ANÁLISE DA PRÁTICA DO CRIME DE FRAUDE PERPETRADO POR ORGANIZAÇÕES CRIMINOSAS E SUAS CONSEQUÊNCIAS NO AMBIENTE VIRTUAL [1]

José Gustavo Alves[2].

Professora Dr. Andréa Flores.

RESUMO

Este trabalho tem como tema a "Análise da prática do crime de fraude perpetrado por organizações criminosas e suas consequências no ambiente virtual" no âmbito do Direito Penal. O tema ganhou relevância no Brasil a partir do aumento da prática de fraudes virtuais por organizações criminosas, tendo como vítimas, principalmente, pessoas vulneráveis como idosos e mulheres. O objetivo geral da pesquisa analisou como as organizações criminosas atuam na prática de fraudes virtuais, bem como identificar as consequências desses crimes no ambiente virtual e no mundo físico. O problema de pesquisa buscou responder como as organizações criminosas perpetram fraudes virtuais e quais as consequências dessas ações? Este estudo justificou-se frente a necessidade de compreender melhor essa prática criminosa para que possam ser criadas políticas públicas e leis que previnam e reprimam esse tipo de crime. A metodologia utilizada foi a revisão bibliográfica de trabalhos e estudos relacionados ao tema, obteve-se como resultado que as organizações criminosas estão mais sofisticadas em suas técnicas de fraudes no ambiente virtual, o que dificulta sua prevenção e combate. As consequências desses crimes são graves para as vítimas e a sociedade em geral, exigindo uma abordagem multidisciplinar com políticas públicas, tecnologias de segurança, treinamentos para usuários e ações policiais. Além disso, destacou a importância da conscientização da população quanto à segurança digital e aos cuidados que devem ser tomados para evitar fraudes e golpes virtuais. É fundamental que novas pesquisas sejam realizadas para aprimorar as estratégias de combate ao crime organizado no ambiente virtual. A pesquisa é relevante e contribuiu para o estudo sobre o desenvolvimento de novas estratégias e tecnologias de combate ao crime de fraude cibernética perpetrado pelo crime organizado.

Palavras-chave: Crime organizado; Fraude virtual; Estelionato.

---

[1] Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de bacharel em Direito, realizado sob orientação da Prof.ª Dr. Andréa Flores.

[2] Acadêmico do curso de Direito da Faculdade de Educação da Universidade Federal de Mato Grosso do Sul (UFMS).

ABSTRACT

The current work has as its theme the "Analysis of the practice of the crime of fraud perpetrated by criminal organizations and its consequences in the virtual environment" in the scope of Criminal Law. The topic gained relevance in Brazil due to the increase in the practice of virtual fraud by criminal organizations, whose victims were mainly vulnerable people, such as the elderly and women. The general objective of the research was to analyze how criminal organizations act in the practice of virtual fraud, as well as to identify the consequences of these crimes in the virtual environment and in the real world. The research problem sought to answer how criminal organizations perpetrate virtual fraud and what are the consequences of these actions? This study is justified by the need to better understand this criminal practice so that public policies and laws can be created to prevent and repress this type of crime. The methodology used was a bibliographical review of works and studies related to the subject, resulting that criminal organizations are more sophisticated in their fraud techniques in the virtual environment, which makes prevention and combat difficult. The consequences of these crimes are severe for the victims and society in general, requiring a multidisciplinary approach with public policies, security technologies, user training and police actions. In addition, it is highlighted the importance of making the population aware of digital security and the precautions that must be taken to avoid fraud and virtual scams. It is essential that new research be carried out to improve strategies to combat organized crime in the virtual environment. The research is relevant and contributed to the study on the development of new strategies and technologies used to combat the crime of cyber fraud perpetrated by organized crime.

Keywords: Organized crime; Virtual fraud; Fraud.

1 INTRODUÇÃO

Com o avanço da tecnologia, a comunicação, a troca de informações e a transferência de valores se tornaram cada vez mais simples, o que contribui para a praticidade do dia a dia das pessoas.

Esse progresso também trouxe um aumento no número de pessoas que utilizam as redes sociais e meios virtuais, especialmente durante a pandemia de Covid-19, que resultou em aulas remotas, home office, audiências online, compras e vendas de produtos, dentre outras atividades.

Esse avanço é observado em diversas áreas, como engenharia, ciências sociais e humanas, ciências biológicas e saúde e tecnologia da informação. No entanto, junto com esses benefícios, cresceu o número de fraudes e armadilhas no meio virtual, evidenciando que o crime organizado se aproveitou desse progresso para se especializar em diferentes formas de fraudes e golpes, utilizando aplicativos, sites, e-mails e mensagens para enganar as pessoas e/ou acessar informações importantes de suas vidas privadas. Como resultado, a legislação penal foi atualizada, com a inclusão de uma nova modalidade de fraude eletrônica, o estelionato virtual, na Lei n° 14.155 de 2021.

Nesse contexto, analisou-se a prática de estelionato perpetrada pelo crime organizado e suas consequências no ambiente virtual. A justificativa se baseou na importância da criminologia em realizar estudos sobre as organizações criminosas, com foco no uso de meios tecnológicos para a operação de crimes.

Além disso, a pesquisa é relevante para os operadores do direito, pois abordou dos aspectos do crime organizado cuja capacidade de adaptação e sobrevivência é contínua, permitindo acompanhar as mudanças na sociedade, mudando suas formas e métodos, aprendendo a dominar as novas tecnologias e a utilizá-las em benefício próprio, promovendo o desenvolvimento de atividades ilícitas.

A metodologia utilizada para o estudo foi uma pesquisa no formato de revisão bibliográfica, por meio do método de pesquisa qualitativa, coletando informações baseadas na observação, análise de pesquisas já realizadas e definições simbólicas. Dessa forma, utilizou-se a informação científica disponibilizada em dados eletrônicos em livros, periódicos e artigos referentes aos sites de pesquisa Google Acadêmico e SCIELO, utilizando as palavras-chave "estelionato virtual", "organizações criminosas" e "crime virtual".

2 A LEGISLAÇÃO REFERENTE AO CRIME ORGANIZADO NO ORDENAMENTO JURÍDICO BRASILEIRO.

Inicialmente, a partir das mudanças estruturais na criminalidade, tornou-se necessário que o Estado criasse mecanismos para combater as organizações criminosas. Com isso, foram criadas legislações para reprimir essas novas estruturas criminosas, trazendo problemas de diferentes naturezas para os atores envolvidos no cotidiano forense, especialmente para aqueles que atuam no direito penal econômico.

A Lei 12.850/13, conhecida como Lei de Organização Criminosa, não foi uma exceção a essa regra. Essa lei foi criada para regulamentar as premissas estabelecidas na Convenção das Nações Unidas contra o Crime Organizado Transnacional, mais conhecida como Convenção de Palermo (BRASIL, 2004; 2013).

A Lei 12.850/13, promulgada em 2 de agosto de 2013, define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal (BRASIL, 2013).

Além de tipificar o crime de organização criminosa, a lei também trata dos meios de obtenção de prova especiais a serem utilizados no enfrentamento da criminalidade organizada, entre eles o da colaboração premiada.

O parágrafo 1° do artigo 1° da Lei apresenta, de forma resumida, os principais pontos do diploma legal em relação a definir organização criminosa, estabelecer os meios de obtenção da prova aplicáveis a sua investigação e tratar do seu procedimento:

> § 1º Considera-se organização criminosa a associação de 4 (quatro) ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional (BRASIL, 2013).
>
> .

O conceito de organização criminosa é complexo e de difícil aceitação pela doutrina, tendo em vista a inexistência de uma concepção unívoca, mas apresenta alguns elementos característicos, tais como associação de pessoas, divisão de tarefas, objetivo econômico e prática de infrações graves.

Na doutrina, a maioria dos conceitos de organização criminosa inclui características como previsão de lucros, hierarquia, divisão de trabalho, ligação com órgãos estatais, planejamento das atividades e delimitação da área de atuação.

De acordo com Mingardi (1995) *apud* Anselmo (2017) existem dois modelos de organização criminosa: o tradicional ou territorial e o empresarial. Além disso, aponta a existência de um terceiro modelo, a organização criminosa institucionalizada no ambiente do Estado.

Com a recepção da Convenção de Palermo, o Supremo Tribunal Federal adotou os critérios definidos na convenção para o julgamento de casos relacionados à matéria do crime organizado, conforme destaca Godoy (2011).

No entanto, Borges (2002) enfatiza que, dependendo do modelo de organização criminosa analisado, pode haver variação de alguns elementos, o que dificulta a criação de um conceito uniforme.

Fernandes (2008) estabelece três correntes doutrinárias que buscam conceituar o crime organizado: a primeira, que define o conceito de organização criminosa e considera como crime organizado qualquer crime praticado por essa modalidade de organização; a segunda, que define os elementos essenciais do crime organizado, sem especificar os tipos penais; e a terceira, que estabelece um rol de tipos penais, qualificando-os como crime organizado.

De acordo com Franco (2007), as características de uma organização criminosa incluem seu caráter transnacional, estruturação organizacional e estratégia de atuação global, capacidade de causar danos sociais acentuados, prática de várias infrações com vitimização difusa ou não, uso de instrumentos tecnológicos modernos, conexões com outros grupos criminosos, contatos com pessoas que ocupam cargos oficiais e a utilização de atos de violência.

Por sua vez, Dipp (2015) afirma que uma organização criminosa se caracteriza por ter um aparato operacional e ser uma instituição orgânica com atuação desviada, podendo ter atividades lícitas com finalidade ilícita.

> Uma organização criminosa de modo geral se revela por dotar-se de aparato operacional, o que significa ser uma instituição orgânica com atuação desviada, podendo ser informal ou até formal, mas clandestina e ilícita nos objetivos e identificável como tal pelas marcas correspondentes. A organização criminosa pode também, eventualmente ou ordinariamente, exercer atividades lícitas com finalidade ilícita, apesar de revestir-se de forma e atuação formalmente regulares. Um estabelecimento bancário que realiza operações legais e lícitas em deliberado obséquio de atividades ilícitas de terceiro, é o exemplo que recomenda cuidado e atenção na compreensão de suas características. A principal delas é ser produto de uma associação, expressão que indica a *afectio* entre pessoas com propósitos comuns ou assemelhados em finalidade e objetivo. É essencial que haja afinidade associativa entre as pessoas (usualmente pessoas físicas, mas não é impossível a contribuição de pessoas jurídicas), ainda que cada uma tenha para si uma pretensão com motivação e objetos distintos das demais e justificativas individuais, todavia logicamente reunidas por intenção e vontade comum nos resultados (DIPP, 2015, p.11).

É essencial que haja uma associação entre as pessoas, mesmo que cada uma tenha uma pretensão com motivação e objetos distintos, mas reunidas por intenção e vontade comum nos resultados. Portanto, a associação de pessoas é o elemento básico para a constituição da organização criminosa, figura central do tipo penal.

É destacado que nos últimos tempos, o Brasil ratificou diversos instrumentos que buscam coibir o crime organizado transnacional. Entre esses instrumentos estão a Convenção de Viena, promulgada pelo Decreto 154 de 26 de julho de 1991, a Convenção de Palermo,

promulgada pelo Decreto 5.015 de 12 de março de 2004, e a Convenção de Mérida, promulgada pelo Decreto 6.587 de 31 de janeiro de 2006.

É importante notar, de acordo com Dipp (2015) é fundamental compreender a noção de organização criminosa de forma sistemática para garantir a clareza e precisão da aplicação da lei em toda a sua amplitude. Pela primeira vez, o crime de pertencer a uma organização criminosa foi tipificado no ordenamento jurídico brasileiro, conforme previsto no artigo 2º da lei:

> Art. 2º Promover, constituir, financiar ou integrar, pessoalmente ou por interposta pessoa, organização criminosa: Pena – reclusão, de 3 (três) a 8 (oito) anos, e multa, sem prejuízo das penas correspondentes às demais infrações penais praticadas. § 1º Nas mesmas penas incorre quem impede ou, de qualquer forma, embaraça a investigação de infração penal que envolva organização criminosa (BRASIL, 2013).

Embora a redação original da Lei 9.613/98 já estabelecesse como crime antecedente da lavagem de dinheiro quando praticado por uma organização criminosa, havia um entendimento jurisprudencial das cortes superiores de que essa regra não se aplicava devido à falta de tipificação do crime de organização criminosa no ordenamento jurídico nacional.

No entanto, alguns especialistas argumentam que, na redação anterior da Lei de Lavagem de Dinheiro, qualquer crime antecedente praticado por uma organização criminosa era considerado como tal, já que a definição de "grupo criminoso organizado" estava prevista na Convenção de Palermo (que foi devidamente internalizada pelo Decreto 5.015 de 12 de março de 2004 e, portanto, tem força de lei).

> “Grupo estruturado de três ou mais pessoas, existente há algum tempo e atuando concertadamente com o propósito de cometer uma ou mais infrações graves ou enunciadas na presente Convenção, com a intenção de obter, direta ou indiretamente, um benefício econômico ou outro benefício material” (BRASIL, 2004).

Apesar da posição firmada pela corte, o voto-vista do ministro Luiz Fux no julgamento indicou que a alegação de que o inciso VII do artigo 1° da Lei 9.613/98 não poderia ser aplicado devido à ausência de definição legal de um crime de organização criminosa é infundada. O ministro argumentou que essa expressão não se refere a um crime em si, mas sim à figura do sujeito passivo responsável pela prática do delito antecedente.

Portanto, qualquer tipo de organização criminosa pode ser considerada como antecedente da lavagem de dinheiro. É importante destacar que a Lei 12.694, de 24 de julho de 2012, que trata do processo e julgamento colegiado em primeiro grau de jurisdição de crimes

praticados por organizações criminosas, considera o conceito de organização criminosa como definido no artigo 2º:

> Art. 2º Para os efeitos desta Lei, considera-se organização criminosa a associação, de 3 (três) ou mais pessoas, estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de crimes cuja pena máxima seja igual ou superior a 4 (quatro) anos ou que sejam de caráter transnacional (BRASIL, 2012).

Observa-se, no ordenamento jurídico brasileiro, a existência de três conceitos diferentes de organização criminosa. O primeiro conceito foi originalmente previsto na Convenção de Palermo, o segundo foi previsto na lei que instituiu os julgamentos colegiados para crimes praticados por organizações criminosas e o terceiro foi estabelecido na atual Lei de Organizações Criminosas (Lei 12.850/13).

A principal diferença entre esses conceitos é o número de elementos necessários para configurar o crime: enquanto os dois primeiros exigem a associação de três ou mais pessoas, o terceiro exige quatro ou mais elementos.

No entanto, o conceito de crime organizado parece não mais abranger os fenômenos criminosos atuais. Nesse contexto, uma nova figura começa a surgir, conhecida como "crime institucionalizado", descrito por Pontes (2014, s/p) como um "novo animal da criminologia". Esse tipo de crime é extremamente perigoso, pois ocorre quando as estruturas criminosas se confundem com a própria estrutura do Estado.

As grandes decisões do Estado são tomadas em benefício do grupo criminoso, que visa maximizar seus lucros, e essas decisões são frequentemente tomadas em detrimento das políticas públicas. Ao contrário das organizações criminosas comuns, o crime institucionalizado não tem apenas um líder, mas uma estrutura em forma de teia, altamente colaborativa e simbiótica.

3 DA FRAUDE VIRTUAL COMETIDA POR ORGANIZAÇÕES CRIMINOSAS NO BRASIL

3.1 A definição jurídica de crimes digitais e a interpretação de organização criminosa de acordo com a Lei 12.850/2013

Os crimes digitais se aproveitam do uso da internet para atingir muitas vítimas em larga escala. A conexão de milhares de pessoas por meio de redes fixas ou móveis permite que, pelo

menos em uma tentativa de crime, haja pelo menos uma vítima, evidenciando a amplitude de alcance e acesso dos crimes digitais.

Contudo, é importante destacar que, apesar de as ações criminosas ocorrerem em um ambiente virtual tão vulnerável, essas práticas também existem no mundo real. Pinheiro (2010, p. 296) alerta para a transferência de crimes reais para o ambiente virtual, visando ampliar o número de vítimas:

> "A maioria dos crimes cometidos na rede ocorre também no mundo real. A internet surge apenas como um facilitador, principalmente pelo anonimato que proporciona. Portanto, as questões quanto ao conceito de crime, delito, ato e efeito são as mesmas, quer sejam aplicadas para o Direito Penal ou para o Direito Penal Digital. As principais inovações jurídicas trazidas no âmbito digital referem à territorialidade e a investigação probatória, bem como a necessidade de tipificação penal em algumas modalidades que, em razão de peculiaridades, merecem ter um tipo penal próprio." (PINHEIRO, 2010, p. 296).

Um exemplo de crime preexistente que pode ocorrer em redes sociais são os crimes contra a honra, como difamação, calúnia e injúria, que já são tipificados no Código Penal brasileiro.

Além disso, temos crimes como ameaça e "*revenge porn*", que é a divulgação de imagens e vídeos íntimos de ex-parceiros como forma de vingança após o fim do relacionamento, prática muito comum na era digital.

Dessa forma, os crimes digitais são compreendidos como condutas proibidas por lei que envolvem meios tecnológicos e são passíveis de sanção criminal, seja porque a conduta se destina a sistemas informatizados e dados, ou porque o meio utilizado é tecnológico, mesmo que o crime pudesse ser cometido de outra forma (CHAIA; et al, 2020).

Esses crimes podem ser divididos em dois grandes grupos: os crimes digitais propriamente ditos, que visam atingir bens jurídicos tecnológicos como dados criptografados e senhas, como disseminação de vírus e acesso não autorizado (*hackers*), e os crimes mistos ou impróprios. Damásio de Jesus (2016, p. 26) destaca para uma informação sobre a relação dos hackers com o Brasil:

> "Pesquisas sempre revelaram que o Brasil está na rota dos crimes cibernéticos. De acordo com a Polícia Federal, em notícia do ano de 2004, de cada dez hackers ativos no mundo, oito vivem no Brasil. Não bastasse, segundo o órgão, à época, dois terços dos responsáveis pela criação de páginas de pedofilia na internet, detectadas por investigações policiais brasileiras e no exterior, teriam origem brasileira" (JESUS, 2016, p. 26)

Por outro lado, os crimes digitais impróprios são definidos como condutas proibidas por lei cujo objetivo é atingir bens jurídicos tradicionais que não sejam tecnológicos, como a vida, a liberdade e a imagem, entre outros.

Como já mencionado, de maneira geral, a organização criminosa é uma associação de indivíduos com o objetivo de cometer crimes. No ambiente virtual, é comum que tais organizações acessem vários links e criem diversas formas de capturar dados bancários, números de telefone e outras informações usadas em práticas de estelionato. Essas organizações são clandestinas, ilícitas e têm um aparato operacional formal ou informal para cometer seus crimes.

A principal característica é a associação com propósitos comuns para práticas ilícitas. No Brasil, existem diversos tratados internacionais ratificados para coibir o crime organizado internacional, como a Convenção das Nações Unidas contra o Tráfico Internacional de Drogas de 1991, a Convenção das Nações Unidas contra o Crime Organizado Transnacional de 2004 e a Convenção das Nações Unidas contra a Corrupção de 2006.

De acordo com Alberto Franco (1994, p. 5), a legislação penal estabelece características da organização criminosa, que revelam os riscos envolvidos na formação dessas associações:

> "Caráter transnacional; aproveita-se de deficiências do sistema penal, a partir de sua estruturação organizacional e de sua estratégia de atuação global; atuação resulta em dano social acentuado; realiza várias infrações, com vitimização difusa ou não; aparelhado com instrumentos tecnológicos modernos; conexões com outros grupos criminosos, organizados ou não; mantém ligações com pessoas que ocupam cargos oficiais, na vida social, econômica e política; utiliza-se de atos de violência; e beneficia-se da inércia ou fragilidade de órgãos estatais" (FRANCO, 1994, p. 05).

A existência de um sistema organizado e estruturado por vezes dificulta o enfrentamento por parte das autoridades responsáveis. A infiltração de policiais em organizações criminosas é uma técnica utilizada para desmantelá-las. Essa técnica consiste na inserção de um agente treinado, com identidade oculta, que busca obter provas que comprovem as atividades ilegais da organização.

É importante destacar que, para além das definições de organização criminosa, é fundamental abordar também a associação criminosa, que consiste na união de diversas pessoas com a finalidade de realizar atividades que possam gerar lucro, sem que necessariamente envolvam práticas criminosas explicitas ou sem propósitos ilícitos.

Dessa forma, é possível compreender que a simples reunião de indivíduos não é suficiente para caracterizar uma organização criminosa, já que pode haver associação sem intenção inicial de cometer delitos, sendo a corrupção humana um fator preponderante na

criação desse tipo penal. Nesse sentido, tanto o Superior Tribunal de Justiça quanto o Supremo Tribunal Federal adotam o entendimento de que a associação criminosa é equiparada ao antigo tipo penal de quadrilha, atualmente denominado de associação criminosa:

> "Vale destacar que, malgrado na maioria das vezes a associação criminosa se forme para fazer da prática de delitos uma atividade lucrativa, a torpeza não se revela imprescindível. Há casos em que o agrupamento objetiva o cometimento de delitos sem nenhum propósito" (STF: HC 77.287/SP. rel. Min. Sydney Sanches, 1ª Turma, j. 17.11.1998; e HC 70.395/RJ, rel. Min. Paulo Brossard, 2ª Turma, j. 08.03.1994; no STJ: HC 123.932/SP, rel. Min. Arnaldo Esteves Lima, 5ª Turma, j. 16.06.2009).

Assim que um agente faccionado começa a fazer insinuações, elogios ou incitação a cometer crimes pela facção à qual pertence, pode-se usar a ideia de facções. Isso porque as organizações criminosas são grupos que se formam com o objetivo de praticar crimes e causar danos a terceiros. Na era digital, essas organizações são frequentemente responsáveis por aplicar golpes em usuários de redes sociais, tanto por meio de ligações fixas quanto pela internet.

3.2 Estelionatos e fraudes virtuais

É necessário fazer uma distinção penal entre a definição de estelionato e fraudes. De acordo com o artigo 171 do Código Penal, o estelionato consiste em "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" (BRASIL, 1940).

Sendo assim, o uso de artifícios como plataformas digitais, *links* fraudulentos, sites inexistentes e até mesmo vírus, são práticas comuns na obtenção de vantagens ilícitas no meio digital.

De acordo com Greco (2017, 513) a partir do artigo 171 "o Código Penal estabelece a fraude como elemento central do crime de estelionato". O autor Nucci (2017, p. 513) destaca que o estelionato é um crime que envolve, "o estelionato é um crime artístico, pois implica representação, convencimento, falas decoradas, cenários montados, figurantes e todos os aparatos necessários para enganar alguém com uma história; a única diferença de uma peça teatral bem produzida", exceto pelo fato de que o estelionatário não recebe aplausos, mas sim uma vantagem ilícita em prejuízo da vítima enganada.

Portanto, de acordo com o que foi dito, o criminoso utiliza de meios fraudulentos para enganar a vítima, com o objetivo de proteger o patrimônio. Conforme a afirmação de Cunha

(2017, s/p): "A incriminação do estelionato visa proteger a inviolabilidade patrimonial, violada pela prática de atos enganosos pelo agente".

Além disso, é importante destacar a explicação sobre o que se entende por artifício e ardil, como complementa Masson (2018, p. 447):

> A extorsão é crime pluriofensivo. A lei penal tutela o patrimônio, principalmente, pois o delito está previsto entre os crimes contra o patrimônio, mas não se olvida da integridade física e da liberdade individual, uma vez que para executá-lo o sujeito se vale de grave ameaça ou violência à pessoa. É preciso destacar que o patrimônio, como bem jurídico protegido pelo art. 158 do Código Penal, há de ser compreendido em sentido mais amplo do que a propriedade e a posse, ao contrário do que se dá no furto e no roubo, pois o tipo penal fala em "indevida vantagem econômica". Destarte, qualquer que seja a vantagem patrimonial obtida ou procurada pelo agente, em detrimento da vítima, estará caracterizado um dos requisitos da extorsão. De fato, é patrimônio, no contexto do crime em apreço, todo bem ou interesse cujo sacrifício represente, para o seu titular, um mal maior do que o prejuízo patrimonial correspondente à vantagem exigida pelo extorsionário. São exemplos de tais bens ou interesses a honra, a tranquilidade pessoal ou familiar, o crédito comercial etc. Contrariamente ao sustentado pela maioria da doutrina, não consideramos correto classificar a extorsão como crime complexo. Como se sabe, crime complexo é o que resulta da fusão de dois ou mais crimes (exemplos: roubo, latrocínio, extorsão mediante sequestro etc.). E, no terreno do delito tipificado pelo art. 158 do Código Penal, não se verifica tal fenômeno. Com efeito, a extorsão nada mais é do que uma espécie do gênero "constrangimento ilegal", art. 146: é o constrangimento ilegal qualificado pelo fim de indébita locupletação e que, por isso mesmo, é trasladado para a órbita dos crimes contra o patrimônio. Núcleo do tipo é "constranger", exatamente como no constrangimento ilegal, e no restante da descrição da conduta criminosa não se verifica a presença de nenhum outro comportamento que, por si só, constitua crime autônomo. Trata-se, portanto, de um constrangimento ilegal com finalidade específica. E nada mais (MASSON, 2018, p. 447).

É relevante destacar que o delito de estelionato pode ser cometido no meio digital, o que é pertinente ao tema abordado neste trabalho. Existem várias estratégias empregadas pelos criminosos para a execução desse crime, mas um exemplo pode ser citado para melhor compreensão do assunto.

Um exemplo de fraude cometida no meio virtual foi o caso da atriz Carolina Dieckmann, que teve fotos íntimas capturadas em seu computador pessoal e sofreu ameaças para que as fotos não fossem divulgadas publicamente (RUSSO; NEGRÃO, 2020).

A atriz Carolina Dieckmann teve sua privacidade invadida quando hackers invadiram suas contas de e-mails e acessaram seus arquivos pessoais, incluindo fotos íntimas. Os criminosos tentaram chantageá-la, pedindo dinheiro para não divulgar as imagens (POMPEU, 2022).

Todavia, a atriz recusou-se a ceder às ameaças e denunciou o caso à Delegacia de Repressão Contra Crimes de Internet, sob a liderança do delegado Gilson Perdigão, que iniciou uma investigação (FRANÇA; SILVA, 2017).

As fotos foram divulgadas em diversos endereços na internet, alcançando mais de 8 milhões de downloads e gerando grande repercussão nas redes sociais, com muitos usuários defendendo a atriz. O caso evidencia a vulnerabilidade da privacidade dos usuários na internet e a necessidade de medidas mais efetivas para garantir a segurança digital (FRANÇA; SILVA, 2017).

O autor desconhecido deste ataque de hackers conseguiu acessar o iCloud da atriz, que é um sistema de armazenamento na nuvem da empresa Apple. A partir daí, o invasor copiou as imagens pessoais da atriz e as usou para extorsão (FRANÇA; SILVA, 2017).

Antes do vazamento, Carolina Dieckmann relatou nas redes sociais que estava sendo alvo de uma tentativa de *hack* e que estava monitorando a situação. Na época do crime, ainda não havia uma tipificação penal específica para esse tipo de crime, e os quatro acusados foram indiciados por furto, extorsão qualificada e difamação, que não eram exatamente os delitos cometidos por eles. No entanto, após a repercussão do caso, o projeto de lei que já estava em tramitação no Congresso recebeu o apoio da atriz, evidenciando a necessidade de atualização da legislação para lidar com o crime cibernético (FRANÇA; SILVA, 2017).

Além disso, o uso de *links* fraudulentos para obter informações bancárias também é uma prática comum. Conforme alertado por Gil (2000, p. 114), o furto mediante fraude no meio digital é a ação mal-intencionada de causar danos a ativos intangíveis por meio de informações e procedimentos, com o objetivo de obter benefícios financeiros ou psicológicos.

Em virtude do aumento das práticas criminosas na era digital, torna-se cada vez mais importante o conhecimento e a conscientização dos usuários sobre as formas de fraude e os cuidados necessários para evitar tais crimes.

A proteção dos ativos intangíveis e a preservação dos dados pessoais se tornam desafios crescentes e, por isso, é fundamental a adoção de medidas preventivas e repressivas para garantir a segurança e a privacidade no ambiente digital. A seguir, serão apresentados as principais vítimas de fraudes virtuais perpetradas por organizações criminosas.

3.3 Fraudes virtuais cometidas por organizações criminosas: uma análise das principais vítimas

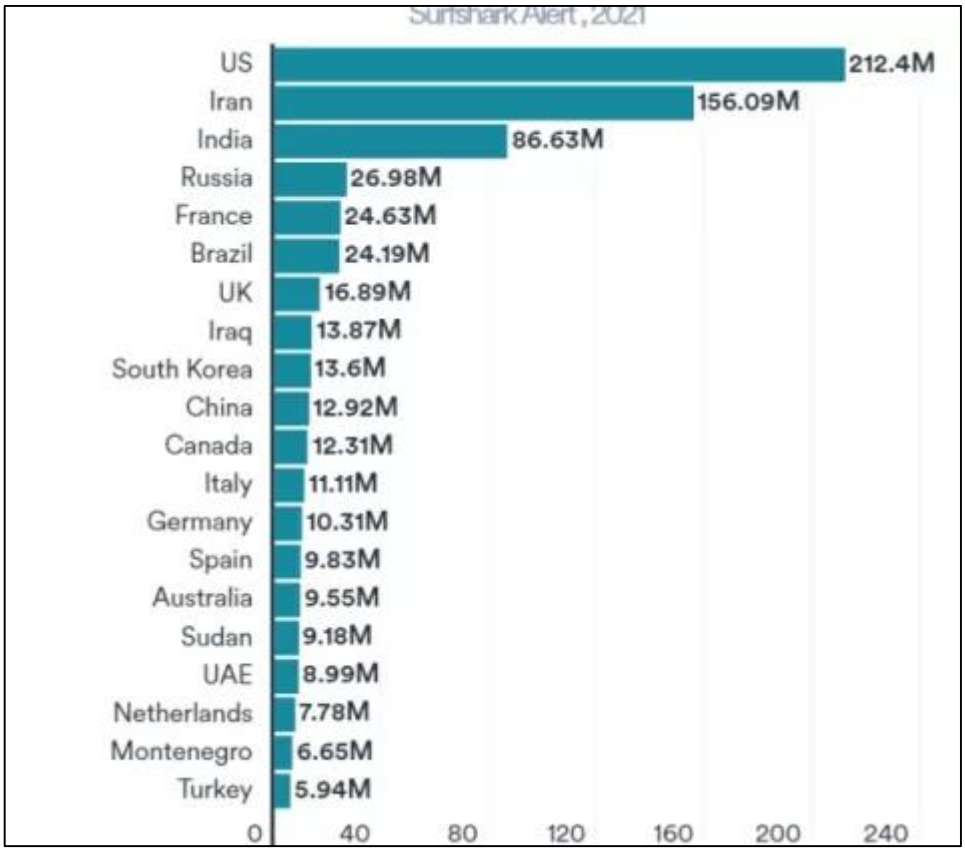
De acordo com um levantamento realizado pela empresa de serviços VPN Surfshark *apud* Machado (2022, s/p) o Brasil ainda enfrenta um cenário preocupante em relação aos

vazamentos de dados, pois apesar da queda de 31% no número de ocorrências entre 2019 e 2020, o país ocupa o sexto lugar entre as 20 (vinte) regiões mais afetadas pelo problema em 2020.

Estima-se que, somente em 2022 24,2 milhões (Vinte e quatro milhões e duzentos mil) perfis de brasileiros tenham tido suas informações expostas devido a ataques ou vulnerabilidades em sistemas (MACHADO, 2022).

Diante da pesquisa supramencionada foi elaborado um gráfico em barras exposto a seguir (figura 1):

Figura 1: Brasil fica em 6º lugar em ranking sobre vazamento de dados



Fonte: Surfshark (2021).

De acordo com o gráfico é possível afirmar que as violações de segurança cibernética são um problema global que afeta diversos países, inclusive os Estados Unidos, o Irã e a Índia. A pesquisa citada indica um aumento de 22% no número de contas vazadas nos Estados Unidos em relação ao ano anterior, demonstrando a importância de medidas eficazes de segurança cibernética para combater essas violações.

É notável também que, embora a Índia tenha sido classificada como o terceiro país mais afetado, ainda assim, foram comprometidas cerca de 86,6 milhões de pessoas, o que representa um número expressivo. Esses dados reforçam a necessidade de uma maior conscientização e investimentos em tecnologias de segurança cibernética para proteger as informações e dados pessoais dos usuários em todo o mundo.

Segundo pesquisa realizada pela Confederação Nacional de Dirigentes Lojistas (CNDL) e pelo Serviço de Proteção ao Crédito (SPC Brasil) *apud* Alvarenga (2021, s/p), o aumento significativo das compras online durante a pandemia de coronavírus resultou em um crescimento expressivo das fraudes financeiras na internet.

De acordo com o levantamento, que teve seus resultados antecipados ao G1, nos últimos 12 meses, 59% dos internautas brasileiros sofreram algum tipo de fraude financeira, representando um contingente de 16,7 milhões de pessoas. O estudo apontou que 51% das vítimas são mulheres, 49% são homens e 56% pertencem à classe C, enquanto 44% são da classe A/B. Além disso, a idade média das vítimas é de 39 anos, sendo que mais da metade (53,6%) possui ensino médio completo ou superior (ALVARENGA, 2021).

Conforme divulgado pela empresa de segurança digital PSafe *apud* Mandelli (2022, s/p), algumas práticas criminosas como o estelionato emocional, *catfishing*[3], falso namoro[4] e sextorsão[5] têm como alvo principal as mulheres. Segundo a pesquisa, uma em cada cinco mulheres brasileiras já foi vítima de fraudes virtuais.

Outro grupo vulnerável no caso de fraudes virtuais são os idosos. Conforme Capez (2016), é frequente a ocorrência de estelionatos cometidos por pessoas próximas e familiares de idosos.

O autor destaca que as estratégias utilizadas são diversas e a mais comum é relatada pelos próprios idosos, quando são enganados por familiares e amigos na hora do saque da aposentadoria no caixa eletrônico. Especialmente em casos de idosos analfabetos ou com pouca

---

[3] *Catfishing* é uma prática de fraude online em que uma pessoa usa uma identidade falsa para estabelecer um relacionamento ou enganar outras pessoas na internet. Esse termo surgiu em 2010, após o lançamento de um documentário intitulado "*Catfish*", que contava a história de um homem que havia sido enganado por uma pessoa que usava uma identidade falsa na internet (CASTRO; ZAGANELLI, 2020).

[4] O crime de falso namoro, também conhecido como romance scam, é uma forma de fraude na qual o criminoso cria um relacionamento falso com a vítima para obter benefícios financeiros ou pessoais. Essa prática é realizada por meio da internet, com o uso de perfis falsos em sites de relacionamento, redes sociais e aplicativos de mensagens. O termo romance *scam* surgiu nos Estados Unidos na década de 90 e começou a se popularizar no Brasil em meados dos anos 2000. Desde então, tem sido cada vez mais comum no país, afetando principalmente mulheres maduras e idosas (GONÇALVES, 2021).

[5] A sextorsão é um crime em que alguém usa imagens ou vídeos sexualmente explícitos de outra pessoa para extorqui-la, ameaçando divulgar o material. O termo surgiu fora do Brasil em 2012 e foi adotado no país em 2017 onde a magistrada Luiza de Moura Correia, da Central de Inquéritos de Teresina, no Estado do Piauí, proferiu a primeira sentença referente a um caso de estupro virtual decorrente de sextorsão (PRAXEDES, 2021).

compreensão do uso de tecnologias, alguns indivíduos se aproveitam da situação para receber a aposentadoria integral e repassar apenas uma pequena porcentagem ao idoso (CAPEZ, 2016).

Segundo Porto (2020) *apud* Redação (2020) o *phishing* é uma das fraudes mais comuns perpetrados contra idosos no ambiente virtual e tem como objetivo roubar dados pessoais, incluindo senhas, números de cartão de crédito e informações pessoais. Essa prática pode levar a novos crimes e afeta qualquer pessoa, mas é mais comum entre os idosos, que muitas vezes não possuem familiaridade com recursos tecnológicos e acabam caindo em golpes virtuais.

Os indivíduos da terceira idade, em especial, tendem a acreditar mais nas informações e são alvos frequentes de fake news. Alguns *hackers* se aproveitam dessa vulnerabilidade para programar *malwares* e obter vantagens ilícitas (PORTO, 2020 *apud* REDAÇÃO, 2020).

Como fora observado ao longo do estudo, os dados apontam que mulheres, adultos e idosos são os grupos mais vulneráveis a fraudes no ambiente virtual. A exposição excessiva das mulheres a crimes relacionados a pornografia de vingança e extorsão sexual é um fator preocupante. Além disso, a falta de conhecimento e a desinformação sobre práticas de segurança na internet entre a população mais velha é outro aspecto relevante.

Os adultos, por sua vez, muitas vezes estão mais expostos a práticas de *phishing* e roubo de identidade, uma vez que possuem maior renda e, consequentemente, movimentam mais dinheiro na internet. A crescente utilização de tecnologias digitais também contribui para que sejam mais expostos a práticas criminosas. No entanto, mesmo com a crescente utilização de tecnologias digitais, a população em geral ainda não está preparada para lidar com os riscos que o ambiente virtual pode apresentar.

Para mitigar o problema do estelionato perpetrado pelo crime organizado no ambiente virtual e as formas que a sociedade pode utilizar para sua proteção, é necessário que medidas de segurança sejam adotadas. É importante que a sociedade em geral tenha acesso a informações precisas e atualizadas sobre práticas de segurança na internet. Além disso, é necessário que o poder público implemente medidas efetivas de combate aos crimes virtuais, por meio da utilização de tecnologias e do fortalecimento das instituições responsáveis pela fiscalização e repressão desses crimes.

O próximo capítulo abordará os meios e alternativas jurídicas para mitigar o problema do estelionato perpetrado pelo crime organizado no ambiente virtual e as formas que a sociedade pode utilizar para sua proteção.

4 MEIOS E ALTERNATIVAS JURÍDICAS PARA MITIGAR E COMBATER A FRAUDE VIRTUAL PERPETRADA PELO CRIME ORGANIZADO

Toda sociedade contemporânea é marcada por uma rápida dinâmica de inovação e adaptação social, onde os avanços tecnológicos e o desenvolvimento de novos mecanismos de interação entre os indivíduos geram novas formas de convivência.

Em consequência, é necessária uma avaliação constante e aprimoramento legislativo em todos os aspectos da sociedade, incluindo a convivência humana na internet, que sofre mudanças diárias devido à criação de novos aplicativos, dispositivos e funções (TOMASEVICIUS FILHO, 2016).

O desafio diário das forças investigativas e do poder judiciário é enquadrar as condutas cometidas nestes meios de acordo com a legislação existente, e para isso, é fundamental que os órgãos responsáveis se reportem ao legislativo para o aprimoramento do conjunto normativo. (TOMASEVICIUS FILHO, 2016).

O uso cada vez mais difundido da *internet* e a constante evolução das tecnologias de informação têm permitido que as pessoas obtenham acesso mais fácil a informações e decisões mais rápidas. No entanto, o aumento da informatização também tem sido usado para fins criminosos, que são comumente referidos como "crimes virtuais" ou "crimes cibernéticos" (BRASIL, 2012a).

Os avanços tecnológicos têm motivado as instituições legislativas a se concentrarem cada vez mais em projetos de lei relacionados aos crimes cibernéticos. Seria um grande avanço se fosse criado um código que especificasse os crimes virtuais, abordando todos os seus aspectos e estabelecendo uma área policial especializada no assunto, com conhecimento avançado em computação para lidar com os conflitos de maneira mais habilidosa, facilitando a identificação dos criminosos virtuais.

É notável que o sistema jurídico ainda não está totalmente preparado para reprimir tais comportamentos e, portanto, se as leis relativas a esses crimes fossem aprimoradas, seria possível reduzir as taxas de criminalidade virtual. As casas legislativas federais brasileiras, Senado e Câmara, estão atentas a esse fenômeno social e muitos de seus legisladores estão trabalhando em projetos de lei relacionados aos crimes cibernéticos (SIQUEIRA, 2017)

As casas legislativas federais brasileiras, Senado e Câmara, têm se mostrado atentas ao fenômeno dos crimes virtuais e diversos projetos de lei relacionados a esse tema estão em tramitação.

Segundo a Revista “Em Pauta - O processo legislativo do Senado à Serviço da Cidadania” Ano V - nº 235 - Brasília, 10 de setembro de 2012, há vários projetos em destaque, incluindo o Projeto de Lei do Senado (PLS) nº 427, de 2011, apresentado pelo Senador Jorge Viana (PT-AC), o Projeto de Lei da Câmara (PLC) nº 35, de 2012, de autoria do Deputado Federal Paulo Teixeira (PT-SP) e o PL do SENADO nº 236, de 2012, de autoria do Senador José Sarney (PMDB-AP).

O Projeto de Lei da Câmara (PLC) nº 35, de 2012, aprovado na Câmara dos Deputados, trata da tipificação criminal de vários delitos informáticos a serem incluídos no Código Penal. O projeto aguarda deliberação do plenário do Senado Federal, já tendo sido aprovado nas comissões temáticas.

Na mesma linha, o Senado Federal possui o Projeto de Lei do Senado (PLS) nº 427, de 2011, que busca alteração no Código Penal para inserir o tipo penal de “crime de atentado contra a segurança de meio ou serviço de comunicação informatizado”. Ambas as iniciativas visam aprimorar a legislação brasileira sobre crimes virtuais.

Na Câmara dos Deputados, a CPI dos Crimes Cibernéticos, instalada em 2016, também gerou propostas de lei, incluindo a perda dos instrumentos do crime doloso destinados à prática reiterada de crimes, como computadores, celulares e dispositivos eletrônicos utilizados em crimes virtuais, e a ampliação da abrangência do crime de invasão de dispositivo informático. (BRASIL, 2012a; BRASIL, 2016)

Diversas propostas de lei relacionadas à crimes cibernéticos estão em tramitação no Congresso Nacional, como é o caso do Projeto de Lei do Senado (PLS) nº 427/2011, apresentado pelo Senador Jorge Viana (PT-AC), que aguarda relatório para ser apreciado pela Comissão de Constituição e Justiça do Senado. Já o Projeto de Lei da Câmara (PLC) nº 35/2012, de autoria do Deputado Federal Paulo Teixeira (PT-SP), foi aprovado na Câmara dos Deputados e aguarda deliberação do plenário do Senado.

Dentre as propostas decorrentes da CPI dos Crimes Cibernéticos, destacam-se projetos que preveem a perda dos instrumentos do crime utilizados em delitos informáticos, a ampliação da abrangência do crime de invasão de dispositivo informático e a inclusão dos crimes praticados contra ou mediante computador no rol das infrações de repercussão interestadual ou internacional.

Além disso, há propostas que visam alterar o Marco Civil da Internet para determinar a indisponibilidade de cópia idêntica de conteúdo infringente e permitir o bloqueio de aplicações de internet por ordem judicial. No entanto, essas iniciativas enfrentam dificuldades de aprovação devido a questões normais do trâmite legislativo e a questões políticas.

Os profissionais responsáveis por lidar com os crimes cibernéticos no Brasil, incluindo Polícias Civis e Federais, o Ministério Público, a Defensoria e o Poder Judiciário, têm o papel de detectar, investigar, prevenir, mitigar, acusar e julgar tais delitos. Em relação especificamente aos profissionais da segurança pública, além das habilidades necessárias para investigar crimes comuns, é necessário que possuam conhecimentos especializados, habilidades e atitudes que lhes permitam identificar, obter, preservar e analisar as evidências digitais de uma maneira que garanta sua admissibilidade em juízo e respeite as exigências da norma processual penal, como a cadeia de custódia.

Dada a escassez de mão de obra qualificada nesta área e o aumento da sofisticação do crime organizado, é necessário promover a cooperação público-privada, com empresas e órgãos da justiça criminal trabalhando juntos na aplicação da lei. A cooperação entre todos os segmentos da sociedade, entidades públicas e privadas, pode resultar em um novo paradigma de combate sistemático a essa ameaça, aumentando os riscos para os *cibercriminosos* e fornecendo benefícios ao trabalhar em conjunto em direção a um objetivo comum.

A adoção de padrões internacionais e de leis modelos é fundamental para enfrentar o cibercrime, por isso é importante que o Brasil adira à Convenção de Budapeste, que preza pela harmonização e simetria nos procedimentos investigatórios.

Na investigação, é possível utilizar a computação e técnicas de Inteligência Artificial, como o Aprendizado de Máquina, para automatizar a análise de dados e acelerar a solução de problemas. Uma proposta é a criação de um Projeto Estadual de combate a fraudes bancárias eletrônicas, em que a Polícia Civil tenha acesso a uma base de dados estruturada para identificação de correlação de vínculos e auxílio na tomada de decisões.

As ferramentas disponíveis para análise de grande volume de dados são úteis, pois proporcionam uma inteligência visual e identificam a relação com outras entidades. Algumas ferramentas disponíveis no mercado são o software “I2” da IBM, o sistema NEXUS da Dígitro e o WEBTIGER da Wytron. A análise de vínculo e a técnica baseada em tecnologia da informação são uma moderna metodologia de investigação que amplia a capacidade de visualização da complexidade do crime com recurso gráfico, conforme ensina Ferro Junior (2007, p.70).

> Facilita a verificação de elementos associados numa relação em teia complexa, por meio de ligações dos fatos, associações de pessoas, empresas, vínculos de contatos telefônicos, do fluxo financeiro et. Torna possível a construção da informação com significado (conhecimento) para a investigação (FERRO JUNIOR, 2007, p. 70 *apud* JORGE; VERGINE, 2022).

A investigação de crimes cibernéticos envolve lidar com muitas relações diversas e complexas, tornando essencial o uso da tecnologia e a capacidade de analisar e compreender o contexto em sua totalidade. O sucesso do trabalho policial, portanto, depende da capacidade de sintetizar dados distintos e reunir tudo em um único ambiente gráfico para melhor compreensão do esquema criminoso.

5 CONSIDERAÇÕES FINAIS

Considera-se por fim, que a análise da prática do crime de fraude perpetrado por organizações criminosas no ambiente virtual é um tema extremamente relevante para o Direito Penal, que tem como objetivo garantir a ordem social e a proteção dos indivíduos.

Evidenciou-se os estelionatos e fraudes virtuais são crimes cometidos no ambiente virtual, utilizando-se de técnicas fraudulentas para enganar as vítimas e obter vantagens ilícitas. Esses crimes podem ser praticados através de diversas formas, como phishing, smishing, pharming, entre outras, e são uma preocupação crescente no contexto atual de intensa utilização da tecnologia.

No âmbito do Direito Penal, é de extrema importância o estudo e a pesquisa sobre os estelionatos e fraudes virtuais, com o objetivo de entender as formas de cometimento desses crimes, bem como as formas de prevenção e repressão. Além disso, é necessário aprimorar a legislação e os mecanismos de investigação e punição, para garantir a proteção dos direitos das vítimas.

O interesse pelo assunto no Brasil começou a ganhar destaque a partir dos anos 2000, com o crescente aumento da utilização da internet e o surgimento de novas formas de cometimento desses crimes. Desde então, houve um aumento significativo na produção acadêmica e na realização de pesquisas sobre o tema, com o objetivo de aprofundar o conhecimento sobre os estelionatos e fraudes virtuais e buscar soluções efetivas para combatê-los.

A observação feita no texto sobre a vulnerabilidade de certos grupos, como idosos e mulheres, em relação a fraudes virtuais é relevante e deve ser levada em consideração no âmbito jurídico.

A falta de familiaridade com a tecnologia e a excessiva confiança em mensagens falsas podem deixar essas pessoas mais expostas aos riscos de fraudes virtuais. Nesse sentido, é importante que sejam criadas medidas de proteção e conscientização específicas para esses

grupos, com o objetivo de reduzir a vulnerabilidade e evitar que sejam vítimas de crimes virtuais.

Além disso, é necessário que haja uma atuação eficiente do Estado na punição dos autores desses crimes, de modo a coibir a prática dessas condutas ilegais. Portanto, a análise crítica do texto é positiva, pois destaca a importância de se levar em consideração a vulnerabilidade de determinados grupos na prevenção e repressão dos crimes virtuais, contribuindo para uma maior proteção e segurança dos cidadãos.

O estudo mostrou que os cibercriminosos são cada vez mais sofisticados e estão constantemente buscando novas maneiras de cometer crimes virtuais, o que exige aprimoramento constante das leis e políticas públicas de combate a esses crimes.

A pesquisa destacou a importância da adoção de padrões internacionais e de leis modelos no enfrentamento do cibercrime, assim como a necessidade de cooperação público-privada para otimização dos recursos humanos e materiais, e a adoção de técnicas de Inteligência Artificial para automatizar e acelerar a solução de problemas de investigação.

É fundamental que novas pesquisas sejam realizadas para aprimorar as estratégias de combate ao crime organizado no ambiente virtual, incluindo o desenvolvimento de novas tecnologias de segurança e a promoção de treinamentos e capacitações para os profissionais da área. Com isso, será possível garantir a efetividade das medidas de prevenção, detecção e punição dos crimes virtuais, protegendo a sociedade e mantendo a segurança jurídica no mundo virtual.

Diante da complexidade do crime de fraude perpetrado por organizações criminosas no ambiente virtual, é notório que a análise e prevenção desses delitos exige ações integradas e especializadas de diversas áreas, como do Direito Penal, da Tecnologia da Informação e da Segurança Pública.

Assim, a pesquisa se mostra relevante e contribui para o desenvolvimento de novas estratégias e tecnologias de combate ao crime de fraude cibernética. Recomenda-se que futuras pesquisas possam ampliar e aprofundar as análises realizadas pelos autores, a fim de aprimorar ainda mais as medidas de prevenção e combate a esse tipo de delito, que traz grandes prejuízos para a sociedade.

No mais, é necessário que haja uma maior conscientização por parte da população quanto à segurança digital e aos cuidados que devem ser tomados para evitar fraudes e golpes virtuais. Somente com ações integradas e constantes será possível reduzir os impactos negativos causados pela prática de crimes cibernéticos por organizações criminosas.

REFERÊNCIAS

ALVARENGA, Darlan. **Cresce nº de consumidores vítimas de fraudes financeiras no Brasil; veja ranking das mais recorrentes.** G1 Economia, 24 jun. 2021. Disponível em: https://g1.globo.com/economia/noticia/2021/06/24/cresce-no-de-consumidores-vitimas-de-fraudes-financeiras-no-brasil-veja-ranking-das-mais-recorrentes.ghtml. Acesso em: 20 abr. 2023.

BORGES, Paulo César Correa. **O Crime Organizado**. São Paulo: Ed. UNESP, 2002, p. 16.

BRASIL, Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 20 abr. 2023.

BRASIL, Decreto nº 5.015, de 12 de março de 2004. **Convenção das Nações Unidas contra o Crime Organizado Transnacional.** Diário Oficial da União, Brasília, DF, 15 mar. 2004. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm. Acesso em: 20 abr. 2023.

BRASIL, Lei nº 12.694, de 24 de julho de 2012. **Processo e o julgamento colegiado em primeiro grau de jurisdição de crimes praticados por organizações criminosas.** Diário Oficial da União, Brasília, DF, 25 jul. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/L12694.htm#:~:text=Disp%C3%B5e%20sobre%20o%20processo%20e,de%2023%20de%20setembro%20de. Acesso em: 20 abr. 2023.

BRASIL, Senado Federal. "O Senado e os Crimes cibernéticos". **Rev. Em Pauta**. Ano V - nº 235 - Brasília, 10 de setembro de 2012a.

BRASIL, Lei nº 12.850, de 2 de agosto de 2013. **Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal.** Diário Oficial da União, Brasília, DF, 5 ago. 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 20 abr. 2023.

BRASIL, Câmara dos Deputados. **CPI dos Crimes Cibernéticos, de 04 de maio de 2016.** Brasília, 2016. Disponível em: < http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D%3E+RCP+10/2015> Acesso em: 20 de mar. 2023.

CASTRO, Cera Daltro de A; ZAGANELLI, Vetis M. **Catfishing**: crime de falsa identidade? **Revista de Estudos Jurídicos da UNESP**, a.24, n.40, 2020. Disponível em: https://ojs.franca.unesp.br/index.php/estudosjuridicosunesp/article/view/3099. Acesso em: 20 de mar. 2023.

CAPEZ, Eduardo. **Estelionato no Brasil:** Idosos vítimas fáceis. 2016. In: AZEVEDO, Ueslaine Cardoso Silva. **A problemática do estelionato praticada contra idosos.** Especialização em Educação Matemática da UEG Campus Cora Coralina, Goiás, 2017. Ano 2017, n. 02, v. 011. Disponível em: https://www.anais.ueg.br/index.php/eem/article/view/9686/6963. Acesso em: 20 abr. 2023.

CHAIA, Raphael Rios; et al. **Crimes cibernéticos:** as invasões de privacidade mediante os novos meios tecnológicos. In: Anais do 10º Congresso Internacional de Ciências Criminais - PUCRS, Direito Penal - Vol. 03. São Paulo, 2020.

CNDL, Confederação Nacional de Dirigentes Lojistas; SPC BRASIL, Serviço de Proteção ao Crédito. In: ALVARENGA, Darlan. **Cresce nº de consumidores vítimas de fraudes financeiras no Brasil; veja ranking das mais recorrentes.** G1 Economia, 24 jun. 2021. Disponível em: https://g1.globo.com/economia/noticia/2021/06/24/cresce-no-de-consumidores-vitimas-de-fraudes-financeiras-no-brasil-veja-ranking-das-mais-recorrentes.ghtml. Acesso em: 20 abr. 2023.

CUNHA, Sanches Rogério. **Manual de direito penal parte especial.** 9ª Ed. Editora jusPODVM. 2017.

DIPP, Gilson Langaro. **A delação ou colaboração premiada**: uma análise do instituto pela interpretação da lei. Brasília: IDP, 2015, p. 11.

FERNANDES, Antonio Scarance. O equilíbrio entre a eficiência e o garantismo e o crime organizado. In: **Revista Brasileira de Ciências Criminais**. São Paulo: RT, ano 16, n. 70, p. 229-268, jan./fev. 2008.

FRANÇA, Karolinne Pires Vital; SILVA, Márcio Ferreira da. **Efetividade da Lei Carolina Dieckmann**. 2017. Trabalho de Conclusão de Curso (Graduação em Direito) - Faculdade Evangélica de Rubiataba. Disponível em: http://repositorio.aee.edu.br/jspui/handle/aee/17530. Acesso em: 20 Abr. 2023.

FRANCO, Alberto Silva. **Crimes hediondos.** 6. ed. São Paulo: Revista dos Tribunais, 2007, p. 67.

GIL, Antônio de Loureiro. **Fraudes Informatizadas.** 2.ed. São Paulo: editora Atlas, 2000.

GODOY, Luiz Roberto Ungaretti de. **O Crime Organizado e seu Tratamento Jurídico Penal.** Rio de Janeiro: Elsevier, 2011, p. 61.

GONÇALVES, Dayane Maciel. **O canto da sereia – da captação de vítimas de estelionato virtual por meio das redes sociais.** Monografia (Bacharelado em Direito) - Faculdade Evangélica de Rubiataba, sob orientação da professora Mestra Leidiane de Morais e Silva Mariano. Rubiataba, GO, 2021, 37p. Disponível em: http://repositorio.aee.edu.br/bitstream/aee/20162/1/2022%20-%20TCC%20-%20DAYANE%20MACIEL%20GON%c3%87ALVES.pdf. Acesso em: 2023-04-22.

GRECO, Rogério. **Código Penal Comentado.** 11ª Ed. Editora Impetus. 2017

JESUS, Damásio de; MILAGRE; José Antonio. **Manual de crimes informáticos.** São Paulo: Saraiva, 2016.

JORGE, Higor Vinicius Nogueira; VERGINE, Gaetano. **Relatos sobre a investigação de crimes cibernéticos**. São Paulo: Editora JusPodivm, 2022.

MACHADO, Simone. **Brasil é 6º país com mais ataques; tentativas de fraude chegaram a 1 milhão.** UOL Tilt, São José do Rio Preto, 08 fev. 2022. Disponível em:

https://www.uol.com.br/tilt/noticias/redacao/2022/02/08/dia-internacional-da-internet-segura-brasil-tem-o-que-comemorar-veja.htm. Acesso em: 20 abr. 2023.

MANDELLI, Mariana. **Todos somos vulneráveis a golpes na internet**. Folha UOL, São Paulo, 10 fev. 2022. Disponível em: https://www1.folha.uol.com.br/educacao/2022/02/todos-somos-vulneraveis-a-golpes-na-internet.shtml. Acesso em: 20 abr. 2023.

MASSON, Cleber. **Direito pena, parte especial.** 11ª ed. Editora Método. 2018.

MINGARDI, Guaracy. **O Estado e o crime organizado.** Boletim IBCCRIM, São Paulo, n. 21, p.03, set. 1994. In: ANSELMO, Márcio Adriano. **O conceito de organização criminosa e crime institucionalizado.** Conjur, 27 de junho de 2017, Disponível em: https://www.conjur.com.br/2017-jun-27/conceito-organizacao-criminosa-crime-institucionalizado. Acesso em: 20 de abr. 2023.

NUCCI, Guilherme de Souza. **Curso de direito penal parte geral**. 3ª Ed. Editora Forense 2018

PINHEIRO, Patrícia Peck. **Direito Digital.** 4.ed. rev., atual. e ampl. São Paulo: Saraiva, 2010.

POMPEU, Ana Luiza Brandão Calil. **Crimes cibernéticos:** a ineficácia da Lei Carolina Dieckmann. 2022. Trabalho de Conclusão de Curso (Graduação em Direito) - Faculdade Facmais. Disponível em: http://65.108.49.104/handle/123456789/509. Acesso em: 20 Abr. 2023.

PONTES, Jorge. **Corrupção sistêmica institucionalizada**. Rio de Janeiro, 2014. Disponível em http://oglobo.globo.com/opiniao/corrupcao-sistemica-institucionalizada-14905059. Acesso em 20 de mar. 2023.

PRAXEDES, Luanna Zane de Souza. **Da sextorsão:** crime cibernético de adequação típica plural. 2021. 49 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Pontifícia Universidade Católica de Goiás, Escola de Direito e Relações Internacionais, Goiânia, 2021. Orientador: Gaspar Alexandre Machado de Sousa. Referee: Gaspar Alexandre Machado de Sousa, Eufrosina Saraiva Silva. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1418. Acesso em: 20 abr. 2023.

PORTO, Thiago. In: REDACÃO. **Golpes virtuais contra idosos cresceram durante a pandemia.** PROTESTE, Brasil, 2020. Disponível em: https://conectaja.proteste.org.br/golpes-virtuais-contra-idosos-cresceram-durante-a-pandemia/. Acesso em: 20 abr. 2023.

RUSSO, G. S; NEGRÃO, A. S. Organização criminosa e os crimes da era digital**. Boletim Jurídico,** 2020. Disponível em: http://boletimjuridico.publicacoesonline.com.br/85336/. Acesso em: 20 de mar. 2023.

SIQUEIRA, Marcela Scheuer et al. Crimes virtuais e a legislação brasileira. **(Re)Pensando o Direito – Rev.** do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13 (2017). Disponível em http://local.cnecsan.edu.br/revista/index.php/direito/article/view/468. Acesso em: 01 mar. 2023.

STF. **Habeas Corpus 70.395/RJ**. Relator Ministro Paulo Brossard. Segunda Turma. Julgado em 8 de março de 1994. Rio de Janeiro: STF, 1994.

STF. **Habeas Corpus 77.287/SP**. Relator Ministro Sydney Sanches. Primeira Turma. Julgado em 17 de novembro de 1998. São Paulo: STF, 1998.

STJ. **Habeas Corpus 123.932/SP**. Relator Ministro Arnaldo Esteves Lima. Quinta Turma. Julgado em 16 de junho de 2009. São Paulo: STJ, 2009.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estud. av**., São Paulo, v. 30, n. 86, p. 269- 285, Abr. 2016. Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142016000100269&lng=en&nrm=iso>. Acesso em: 01 mar. 2023.