmula genérica para admitir qualquer espécie de fraude que possa enganar a vítima. (Bitencourt 2015, p. 836).

Levando-se em conta também a gravidade que implicam os delitos informáticos, é necessário que o Código Penal inclua figuras delitivas que contenham os crimes de computador, já que a consequência direta de não fazê-lo será a ausência de figuras concretas que possam ser aplicadas nessa matéria, o que pode levar à ausência de punição aos autores desses fatos, ou a obrigar os tribunais a aplicarem

preceitos que não se ajustem de forma perfeita à natureza dos fatos cometidos (LIMA, 2015, p.4)

Veja como Cezar Roberto Bitencourt leciona sobre esta interpretação do princípio da legalidade:

> O princípio da legalidade ou da reserva legal constitui efetiva limitação ao poder punitivo estatal. Feuerbach, no início do século XIX, consagrou o princípio da reserva legal por meio da fórmula latina nullum crimen, nulla poena sine lege. O princípio da reserva legal é um imperativo que não admite desvios nem exceções e representa uma conquista da consciência jurídica que obedece a exigências de justiça; somente os regimes totalitários o têm negado (BITENCOURT, 2015, p. 109).

Nesse norte, é necessário também três requisitos essenciais para a composição do fato típico, ou seja, o crime deve ser típico, ilícito e culpável. Ademais, entre a conduta e o dano deve haver o nexo causal. Rogerio Greco, de forma didática explica a respeito do nexo de causalidade: O nexo causal, ou relação de causalidade, é aquele elo necessário que une a conduta praticada pelo agente ao resultado por ela produzido. Se não houver esse vínculo que liga o resultado à conduta que levada a efeito pelo agente, não se pode falar em relação de causalidade e, assim, tal resultado 34 não poderá ser atribuído ao agente, haja vista não ter sido ele seu causador. (GRECO, 2018, p.294).

Guilherme Feitoza demonstra como ocorre o estelionato no modo virtual: “Uma das formas mais recorrentes do estelionato no ciberespaço é a invasão do correio eletrônico da vítima, em particular, o daquelas pessoas que possuem o costume de consultar seus saldos e extratos bancários pelo computador”.

Nesta situação, o estelionatário (crackler) encontra alguma maneira de clonar a página legítima da internet banking do usuário e fazer com que ele tente fazer o acesso, sem saber que os dados que estão sendo inseridos serão interceptados por um terceiro de má-fé que irá usá-los indevidamente (FEITOZA, 2012, p. 48).

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, p. 325)”.

Atuais são as palavras de Pinochet (2016) 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, 2016)”.

Ademais, cabe trazer a atual jurisprudência do Egrégio Tribunal de Justiça do Distrito Federal e Territórios acerca do assunto, in verbis:

> **CIVIL. PRESTAÇÃO DE SERVIÇO TELEFÔNICO. FALHA: USURPAÇÃO DA LINHA TELEFÔNICA UTILIZADA PELA PARTE CONSUMIDORA (BLOQUEIO) E VIOLAÇÃO DA PRIVACIDADE MEDIANTE ACESSO AOS DADOS EXTRAÍDOS DE SUA REDE SOCIAL NO "WHATSAPP", A PONTO DE PERMITIR O COMETIMENTO DE FRAUDES POR TERCEIROS (ESTELIONATO CIBERNÉTICO).** DANO MORAL CONFIGURADO (LEI 8.078/90, ARTIGO 14, "CAPUT"; LEI 12.965/14, ARTIGO 7º C/C CÓDIGO CIVIL, ARTIGO 186): VALOR QUE NÃO VIOLA O PRINCÍPIO DE PROIBIÇÃO DE EXCESSO. RECURSO IMPROVIDO. I. Rejeitada a preliminar de ilegitimidade passiva, porquanto exsurge, à luz da narrativa da inicial, a pertinência subjetiva para que a ora recorrente figure no polo passivo da demanda (suposta fraude praticada por terceiros), de sorte que a aferição da responsabilidade da recorrente constitui matéria afeta à questão de fundo. II. Mérito: A. A questão de direito material deve ser dirimida à luz das normas protetivas do CDC (artigos 6º e 14). B. Ação ajuizada pelos consumidores (ora recorridos), em desfavor de CLARO S.A., com vistas à compensação dos danos morais

decorrentes de "estelionato virtual". Recurso contra a sentença de procedência dos pedidos (condenação da empresa ao pagamento de R$ 2.000,00 a título de danos extrapatrimoniais, para cada requerente). C. No caso concreto, incontroversa a falha na prestação dos serviços (ofensa ao dever de segurança - CDC, art. 14, § 1º), que culminou na usurpação (e bloqueio) da linha telefônica da parte consumidora e na violação de sua privacidade, em função do acesso aos dados extraídos de sua rede social no "WhatsApp", a ponto de permitir o cometimento de fraudes por terceiros que se fizeram passar pela parte requerente em sua própria rede social (estelionato virtual). D. No ponto, como bem salientado na sentença ora revista, a parte ré não se desincumbiu do ônus de demonstrar a segurança que se espera na utilização dos serviços telefônicos e no uso dos aplicativos de celular, permitindo que terceiros fraudadores realizassem a clonagem da linha telefônica do requerente, tivessem fácil acesso aos aplicativos, procedessem a operações bancárias na conta do autor e deixassem os serviços indisponíveis. E. E, no particular, os transtornos e aborrecimentos experimentados pelos consumidores causados diretamente pela defeituosa prestação de serviços da empresa de telefonia, que deixou de oferecer a segurança que deles pudesse esperar a parte consumidora (CDC, art. 14, § 1º), superam a esfera do mero aborrecimento e subsidiam a pretendida compensação por danos extrapatrimoniais (CF, art. 5º, V e X e CC, art. 186). Precedente: TJDFT, 3ª Turma Recursal dos Juizados Especiais, acórdão 1008535, DJE 10.4.2017. F. Escorreita, pois, a condenação da empresa à compensação por danos extrapatrimoniais, proporcionalmente fixados em R$ 2.000,00 para cada requerente, montante suficiente a compensar os dissabores decorrentes da referida violação

> (clonagem e habilitação do chip em outro aparelho celular; ofensa à intimidade, privacidade e honra; acesso não autorizado à conta bancária, e realização de operações financeiras; situação externa vexatória perante pessoas próximas das quais foram solicitadas a realização de transferências de valores), sem violar o princípio de proibição de excesso. III. Rejeitada a preliminar. Recurso conhecido e improvido. Sentença confirmada por seus fundamentos. Condenada a recorrente ao pagamento das custas processuais e dos honorários advocatícios, estes fixados em 10% do valor da condenação (Lei 9.099/95, arts. 46 e 55). (Acórdão 1338914, 07142532220208070020, Relator: FERNANDO ANTONIO TAVERNARD LIMA, Terceira Turma Recursal, data de julgamento: 12/5/2021, publicado no DJE: 19/5/2021. Pág.: Sem Página Cadastrada.)

Neste sentido, o cometimento de crimes cibernéticos é uma realidade a ser enfrentada com todos os meios educativos possíveis, visto que está amplamente documentada em julgados sobre a temática, cabendo, para tanto, a divulgação das formas de se evitar esse crime.

3. Considerações Finais

A presente pesquisa teve por objetivo analisar a temática do estelionato eletrônico, cujos meios de realização ocorre por via digital.

Conforme se pode observar a cada dia que passa esse tipo de ilícitos vem trazendo uma série de problemáticas para a sociedade, tornando-se cada vez mais usuais.

Foi demonstrado que a melhor forma de combater esses abusos cometidos contra o cidadão, em especial àqueles grupos mais vulneráveis da sociedade que estão mais alheios às formas de utilização da tecnologia, é conscientizando a comunidade, com medidas preventivas que possibilitarão uma melhor compreensão de como são essas “armadilhas digitais” e quais as estratégias para não ser vítima delas.

Para então, tornar os cidadãos mais conhecedores de como usar o meio digital com mais cautela e, por conseguinte, precaver, para que saibam reconhecer uma possível tentativa de golpe e\ou certas formas de simulação de negociações que na verdade se revelam maliciosas, levando a prejuízos financeiros dos cidadãos.

Referências Bibliográficas

ATAÍDE, Amanda Albuquerque de. **Crimes Virtuais: uma análise da impunidade e dos danos causados às vítimas**. Maceió, 2017. Disponível em:< http://www.faaiesa.edu.br/aluno/arquivos/tcc/tcc_amanda_ataide.pdf>. Acesso em: 20, ago. 2023.

AUTENTIFY. **Segurança em primeiro lugar: Como se proteger contra fraudes na internet**. Autentify. 20, mai. 2023. Disponível em: https://www.autentify.com.br/antifraude/seguranca-em-primeiro-lugar-como-se-proteger-contra-fraudes-na-internet/ Acesso em: 28, ago. 2023.

BITENCOURT, Cezar Roberto. **Código Penal Comentado**. 7 ed. São Paulo: Saraiva, 2015.

BIASOLI, Luiz Carlos. **Da necessidade de tipificação do crime de estelionato praticado na internet.** Conteúdo Jurídico. 23 jan. 2010. Disponível em: https://conteudojuridico.com.br/consulta/Monografias-TCC-Teses-E-Book/19147/da-necessidade-de-tipificacao-do-crime-de-estelionato-praticado-na-internet. Acesso em: 28, ago. 2023.

BRASIL. Conselho Nacional de Justiça. **CNJ Serviço: qual a diferença entre crime e contravenção?** Disponível em:< https://www.cnj.jus.br/cnj-servico-qual-a-diferencaentre-crime-e-contravencao/>. Acesso em: 20, ago. 2023.

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. **Código Penal.** Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1851-1899/d847.htm. Acesso em: 28, ago. 2023.

FEBRABAN. **Lei endurece penas para crimes eletrônicos, como clonagem do WhatsApp e outros golpes via internet.** 28, mai. 2021. Disponível em: https://portal.febraban.org.br/noticia/3631/pt-br. Acesso em: 28, ago. 2023.

FEITOZA, Luís Guilherme de Matos. **Crimes Cibernéticos: o Estelionato Virtual. Brasília**, 2012.

FREITAS, Riany Alves de. **Segurança Estelionato Digital**. 2009. Disponível em:< https://aplicacao.mpmg.mp.br/xmlui/bitstream/handle/123456789/502/Estelionato%20digital.pdf?sequence=3>. Acesso em: 19, ago. 2023.

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

GRECO, Rogério. **Código Penal Comentado**. 5 ed. Rio de Janeiro: Impetus, 2018.

HUNGRIA, Nélson. **Comentários ao Código Penal**. 4ª ed. v. 7. arts. 155 a 196. Ed. Forense. 1980.

JÚNIOR, Hélio Santiago Ramos. **Estudo sobre a aplicabilidade das leis penais aos crimes informáticos no Brasil**. In: Proceedings of the Third International Confeerence of Forensic Computer Science. Rio de Janeiro: ABEAT, 2008.

MIRABETE, Júlio Fabbrini. **Código penal interpretado**. 4. ed. São Paulo: Atlas, 2003.

MOREIRA, Paulo. Estelionato praticado por meio da internet: Uma visão acerca dos crimes digitais. 16, fev. 2022. Migalhas. Disponível em: https://www.migalhas.com.br/depeso/359821/estelionato-praticado-por-meio-da-internet. Acesso em: 28, ago. 2023.

PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro**. Parte Especial - arts. 121 a 183. V. 2. Ed. Filiada. 2002. p. 523.

ROSA, Fabrízio. **Crimes de Informática**. 2º ed. Campinas: Bookseller, 2005.