ESTELIONATO ELETRÔNICO

ELECTRONIC SCAMMER

Cleidiane da Silva Souza
Gabriela Rodrigues de Abreu
Geovanna Marques de Oliveira Souza
Hamilton Rodrigues Fernandes
Hadrian Thompson
João Teodoro da Silva Filho
Letícia de Souza Vieira
Maria Eduarda Alves Barbosa

Resumo

A pesquisa refere-se ao crime de estelionato virtual, às atividades ilícitas praticadas na internet ou com o auxílio de dispositivos eletrônicos. A migração dos criminosos para o ambiente virtual é impulsionada pela atratividade do anonimato proporcionado pelas redes sociais, levando-os a adaptar suas práticas delituosas para o mundo online. O objetivo é distinguir entre crimes virtuais próprios e impróprios, e também identificar o comportamento associado ao estelionato eletrônico. A problematização central da pesquisa está relacionada à distinção entre furto por meio de fraude eletrônica e estelionato por meio de fraude eletrônica. Para isso, a pesquisa sobre delitos na internet será conduzida através de um estudo bibliográfico descritivo, que incluirá a análise de artigos, livros e doutrinas, destacando os acontecimentos decorrentes do aumento significativo dos crimes virtuais na sociedade. Além disso, a análise da Lei 14.155/2021, ao abordar a preocupação com os crimes virtuais e ao aumentar as penas para o estelionato digital, contribui para a conscientização sobre esse tema, visando tornar esses crimes menos atrativos para os criminosos que percebem a internet como uma "terra sem lei".

Palavras – chaves: Estelionato Virtual,Crimes Virtuais e Lei 14.155/2021.

Abstract

The research refers to the crime of virtual fraud, illicit activities carried out on the internet or with the help of electronic devices. The migration of criminals to the virtual

environment is driven by the attractiveness of the anonymity provided by social networks, leading them to adapt their criminal practices to the online world. The objective is to distinguish between proper and inappropriate virtual crimes, and also to identify the behavior associated with electronic fraud. The central question of the research is related to the distinction between theft through electronic fraud and embezzlement through electronic fraud. To this end, research on crimes on the internet will be conducted through a descriptive bibliographic study, which will include the analysis of articles, books and doctrines, highlighting the events resulting from the significant increase in virtual crimes in society. Furthermore, the analysis of Law 14,155/2021, by addressing the concern about virtual crimes and increasing penalties for digital fraud, contributes to raising awareness on this topic, aiming to make these crimes less attractive to criminals who perceive the internet as a "lawless land".

***Keywords*:**Virtual Robbery, Virtual Crimes and Law 14,155/2021.

1. INTRODUÇÃO

O uso da internet é um fenômeno que está diretamente relacionado com a globalização, em razão de sua característica de promover o envolvimento de culturas e sistemas jurídicos diferentes.

Precisamente, os crimes digitais consistem nas menções a condutas de acesso não autorizado a sistemas informáticos, nesse campo a perpetuação são de diversos crimes desde a interceptação de comunicações até a propagação da pornografia infantil, entre outros, já tipificados no ordenamento jurídico.

Isto posto, nota-se que o ciberespaço é um meio para prática de delitos já tipificados em vários ordenamentos jurídicos. Dentre crimes comumente praticados na era digital e com a abertura dos ciberespaços, está o estelionato eletrônico. O notável crime de estelionato, tipificado no artigo 171 do Código Penal (BRASIL, 1940), consiste na prática de golpe onde o criminoso engana a vítima para obter algum tipo de vantagem, na maioria das vezes essa vantagem é econômica.

É claro que com o avanço da tecnologia o uso comum e habitual da internet, bem como dos smartphones, os golpes evoluíram desmedidamente não só pela quantidade em que ocorrem, como pelas diversas formas de se enganar e atrair vítimas.

O Estelionato Digital se configura, quando mediante redes sociais, por meio de contatos telefônicos, correio eletrônico falso e etc. o criminoso consegue convencer a vítima a fornecer dados confidenciais, senhas de acesso bancário, números de cartões de crédito ou débito, ou a levar a vítima a realizar compras que o beneficie. Convém trazer à luz deste estudo, que a Fraude Eletrônica ou Estelionato Digital é uma qualificadora do crime de Estelionato, nesse sentido a prática do crime recebe pena mais severa.

O estelionato comum prevê a pena de 1 a 5 anos de prisão, na fraude eletrônica a pena está entre 4 a 8 anos e pode ser aumentada em até ⅔, se o crime for cometido com uso de servidor que se encontre fora do Brasil. Outra hipótese de majoração da pena é se o crime for cometido contra entidade pública, institutos de economia popular ou assistência social.

Nesse sentido, a Lei 14.155/2021 trouxe modificações importantes no campo jurídico, que serão discutidas no decorrer da pesquisa (BRASIL, 2021).

2. Desenvolvimento da pesquisa

2.1 A legislação acerca do tratamento jurídico da internet no Brasil

O Estelionato eletrônico ocorre quando o infrator consegue ludibriar alguém por meio de redes sociais, contatos telefônicos, correio eletrônico falso ou qualquer outro meio fraudulento que forneça dados confidenciais.

A Lei nº 14.155, de 27 de maio de 2021**,** trouxe modificações muito relevantes ao campo jurídico brasileiro, alterando os crimes cibernéticos. Algumas dessas alterações ocorreu no artigo 154–A, § 2º e § 3º do Código Penal Brasileiro, (BRASIL, 1940 e 2021):

> "Art. 154-A. Invadir dispositivo informático de **uso alheio**, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, **de 1 (um) a 4 (quatro) anos**, e multa.
> § 2º **Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.**
> § 3º Se da **invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações**

> **sigilosas**, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> **Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa."**

Foi incluído o termo "uso alheio". Isso ampliou a interpretação da invasão ao dispositivo informático, não se restringindo mais apenas ao proprietário, mas também a qualquer usuário cuja privacidade seja violada. E tornou as penas mais brandas, com qualificadoras, perdendo a natureza de menor potencial ofensivo.

Além disso, foram criados os crimes específicos de furto mediante fraude eletrônica do artigo 155, § 4º-B e C, e incisos I, II, do Código Penal Brasileiro (Brasil, 1940):

> "Art. 155. (...)
> § **4º B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores,** com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
> § 4º C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado **gravoso:**
> **I – 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;**
> **II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável."**

E foi criado também de fraude eletrônica propriamente dita, no disposto do artigo 171, § 2º Código Penal Brasileiro (BRASIL, 1940):

> **"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
> **§ 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."**

Destaca-se ainda que, no artigo 171 do Código Penal, que trata do estelionato, foi adicionado o § 2º-A, introduzindo uma modalidade qualificada de estelionato

conhecida como "fraude eletrônica". Esta modalidade é definida legalmente da seguinte forma: 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 (BRASIL, 1940).

O Marco Civil da Internet (BRASIL, 2014), como a principal norma federal que regula o uso dessa ferramenta no Brasil, estabelece objetivos, princípios, garantias e deveres para o uso da rede mundial de computadores, além de especificar diretrizes para a atuação do poder público, incluindo inclusão digital e educação informática (JESUS; OLIVEIRA, 2014, p.17-30).

O Brasil é pioneiro na regulamentação da internet, e o Marco Civil (BRASIL, 2014) busca controlar conteúdos, proteger os usuários e enumerar direitos fundamentais, como proteção de dados e privacidade. Importante ressaltar que a referida norma não tipifica condutas penais; para casos de crimes virtuais, são aplicadas as disposições do Código Penal e do Código Civil referentes à compensação por danos civis e responsabilidade civil objetiva (GARCIA, 2020).

A legislação também definiu qual será o foro competente para julgar os casos de estelionato envolvendo cheques sem fundos ou transferências de valores, determinando que o local de residência da vítima será o responsável pelo julgamento desses casos. Esse tipo penal foi criado em resposta ao significativo aumento de fraudes no ambiente digital, especialmente devido ao crescimento das transações eletrônicas durante a pandemia.

A distinção entre furto qualificado por fraude e fraude eletrônica está no envolvimento da vítima na obtenção do benefício. No furto qualificado, a vítima não tem participação na ação. Por exemplo, um hacker que rouba os dados da vítima e acessa suas informações bancárias. Já na fraude eletrônica, a vítima tem um papel significativo. Um exemplo é o golpe via WhatsApp, onde o fraudador se passa por um parente da vítima e solicita dinheiro para uma emergência.

A rapidez com que as tecnologias da informação evoluem e se adaptam constantemente, assim como sua capacidade de impactar uma variedade de interesses jurídicos, tem levado o governo a concentrar-se mais na proteção legal da segurança dos usuários e dos dados no ambiente virtual, especialmente durante o

período de 2012 a 2022. Os crimes virtuais têm uma natureza transnacional ou global, ultrapassando as fronteiras de países, afetando pessoas de todas as classes sociais, com o objetivo comum para os criminosos de obter vantagens ilegais. Como resultado, esses crimes são conhecidos por várias designações, incluindo crimes de computador, infrações cometidas por meio da informática, fraude informática, delinquência informática, crimes digitais, crimes relacionados a computadores, cibercrimes ou crimes cibernéticos.

TIPOS DE FRAUDE NA INTERNET

Os cibercriminosos usam uma variedade de vetores e estratégias de ataque para cometer fraudes na Internet. Isso inclui software malicioso, serviços de e-mail e mensagens instantâneas para espalhar malware, sites falsificados que roubam dados do usuário e esquemas de phishing elaborados e de amplo alcance.

A fraude na Internet pode ser dividida em vários tipos principais de ataques, incluindo:

1- *Phishing* **e** *spoofing*: O uso de e-mail e serviços de mensagens on-line para induzir as vítimas a compartilhar dados pessoais, credenciais de login e detalhes financeiros.

Phishing: tem origem no inglês, em *fishing* (pescar). A analogia remete a um pescador jogando um anzol com isca (o e-mail de phishing) e esperando que a vítima a morda. (Por Serasa)

Spoofing**:** imitar, fingir. Segundo Ronaldo Gogone, ocorre quando são criados sites de lojas e outros, parecidos com os sites verdadeiros.

2- **Negação de serviço (DoS**): É um ataque cibernético malicioso, em que o autor tem a intenção de tornar um dispositivo eletrônico indisponível para o para os usuários. Os ataques DoS costumam funcionar sobrecarregando ou inundando uma máquina alvo com solicitações até que o tráfego normal não seja processado, o que resulta em negação de serviço para usuários adicionais.

3- ***Malware***: Programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um dispositivo ou rede. (Por Blockbit)

4- ***Ransomware***: Trata-se de um software malicioso que se utiliza da criptografia para a extorsão de dados digitais. Trata-se de um crime que usa como refém arquivos computacionais da própria vítima, para posteriormente cobrá-la um resgate para restaurar esses arquivos. (Por ESET)

5- Comprometimento de e-mail comercial (BEC): uma forma sofisticada de ataque direcionada a empresas que fazem pagamentos eletrônicos com frequência. Compromete contas de e-mail legítimas através de técnicas de engenharia social para enviar pagamentos não autorizados.

6- **Golpes de *phishing* por *e-mail***

Os golpes de phishing baseados em e-mail estão entre os tipos mais comuns de fraude na Internet, que continuam a representar uma séria ameaça para usuários e empresas da Internet.

As estatísticas da Security Boulevard mostram que, em 2020, 22% de todas as violações de dados envolveram um ataque de phishing e 95% de todos os ataques direcionados a redes empresariais foram causados por spearphishing.

Além disso, 97% dos usuários não conseguiram identificar um e-mail de phishing sofisticado, 1,5 milhão de novos sites de phishing foram criados todos os meses e 78% dos usuários entendem o risco de hiperlinks em e-mails, mas clicam neles mesmo assim.

Os golpes de phishing baseados em e-mail estão em constante evolução e variam de ataques simples a ameaças mais sorrateiras e complexas que visam indivíduos específicos.

Os golpes de phishing por e-mail fazem com que os criminosos cibernéticos se disfarcem como indivíduos que suas vítimas conhecem ou considerariam respeitáveis. O ataque tem como objetivo incentivar as pessoas a clicarem em um link que leva a um site malicioso ou falsificado, projetado para parecer um site legítimo, ou a abrir um anexo que contenha conteúdo malicioso.

O hacker compromete um site legítimo ou cria um falso e obtém uma lista de endereços de e-mail para enviar mensagens que induzam as pessoas a clicar em um link para esse site. Quando uma vítima clica no link, ela é redirecionada para o site falso, que solicita nome de usuário e senha ou baixa automaticamente malware em seu dispositivo, roubando dados e informações de login.

O hacker pode usar esses dados para acessar as contas online do usuário, obter mais informações, como detalhes de cartão de crédito, acessar redes corporativas conectadas ao dispositivo ou cometer fraudes de identidade mais amplas.

Os golpistas que utilizam phishing por e-mail frequentemente criam um senso de urgência para suas vítimas, informando que sua conta online ou cartão de crédito está em risco e que precisam fazer login imediatamente para resolver o problema. (Por Security Boulevard)

O Código Penal, em seu artigo 154-A descreve o delito de invasão de dispositivo tecnológico/informático.

O crime tem como objetivo invadir computador ou dispositivo semelhante de outrem, modificar, apagar, ter acesso à informações privativas do intuito de obter vantagem.

Art. 154-A: Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

7- **Golpes de cartão de crédito -** São muito comuns na era digital. Em regra acontece quando o criminoso consegue adquirir de forma ilícita seja ela por furto de dos dados ou por convencer a vítima e entregá-los por engano ou ameaça, detalhados dos cartões de crédito ou débito. Normalmente atraem vítimas com ofertas atraentes de crédito.

8- **Golpes de namoro on-line:** O golpista leva a vítima a acreditar que está num relacionamento constante e recíproco com alguém que conheceu online, em app. Porém, nesse momento, a verdadeira intenção do criminoso é envolver a vítima emocionalmente, para com isso, iniciar um ciclo de extorsão de vantagens, não só em dinheiro mas também, informações confidenciais para chantageá-la e extrair dinheiro e informações quando na verdade o interesse do criminoso é enganar as vítimas. O golpe é aplicado com facilidade devido a quantidade de aplicativos de relacionamentos.

9- **Fraude em taxas de loteria ou golpe do bilhete premiado -** Os jogos de loteria são grandes atrativos para os apostadores.

Outra forma comum de fraude na Internet são os golpes por e-mail que informam às vítimas que ganharam na loteria. Esses golpes informarão aos destinatários que eles só poderão reivindicar seu prêmio depois de pagarem uma pequena taxa.

Os fraudadores de taxas de loteria normalmente criam e-mails para parecerem confiáveis, o que ainda faz com que muitas pessoas caiam no golpe. O golpe tem como alvo o sonho das pessoas de ganhar grandes quantias de dinheiro, mesmo que nunca tenham comprado um bilhete de loteria.

Além disso, nenhum esquema de loteria legítimo exigirá que os vencedores paguem para reivindicar seu prêmio.

10-**O príncipe nigeriano:** O golpe “o príncipe nigeriano” está entre as modalidades mais antigas dentro do *phishing.* É uma forma de spam. O golpe consiste basicamente em um email vindo de parente próximo ou advogado representante de ente falecido milionário, oferecendo retorno em dinheiro para fazer a assistência à herança.

COMO SE PROTEGER DE GOLPES NA INTERNET

Os utilizadores da Internet podem proteger-se e evitar serem apanhados numa linha de phishing, permanecendo vigilantes relativamente aos tipos comuns de fraude na Internet listados acima.

É vital nunca enviar dinheiro a alguém conhecido pela Internet, nunca partilhar dados pessoais ou financeiros com indivíduos que não sejam legítimos ou confiáveis e nunca clicar em hiperlinks ou anexos em e-mails ou mensagens instantâneas.

Uma vez visados, os usuários da Internet devem denunciar atividades de golpistas on-line e e-mails de phishing às autoridades.

A fraude com cartão de crédito também pode ser evitada mantendo-se atento às contas bancárias, configurando notificações sobre a atividade do cartão de crédito, inscrevendo-se no monitoramento de crédito e utilizando serviços de proteção ao consumidor. Se os usuários sofrerem fraude com cartão de crédito, deverão denunciá-la às autoridades legais e agências de crédito relevantes.

A importância da tutela jurídica do ambiente virtual

O Brasil ocupa a 5ª posição no ranque de países que mais sofrem com crimes pela internet, segundo uma pesquisa divulgada pela empresa russa Kaspersky (KASPERSKY, s. d.). Para além da popularização do acesso à internet e das causas que aceleram a migração das relações analógicas para as digitais como a covid 19, há um aumento expressivo de criminosos incentivados a práticas de crimes nesse ambiente. No que diz respeito à conduta de fraude eletrônica, houve um crescimento de 500% entre os anos de 2018 e 2021 em todo o Brasil, passando de 7.591 para 60.590 casos (CAETANO, 2022). Seja pela facilidade do anonimado ou mesmo pela dificuldade de responsabilização dos criminosos, a internet tem se notabilizado um ambiente propício para praticas delituosas, uma vez que é possível maior alcance de vítimas, bem como ações rápidas, sucessivas e exitosa devido a fluidez dos dados sensíveis e o alcance das redes sociais.

Naturalmente, as mudanças legislativas não acompanham a globalização impulsionada pela internet e os processos tecnológicos, fazendo com que o direito penal enfrente uma grande dificuldade em acompanhar tais evoluções, a fim de adaptar-se e combater com maior precisão os crimes praticados no ambiente virtual. Nesse sentido, o legislativo pátrio tem atuado por meio de pressão popular como no caso da atriz Carolina Dieckmann, que teve seu computador pessoal invadido por hacker e, na época do fato, não havia dispositivo legal para enquadrar o crime. A partir desse fato e muita pressão da grande mídia foi editada a lei 12.737 de 2012 que

estipulou tipo penal de invasão de dispositivo informático, acrescentando o artigo 154-A ao código penal brasileiro.

Outro acontecimento marcante na evolução das relações comerciais e de prestação de serviços por meio da internet foi a pandemia de covid-19. O exponencial crescimento de casos de estelionatos digitais impulsionou o legislador novamente para construir um ambiente digital mais seguro tanto nas relações comerciais quanto nos espaços de convivência com a edição da lei 14.155 de 2021, que alterou diversos dispositivos do código penal, introduzindo o crime de fraude eletrônica e majorando os crimes praticados a partir de servidores de páginas fora do país de acordo com o § 2º-B do artigo 171 da codificação penal.

> 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 forncediades pela vitima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônicos fraudulento, ou por qualquer outro meio fraudulento análogo.
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. (BRASIL, 1940)

Com essas medidas, inicia-se um processo de combate ao anonimato que a rede mundial de computadores oferece aos criminosos, servindo como uma espécie de manto protetor o ambiente virtual.

Tendo em vista as enormes facilidades que a rede oferece para a prática de crimes cibernéticos mormente com a engenharia social atrelada a massificação do *e-commerce*, há ainda grandes vácuos legais que precisam ser sanados no desafiante mundo digital. O Brasil vem tomando medidas efetivas por intermédio do sancionamento de leis modernas, a tipificação de novos atos, específicos de meios virtuais, além de políticas públicas integradas com o setor privado. Neste sentido, destaca-se, em junho de 2022, a criação da Unidade Especial de Investigação de Crimes Cibernéticos (UEICC) do Ministério da Justiça e Segurança (MJSP) em parceria com a Federação Brasileira de Bancos (Febraban), para combater e prevenir com maior efetividade os crimes no mundo digital (BRASIL, 2022ª).

As parcerias público-privadas podem oferecer um horizonte esclarecedor para o legislador brasileiro, bem como um fortalecimento de políticas preventivas contra fraudes eletrônicas. Em sua maioria, os usuários de tecnologias digitais têm pouca

informação sobre segurança digital e como detectar golpes na internet. O uso dessas parcerias oferece maior alcance ao consumidor de serviçõe bancários, em plataformas e servidores da web. Dessa forma, a tutela jurisdicional faz-se necessária em vista de maior efetividade para alcançar os cidadãos mais vulneráveis que, em regra, são os de programas sociais de distribuição de renda, idosos e os de pouco acesso a conteúdo de segurança digital. O Estado, como principal fomentador de políticas públicas de distribuição de renda e garantidor de direitos fundamentais, deve criar condições de acesso a sistemas informatizados de forma segura junto com os objetivos de inclusão social dos mais vulneráveis.

Atitudes a serem tomadas ao sofrer um golpe:

Ao longo das décadas da era digital o Estado tem contribuído amplamente para o enfrentamento dos crimes cibernéticos. Nesse sentido, as políticas públicas, ações e medidas do Estado para promover e colocar em prática os direitos, bem como solucionar problemas surgiu a Lei de n° 12.965 de 2014, denominada como Marco Civil da Internet (Brasil, 2014) regula o uso, dispõe sobre os direitos e princípios da internet e pune ilícitos civis.

O estelionato virtual, quando praticado por meio eletrônico, é enquadrado no artigo 171, § 2º-A, do Código Penal brasileiro. Essa inclusão foi realizada pela Lei nº 14.155/2021. De acordo com essa lei, a pena para o estelionato virtual varia de 4 a 8 anos de reclusão, além da aplicação de multa.

A polícia investiga e rastreia crimes virtuais através de ferramentas especializadas para localizar e recolher informações relevantes, como registros de acesso, logs de servidores, conversas em aplicativos de mensagens e redes sociais, etc.

Os indícios coletados através das investigações feitas são fundamentais para a identificação de criminosos e a comprovação de suas ações.

É recomendável que vítimas de crimes eletrônicos procurem uma Delegacia Especializada em Crimes Eletrônicos para registrar um boletim de ocorrência. Essas delegacias possuem expertise e recursos específicos para lidar com esse tipo de crime, o que pode resultar em uma investigação mais eficaz.

No entanto, caso não haja uma Delegacia Especializada em Crimes Eletrônicos na região da vítima, ainda é possível registrar a denúncia em uma Delegacia comum.

É importante que a vítima não deixe de registrar a ocorrência, independentemente do tipo de delegacia, para que as autoridades possam iniciar uma investigação e tomar as medidas necessárias para resolver o caso.

Ao comunicar um crime de estelionato envolvendo a clonagem de cartão de crédito, é necessário fornecer informações detalhadas, incluindo:
NÚMERO DO CARTÃO, NOME DO BANCO OU OUTRO ESTABELECIMENTO EMISSOR, COMO LOJAS, E O NÚMERO DA AGÊNCIA BANCÁRIA VINCULADA AO CARTÃO. Isso é essencial para que as autoridades possam iniciar uma investigação eficaz e tomar as medidas adequadas para resolver o caso.

Da mesma forma, nos casos de furto mediante fraude em que ocorreram débitos indevidos na conta bancária da vítima, é importante fornecer o NOME DO BANCO, A AGÊNCIA BANCÁRIA COM SEU ENDEREÇO E O NÚMERO DA CONTA BANCÁRIA AFETADA. Essas informações são cruciais para que as autoridades possam rastrear as transações fraudulentas e identificar os responsáveis pelo crime.
Onde denunciar:

Procure uma delegacia mais próxima de sua casa, ou registre um Boletim.
A capital também conta com duas delegacias especializadas no atendimento à mulher, na Asa Sul e em Ceilândia:
Delegacia Especial de Atendimento à Mulher (DEAM)
Endereço: EQS 204/205, Asa Sul, Brasília
Telefones: (61) 3207-6195 e (61) 3207-6212
Delegacia de Atendimento Especial à Mulher (DEAM II)
Endereço: QNM 2, Conjunto G, Área Especial, Ceilândia Centro
Telefone: (61) 3207-7391

Delegacias Online:
Delegacia Eletrônica, Estelionato, Fraudes e Apropriações.
Site de Denuncia: https://www.pcdf.df.gov.br/servicos/delegacia-eletronica/estelionato-fraudes-e-apropriacoes#

Delegacia Eletrônica:
WhatsApp: (61) 98626 – 1197
Telefone: 197 ou 3207 – 4892

E-mail: denuncia197@pcdf.df.gov.br
https://www.pcdf.df.gov.br/servicos/delegacia-eletronica

3. Considerações Finais

Os delitos cibernéticos, também conhecidos como crimes digitais, são violações legais que ocorrem no ambiente virtual. O estelionato online tornou-se uma ocorrência comum na sociedade, causando insegurança e prejuízos para muitas pessoas. Diversos métodos de golpes têm sido registrados no Brasil, como a "ligação premiada", o "envelope bancário vazio" e o "anúncio de veículo". Esses golpes variam em suas abordagens, incluindo falsos sorteios, solicitações de dinheiro para situações fictícias, como reparos em veículos, ou até mesmo confirmações de resgate de carros roubados.

Normalmente, esses golpes são realizados por indivíduos detidos. Para se proteger contra esses golpes, é importante que os cidadãos adotem algumas medidas preventivas, como verificar informações sobre supostas premiações, entrar em contato com parentes antes de fornecer qualquer dado pessoal e nunca depositar dinheiro em resposta a pedidos feitos através de redes sociais. Em situações de premiações das quais não se está participando ou em ofertas de empréstimos via redes sociais, é essencial desconfiar e buscar informações concretas sobre o serviço oferecido. Em caso de dúvida, é recomendável procurar ajuda especializada, especialmente junto às autoridades policiais.

Atualmente, é comum a criação de novos tipos penais, pois muitas condutas fraudulentas praticadas no ambiente virtual não se enquadram diretamente em crimes já existentes. Por isso, a legislação tem buscado tornar as penalidades mais rígidas e criar formas qualificadas de crimes, especialmente quando praticados em meio cibernético. A Lei 14.155, de 27 de maio de 2021, trouxe alterações significativas ao Código Penal, incluindo a adição do crime de invasão de dispositivo informático e a inserção da fraude eletrônica como modalidade de furto e estelionato.

Referências

AVELAR, Michael Procopio. Lei 14.155/2021: **A fraude eletrônica e outras alterações no Código Penal**. Estratégia Concursos, 28 set 2021. Disponível em: https://www.estrategiaconcursos.com.br/blog/lei-14-155-2021-a-fraude-eletronica-e-outras-alteracoes-no-codigo-penal . Acesso em 19 mar 2024.

BARBAGALO, Fernando Brandini. **O novo crime de fraude eletrônica e o princípio da legalidade.** Migalhas, 02 jun 2022. Disponível em:https://www.migalhas.com.br/depeso/367289/o-novo-crime-de-fraude-eletronica-e-o-principio-da-legalidade. Acesso em 19 mar 2024.

BLOCKBIT. **O que é malware? Você conhece os tipos mais comuns?**Disponível em:ttps://www.blockbit.com/pt/blog/tipos-de-malware/?gad_source=1&gclid=EAIaIQobChMI_LDGmO2XhQMV5tjCBB2MYgomEAAYASAAEgJfmvD_BwE. Acesso em 28 mar 2024.

BLOCKBIT. **O que é ransomware? Conheça o tipo de ataque virtual que ocupou as manchetes mundiais**. https://www.blockbit.com/pt/blog/o-que-ransomware/?gad_source=1&gclid=EAIaIQobChMIoYqNm_KXhQMVnGFIAB29eQ83EAAYASAAEgILp_D_BwE. Acesso em 28 mar 2024.

BRASIL, Código Penal Brasileiro, 07 de dezembro de 1940, disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acessado em 30 mar. 2024.

BRASIL. **Decreto-lei nº 14.155**, de 27 de maio, de 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm. Acesso em: 18 mar. 2024.

BRASIL.Decreto-lei nº 2.848, de 07 de dezembro de 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/Decrto-lei/Del2848compilado.htm. Acesso em: 27 mar. 2024.

BRASIL. Ministério da Justiça. **Polícia Federal cria Unidade Especial para intensificararepressãoacrimescibernéticos.**Brasília,05jul2022a. Disponívelem: https://www.gov.br/mj/pt-br/assuntos/noticias/policia-federal-cria-unidade-especial-para-intensificar-a-repressao-a-crimes-ciberneticos. Acesso em: 27 mar. 2024.

BRASIL.Decreto-lei nº 2.848, de 07 de dezembro de 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm. Acesso em: 19 mar. 2024.

BRASIL. **Lei n. 12.965**, de 23 de abril de 2014. Institui o Marco Civil da Intener. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 04 abr. 2024.

BRUSH, Kate. COBB, Michael. **CybercrimeDefinition**. Tech Target, jan 2024. Disponível em: https://www.techtarget.com/searchsecurity/definition/cybercrime. Acesso em 19 mar 2024.

CAETANO, Guilherme. EstelionatodigitalexplodenoBrasilecresce500 em4anos. **O Globo**, 28 jun 2022. Disponível em: https://oglobo.globo.com/brasil/noticia/2022/06/estelionato-digital-explode-no-brasil-e- cresce-500percent-em-4-anos.ghtml. Acesso em: 27 mar. 2024.

CG. Cuidado! Golpes virtuais têm aumentado no DF. Disponível em: https://www.cg.df.gov.br/cuidado-golpes-virtuais-tem-aumentado-no-df/. Acesso em 31 de mar 2024.

EUR-LEX**. 46 Regulation UE 2016/679**. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679. Acesso 25 mar 2024.

FMP. Fundação Escola Superior do Ministério Público. **Lei Carolina Dieckmann: você sabe o que essa lei representa?** Porto Alegre, 16 ago 2021. Disponível em: https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/.Acesso em: 26 mar. 2024.

G1.GLOBO. 'Estelionato amoroso': delegada do DF dá dicas para evitar cair no golpe e ensina como denunciar. Disponível em: https://g1.globo.com/df/distrito-

federal/noticia/2022/01/16/estelionato-amoroso-delegada-do-df-da-dicas-para-evitar-cair-no-golpe-e-ensina-como-denunciar.ghtml. Acesso em 31 de mar 2024.

GARCIA, Lara R. **Lei Geral de Proteção de Dados (LGPD): Guia de implantação**. [Digite o Local da Editora]: Editora Blucher, 2020. E-book. ISBN 9786555060164. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555060164/. Acesso em: 30 mar. 2024.

HACKERNOON. O e-mail do príncipe nigeriano e a história das técnicas de engenharia social. Disponível em: https://hackernoon.com/pt/o-e-mail-do-pr%C3%ADncipe-nigeriano-e-a-hist%C3%B3ria-das-t%C3%A9cnicas-de-engenharia-social. Acesso em: 18 mar. 2024.

Fraude na Internet O que é fraude na Internet? Disponível em: https://www.fortinet.com/resources/cyberglossary/internet-fraud. Acesso em: 03 abr. 2024.

JESUS, Damásio Evangelista D.; OLIVEIRA, José Antônio M. Milagre D. **Marco Civil da Internet: comentários à Lei n. 12.965, de 23 de abril de 2014**, 1ª Edição,. [Digite o Local da Editora]: Editora Saraiva, 2014. E-book. ISBN 9788502203200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502203200/. Acesso em: 30 mai. 2022, p.17-30.

KASPERSKY.**CiberameaçaMapaemtemporeal**.[s.d.].Disponívelem: https://cybermap.kaspersky.com/pt/stats. Acesso em: 27 mar. 2024.