O MUNDO DIGITAL E SEUS DESAFIOS: INFORMAÇÕES IMPORTANTES PARA A PREVENÇÃO E COMBATE AOS CRIMES CIBERNÉTICOS E SUAS VARIAÇÕES

Ana Paula Mendes de Oliveira
Beatriz Maria de Oliveira Santos
Daniel Dias Araújo
Davi Gomes Cavalcante
Luiz Eduardo de Carvalho Brito
Mariana Cunha Alves da Silva
Sara Neves Rozendo
Thamirys Moreira Batista[1]

Resumo

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

O mundo atual é movimentado pela internet e pelo meio digital. Dessa forma, as pessoas precisam entender como se comportar na internet e terem consciência de como agirem em caso de serem vítimas crimes contra a honra praticados na internet, estelionato eletrônico e demais golpes. Ainda, os idosos são um público vulnerável, visto que não têm vasto conhecimento no que diz respeito à tecnologia. Então esse é um tema de grande importância, uma vez que irá promover conscientização ao público, ajudando até mesmo no combate a essas questões apresentadas. A informação promove melhoras na sociedade. Dessa forma, acredita-se que o presente trabalho contribuirá nesse sentido. Ainda, é importante porque direcionará o público para a prevenção dos golpes praticados na internet.

1. Introdução

[1] Graduandos em *Direito* pelo Centro Universitário UniProcessus.

A ascensão das tecnologias digitais revolucionou a forma como interagimos, vencemos, e até mesmo cometemos crimes. A era digital trouxe não apenas oportunidades de inovação e conectividade, mas também desafios complexos relacionados à segurança cibernética e aos crimes digitais. Este projeto tem como objetivo investigar e analisar o cenário dos crimes digitais, compreendendo suas origens, impactos e as medidas necessárias para prevenção e combate. Na sociedade contemporânea altamente interconectada, os crimes digitais abrangem uma ampla gama de atividades maliciosas que exploram vulnerabilidades em sistemas, redes e dispositivos eletrônicos. Desde o roubo de informações fornecidas até ataques cibernéticos em larga escala, os crimes digitais apresentam desafios únicos que exigem uma abordagem multidisciplinar para entendê-los e lidar com eles eficazmente. Nossa pesquisa investigará os diferentes tipos de crimes digitais, incluindo, mas não se limitando a: 1. Fraudes Online: Exploração de vulnerabilidades para roubo de informações financeiras, números de cartão de crédito e identidades. 2. Ciberataques: Ataques direcionados a sistemas computacionais. Por meio das redes sociais (Instagram) e da produção de panfletos afim de alertar a sociedade sobre os perigos do mundo digital.

2. Desenvolvimento do tema pesquisado

2.1. Apresentação do tema: "O que são crimes cibernéticos?"

Notoriamente, os casos de golpe nas redes sociais e demais mídias vem se tornando cada dia mais recorrentes e por consequência trazendo consigo inúmeros problemas à sociedade. Nesse parágrafo, iremos falar sobre um crime bastante atual e como ele afeta o nosso cotidiano, o estelionato eletrônico.

O crime de estelionato está presente na sociedade desde muito tempo, contudo assim como todos os outros crimes já encontrados no Código

Penal, este passou por modificações e acréscimo de qualificadoras, para fins de sanar/diminuir os danos causados.

O estelionato eletrônico, conhecido como fraude eletrônica, nada mais é que um criminoso se aproveitar das mídias sociais para defraudar pessoas com os seus dados pessoais.

O grande diferencial do presente crime, advém das formas que os criminosos utilizam para se beneficiar, sendo o objeto do crime o meio eletrônico.

No que diz respeito ao estelionato, a lei 14.155/2021 fez algumas mudanças significativas no artigo 171 do Código Penal, como exposto a seguir:

Fez a inserção § 2º-A, com a previsão de qualificação do estelionato por intermédio de fraude eletrônica.

Adicionou § 2º-B, como forma de majoração de pena em referência ao parágrafo acima citado.

Converteu a composição da causa de majoração da pena do § 4º.

Vale mencionar, que a alteração do Código Penal se fez com a finalidade de moderar a prática desse crime, e trazer uma penalidade mais soturna.

Importante mencionar que antes da majoração da pena, esta deveria ser dobrada, e atualmente ela pode ser aumentada de 1/3 até o dobro da pena.

Desse modo, temos expressamente que a fraude eletrônica vem se tornando cada dia mais assíduo, devido ao desenvolvimento das mídias sociais.

O estelionato de forma não qualificada, detém de uma pena de 1 a 5 anos de prisão. Já a fraude eletrônica perfaz a pena de 4 a 8 anos de reclusão, cumulada a multa. Além do mais, pode ser majorada até ⅔, caso o delito seja praticado em servidores, sendo estes computadores, que se encontre fora do país.

2.2. Crimes contra a honra praticados na internet.

É importante destacar que nem tudo é opinião, muitas vezes pode ser crime. Nessa era em que tudo é digital, as pessoas acham que podem dizer o que quiserem sem medo de repreensão, a nossa Constituição Federal estabelece direitos e garantias individuais que vão assegurar o direito e a existência digna da pessoa humana. Portanto, a CF visa, dentre vários outros direitos, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, assegurando também o direito de indenização pelo dano decorrente de sua violação.

Sabemos que existem três tipos de crimes contra a honra, que são: injúria, calúnia e difamação. Mas como vemos isso no mundo da internet? Ocorre que muitas pessoas

não sabem como esses crimes funcionam, e na maioria das vezes, com a intenção de fazer uma “simples fofoquinha” e comentários sobre os outros acabam por destruir a imagem de alguém que está por trás, sem saber se podem elas ser inocentes ou não. Vamos fazer uma explicação pratica sobre cada um deles:

Caracteriza-se crime de calúnia, por exemplo, expor na internet o nome e foto de uma pessoa como autor de um homicídio, sem ter provas. Quando, por exemplo, uma atriz tem detalhes de sua vida privada exposta em uma revista, ainda que o fato seja verdadeiro, divulgá-lo constitui difamação. E por outro lado, chamar uma pessoa de “ladrão”, “agressivo”, “mentiroso”, é cometer injúria, pois ofende pessoalmente a vítima caracterizando o crime.

Tais características traz a suposta sensação de impunidade para os delinquentes que buscam denegrir a imagem de terceiros, tornando-a atrativa. Nesse sentido, o STJ se manifestou em razão desses fatos de modo que os crimes contra a honra praticados em ambientes virtuais são formais, consumam-se independente do resultado naturalístico.

Cada vez mais há maiores números de expansão desses ambientes virtuais no mundo, como por exemplo, o WhatsApp, Instagram e Facebook que trazem ferramentas de conversas privadas que, ao contrário dos outros tipos de publicações, limitam o acesso apenas aos usuários da respectiva conversa. Ao analisar casos assim, o STJ firmou entendimento no sentido que a competência para a apuração e julgamento desses delitos é do local em que a vítima tomou conhecimento da ofensa.

É possível também cometer dois ou mais dos crimes ao mesmo tempo. Exemplo: acusar alguém de mentirosa (injúria), afirmando que ela agrediu determinada pessoa e está sendo processada por isso (calúnia), no meio de um grupo de pessoas dizendo para tomar cuidado com ela (difamação). O código penal tipifica esses crimes e vai além, pois existem as agravantes sobre esses crimes, em especial temos uma com a intenção de focar: “no artigo

141 §2° diz " Se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplica-se em triplo a pena".

Sendo assim, qualquer dos crimes descritos acima, cometidos em conversas, privadas ou não, em qualquer rede social terão a pena aumentada em 3 vezes.

Já parou para pensar que o que você deixa de fazer na nossa lei tem relevância? Não podemos deixar de destacar que há várias possibilidades em que a omissão de uma pessoa traz consequências.

Se alguém toma conhecimento da prática de algum desses crimes e nada faz para impedir a repercussão que isso pode causar, ele está de omitindo, se tornando, portanto, o omisso coautor do delito. Tudo que acontece nas redes sociais se espalha rapidamente, sabemos que infelizmente depois de feito fica difícil ser apagado e esquecido, é bom pensar em ambos os lados.

Não nos limitamos só nos danos psicológicos e morais a vítima, ao contrário do que muitos delinquentes pensam, a internet não é terra sem lei, a todos pseudo valentes que se encorajam apenas atrás de uma tela fiquem espertos, imputar falsamente crimes a pessoas inocentes, destruindo suas imagens e imputando ofensas abomináveis não é liberdade de expressão, e sim crime.

2.3. Como se proteger dos crimes cibernéticos, quais os cuidados e os principais golpes.

Para compreender quais são os principais tipos de crimes cibernéticos e quais são as orientações para se proteger e evitar que mais pessoas sejam atingidas, é necessário assimilar o que de fato são os crimes cibernéticos.

Os crimes cibernéticos são também conhecidos por “crimes de internet”, como a própria nomenclatura diz são os delitos que acontecem no espaço cibernético (O espaço cibernético é a instauração de uma rede de todas as memórias informatizadas e de todos os computadores – conceito disposto na Palestra realizada no Festival Usina de Arte e Cultura, promovido pela Prefeitura Municipal de Porto Alegre).

Tratando ainda desse ponto, cabe mencionar que o ordenamento jurídico brasileiro já vem regulamentando alguns crimes cibernéticos, é importante explicitar que com os avanços tecnológicos e as constantes variações da modalidade criminosa, fixa-se um desafio para o ordenamento jurídico.

Nesse sentido, é oportuno mencionar que o Brasil, em 2021 aderiu à Convenção de Budapeste de cooperação jurídica internacional no combate aos crimes cibernéticos. Por meio dessa colaboração as autoridades brasileiras terão acesso mais ágil a provas eletrônicas produzidas sob jurisdição estrangeira.

Feita essa análise inicial, trataremos sobre os principais crimes dessa modalidade. Os crimes cibernéticos mais comuns são os de invasão de dispositivos, furto qualificado, extorsão, cryptojacking (O uso não autorizado de dispositivos para mineração de

criptomoedas), venda de jogos de azar ilegais, espionagem, estelionato e os ataques cibernéticos.

Quando se fala nos ataques, estamos diante de uma gama de assuntos que perpassam desde os crimes relacionados a honra (Calúnia, difamação e injúria) até a invasão de dispositivos informáticos para a disseminação de vírus e malware que coleta dados (e-mail, telefone, dados bancários e etc).

Podemos ainda citar a distribuição descomedida de notícias falsas, as falsificações de dados e distribuição de materiais pornográficos e de pedofilia.

Veja que esse assunto é muito amplo, os delitos são variados. Cada uma dessas práticas possui pontos sensíveis, com modus operandi distintos. Mas o cuidado que a população deve tomar são os mesmos.

Passamos agora a analisar quais são as precauções que todos devem ter para evitar golpes. Especialistas reforçam que a primeira dica de proteção é evitar navegar em sites suspeitos e clicar em links desconhecidos, pode ser golpe. Atente-se a veracidade das mensagens e na dúvida não siga os comandos encaminhados. Esse cuidado parece simples, mas evita que invasores acessem o seu dispositivo.

Evite também abrir e-mails de spam pois o indicie de invasão é alto. Outra dica importante, é o fortalecimento da segurança das contas. A maioria dos sites e aplicativos oferecem a autenticação de dois fatores, essa é uma forma de dificultar o acesso de criminosos. É necessário ainda alertar que ao criar uma senha evite combinações óbvias, como por exemplo, números em sequência, datas de aniversário e nomes de pessoas da família. As senhas fracas ameaçam a segurança e facilitam os ataques.

Seguindo a linha de cuidados, recomenda-se manter o software e o sistema operacional atualizados pois isso previne a vulnerabilidade dos dispositivos.

Cabe orientar os usuários que antes de realizar qualquer ação precipitada analise bem a mensagem recebida. Desconfie de solicitações de informações pessoais, como telefone,

CPF, RG, informações da conta do banco ou de qualquer aplicativo financeiro.

Não clique em links sensacionalistas, não ligue em números sugeridos por mensagens de texto, desconfie de promessas milagrosas e “oportunidades” vantajosas demais. Verifique sempre a reputação da empresa, pesquise sobre o assunto e se existem outros relatos sobre o mesmo caso.

Reforça-se o cuidado em não passar os dados pessoais, número de cartão ou informações bancárias a ninguém. Também não recomendamos investimentos, pix, transferências a terceiros sem a devida verificação.

Muitos golpistas se aproveitam da vulnerabilidade das vítimas para efetuar o golpe, utilizam mensagem com propostas irrecusáveis, garantias de dinheiro rápido e fácil. Investimentos que prometem lucros exorbitantes sem nenhum esforço, prática ou conhecimento. Alguns criminosos colocam fotos, vídeos e depoimentos de pessoas que supostamente realizaram aquela operação e estão realizados. Alerta-se que essas mídias em sua maioria são falsas e usadas de forma ilegal. Usam imagens de pessoas aleatórias e sem autorização para convencer pessoas a caírem no golpe.

É importante orientar e alertar os amigos, familiares e colegas pois qualquer pessoa pode ser vítima.

Caso você seja vítima de um crime cibernético, recomendamos que realize o mais rápido possível o bloqueio do cartão utilizado, seja virtual ou não; informe à instituição financeira que foi vítima de golpe; reúna elementos probatórios, como conversas, prints e comprovantes; e procure a delegacia para registrar um Boletim de ocorrência.

2.4. O que é o estelionato eletrônico (Fraude eletrônica)?

Notoriamente, os casos de golpe nas redes sociais e demais mídias vem se tornando cada dia mais recorrentes e por consequência trazendo consigo inúmeros problemas à sociedade. Nesse parágrafo, iremos falar sobre um crime bastante atual e como ele afeta o nosso cotidiano, o estelionato eletrônico.

O crime de estelionato está presente na sociedade desde muito tempo, contudo assim como todos os outros crimes já encontrados no Código

Penal, este passou por modificações e acréscimo de qualificadoras, para fins de sanar/diminuir os danos causados.

O estelionato eletrônico, conhecido como fraude eletrônica, nada mais é que um criminoso se aproveitar das mídias sociais para defraudar pessoas com os seus dados pessoais.

O grande diferencial do presente crime, advém das formas que os criminosos utilizam para se beneficiar, sendo o objeto do crime o meio eletrônico.

No que diz respeito ao estelionato, a lei 14.155/2021 fez algumas mudanças significativas no artigo 171 do Código Penal, como exposto a seguir:

Fez a inserção § 2º-A, com a previsão de qualificação do estelionato por intermédio de fraude eletrônica.
Adicionou § 2º-B, como forma de majoração de pena em referência ao parágrafo acima citado.
Converteu a composição da causa de majoração da pena do § 4º.
Vale mencionar, que a alteração do Código Penal se fez com a finalidade de moderar a prática desse crime, e trazer uma penalidade mais soturna.
Importante mencionar que antes da majoração da pena, esta deveria ser dobrada, e atualmente ela pode ser aumentada de 1/3 até o dobro da pena.
Desse modo, temos expressamente que a fraude eletrônica vem se tornando cada dia mais assíduo, devido ao desenvolvimento das mídias sociais.
O estelionato de forma não qualificada, detém de uma pena de 1 a 5 anos de prisão.
Já a fraude eletrônica perfaz a pena de 4 a 8 anos de reclusão, cumulada a multa.
Além do mais, pode ser majorada até ⅔, caso o delito seja praticado em servidores, sendo estes computadores, que se encontre fora do país.

2.5. Acessibilidade para idosos

Como bem sabemos a tecnologia abre portas para avanços em diversas áreas, porém também pode indiretamente estabelecer algumas barreiras, por exemplo no caso dos idosos e pessoas de idade mais avançada que passaram a maior parte de suas vidas sem o contato direto com tanta tecnologia no seu dia a dia.
A tecnologia já vinha em um cenário de crescente nos últimos anos e com a pandemia da Covid-19 e consequentemente o isolamento social essa crescente ficou ainda maior com aumento de atividades online em praticamente todos os âmbitos da sociedade e muitos idosos tiveram o primeiro contato com celulares por exemplo. A falta de conhecimento com relação ao ambiente virtual junto ao processo acelerado de inclusão digital dos idosos, gerou possibilidades para pessoas mal intencionadas praticarem crimes cibernéticos.
Uma empresa chamada LexisNexis Ricks Solutions de análise de risco realizou um levantamento e apontou que a população com mais de 75 anos, proporcionalmente, é a que mais sofre com crimes cibernéticos. O relatório mostra que isso também pode acontecer dentro do ambiente familiar pelos próprios parentes e pessoas próximas,

que utilizam os aparelhos celulares das vítimas para fazer transferências, compras e empréstimos.

Por essa razão é natural que o público idoso encontre mais dificuldade para se adaptar a essa nova era, pois diferentemente da conhecida como “geração Z“ não nasceram imersos num ambiente regido pela tecnologia e dessa forma podem acabar sendo alvos ainda mais fáceis em golpes eletrônicos e semelhantes. Portanto se faz necessário buscar por soluções e meios para facilitar o acesso das pessoas mais velhas a tais informações.

Uma pesquisa realizada pelo IPESPE, entrevistou em cinco regiões do país aproximadamente 3 mil pessoas, exatamente sobre a inclusão digital de pessoas mais velhas e foi constatado que cerca de 70% dos idosos não se sentem seguros na internet justamente por medo de golpes e fraudes que são os principais motivos juntamente com a dificuldade de adaptação.

Os principais golpes realizados contra idosos ocorrem por meio de e-mails, sms, até mesmo por ligações telefônicas, geralmente falando sobre questões de aposentadoria dentre outros para roubar os dados e até dinheiro desses idosos.

Outro método comumente utilizado é através de links falsos também com intuito de roubar dados, clonagem de cartão, contas e mais. Nestes golpes, em que os infratores enviam um link para capturar dados pessoais são potencialmente mais perigosos, pois as vítimas muitas vezes também compartilham esse conteúdo e acabam fazendo com que outras pessoas também caiam.

Primeiramente para proteger o público mais velho é necessário trazer a informação, ou seja, por tantos meios quanto possível. Campanhas a respeito podem ser muito eficazes para levar as informações mais relevantes a esse público.

Além disso algo mais prático e no alcance de qualquer pessoa é que os próprios jovens e pessoas familiarizadas a tecnologia levar essas informações aos idosos que conhecem e até mesmo oferecer ajuda se for necessário, pois em muitos casos será preciso. E por fim uma alternativa para mais segurança de suas contas e dados é a autenticação em dois fatores para que assim apenas uma pessoa terá acesso a essa conta de e-mail por exemplo através do método escolhido.

2.6 A utilização de deepfake para estelionato eletrônico

A inteligência a artificial é um dos termos mais empolgantes para discussão no século XXI. A possibilidade de criação de máquinas que podem exercer tarefas que exigem tempo e trabalho, como tomar decisões, raciocinar e aprender, antes era uma utopia que hoje se tornou uma realidade palpável. Dessa forma, a IA se tornou uma aliada valiosa na resolução de problemas complexos, desde previsões meteorológicas mais precisas até os diagnósticos médicos mais confiáveis. Assim, essa tecnologia promete uma revolução em áreas cruciais como educação, transporte, saúde e segurança.

É crucial destacar, por exemplo, que a automação, impulsionada pela IA, está transformando indústrias inteiras, tornando processos mais eficientes, rápidos custos e melhorando a qualidade. Na indústria automobilística, a IA é fundamental para o desenvolvimento de veículos independentes, com o potencial de tornar o transporte mais seguro e eficiente.

Além disso, a IA desempenha um papel crucial na personalização de produtos e serviços. Algoritmos de recomendação, como os usados por empresas de streaming de vídeo e música, são gerenciados por Inteligência Artificial, e proporcionam experiências mais relevantes e interessantes para os consumidores. Isso não apenas aumenta a satisfação do cliente, mas também impulsiona a fidelidade à marca e os lucros.

Na área da saúde, a IA está causando um impacto significativo, onde ela é utilizada para auxiliar os médicos em diagnósticos e tratamentos mais adequados para os pacientes. Para mais, dispositivos de saúde conectados à IA podem monitorar pacientes em tempo real, fornecendo dados insuficientes aos médicos. Isso é particularmente valioso para pacientes com doenças crônicas.

Essa crescente ascensão da IA vem de avanços significativos em algoritmos de aprendizado de máquina e poder computacional. Essa combinação permitiu o processamento de grandes volumes de dados em tempo real, possibilitando a IA a tomar decisões complexas e aprender com base em experiências passadas.

No entanto, cabe destacar sobre os desafios éticos e sociais associados a IA, incluindo questões de privacidade, discriminação algorítmica e desigualdade no acesso a tecnologias de IA avançadas.

Aplicativos como o FaceApp, por exemplo, que conquistaram grande aceitação do público, têm a habilidade de substituir o rosto de um indivíduo pelo de outro. Embora à primeira vista possam parecer que não fazem mal a ninguém, eles têm suscitado

debates sobre como os produtos da adulteração fotográfica poderão ser usados no futuro. Esse tipo de manipulação, é chamada de deepfake.

Os deepfakes são uma aplicação de IA que utiliza algoritmos de aprendizado para criar conteúdo de áudio e vídeo altamente convincente e realista, muitas vezes replicando o rosto e a voz de uma pessoa com a intenção de enganar ou manipular.

Os deepfakes usam softwares para mapear os traços faciais, expressões e movimentos labiais de uma pessoa e aplicá-los a outra em tempo real. Isso pode resultar em vídeos aparentemente autênticos de pessoas fazendo ou dizendo coisas que nunca disseram.

Essa aplicação é utilizada em diversas áreas, desde entretenimento e arte até aplicações mais maliciosas, como disseminação de desinformação, chantagem e fraude. É assim que os sistemas de reconhecimento facial estão se tornando notavelmente mais precisos, representando um risco potencial.

Com o avanço das técnicas de Inteligência Artificial, agora é possível realizar substituições de maneira quase indetectável. Isso marca um desenvolvimento que gera preocupações, uma vez que indivíduos de má-fé podem usar essa tecnologia para fins criminosos. Algumas pessoas também usam os deepfakes para criar vídeos pornográficos, o que é ilegal em muitos países.

Um exemplo ilustrativo aconteceu durante a eleição de 2022, quando a âncora do Jornal Nacional, Renata Vasconcellos, tornou-se alvo de um deepfake. Um vídeo forjado começou a circular nas redes sociais e em aplicativos de mensagens instantâneas, como o WhatsApp, gerando muitos debates.

A apresentadora mostrava o candidato a presidente Jair Bolsonaro em primeiro lugar, com 44% nas pesquisas de intenção de voto, e Luiz Inácio Lula da Silva em segundo lugar, com 32%. Contudo, a verdade era que Lula era o primeiro, com 44% das intenções dos votos, e Bolsonaro o segundo, com 32%.

Ainda houve outra situação em que William Bonner supostamente chamava o candidato Luiz

Inácio Lula da Silva de “ladrão”. Entretanto, a voz que parecia ser a de Bonner, na verdade, foi gerada artificialmente a partir de um texto escrito.

A mais recente produção da TV Globo, a novela “Travessia”, revisita o tema dos deepfakes. A protagonista da história, Brisa (interpretada por Lucy Alves), torna-se alvo desse tipo de manipulação de mídia e, como resultado, é associada a um caso

de rapto de bebês, após terem criado uma montagem com imagens dela encontradas em seu perfil no Instagram.

A novela foi inspirada no caso real de Fabiane Maria de Jesus, uma mulher vítima de deepfake, que infelizmente levou a uma grande fatalidade.

Através da plataforma Facebook, uma notícia falsa envolvendo Fabiane, começou a ser compartilhada em 2104. Ela acabou sendo associada a um sequestro de crianças com a intenção de rituais de magia negra. A jovem faleceu na manhã de 5 de maio de 2014, dois dias após ter sido brutalmente agredida por um grupo de moradores no Guarujá, na região do bairro Morrinhos.

Outro exemplo, foi uma organização criminosa especializada em fraude em contas bancárias, alvo de uma operação da Polícia Civil do Distrito Federal (PCDF). O grupo havia roubado em torno de R$ 338 mil de várias pessoas moradoras do DF e ainda de outros locais do Brasil. Foram cumpridos três mandados de busca e apreensão em Taguatinga e Águas Claras.

Wilson Peres, o diretor da divisão de fraudes, esclareceu que os responsáveis enviavam mensagens de texto aos clientes, informando sobre questões nas contas bancárias ou solicitando uma atualização de informações cadastrais. As mensagens enviadas pelos criminosos, continham um link que fazia com que as vítimas instalassem um programa em seus aparelhos. Esse programa possibilitava o acesso dos criminosos à conta bancária das vítimas.

Como mencionado anteriormente, apesar de parecerem inofensivos, os deepfakes representam uma ameaça devido à sua facilidade de criação e disseminação. Portanto, é essencial estar atento e seguir um guia para evitar cair em armadilhas. Primeiro, verifique a fonte da notícia e procure por confirmações em outras; analise o conteúdo da notícia em busca de distorções ou informações melhores e observe se há algum viés político ou ideológico; ao assistir a vídeos, preste atenção no áudio, pois a tecnologia ainda não é perfeita e pode apresentar ruídos; além disso, observe o movimento dos lábios, que às vezes pode parecer artificial; se houver suspeitas de que uma notícia seja falsa, é fundamental realizar uma pesquisa mais profunda.

Por outro lado, é importante reconhecer que o deepfake também tem potencial para aplicações positivas. Pode ser usado em simulações e treinamentos em ambientes virtuais, proporcionando experiências de aprendizado e experimentação em cenários seguros. Por exemplo, na área da saúde, médicos e cirurgiões podem praticar

procedimentos complexos virtualmente antes de realizá-los em pacientes reais, o que pode aumentar a segurança e a eficácia.

No entanto, à medida que a tecnologia de deepfake continua a evoluir, é crucial que a sociedade esteja atenta aos riscos envolvidos. Devem ser inovadoras medidas de regulamentação e segurança para evitar abusos, como a difamação ou o uso indevido dessa tecnologia para enganar o público. Além disso, a conscientização sobre a existência e os riscos dos deepfakes é fundamental para as pessoas poderem tomar decisões informadas e críticas ao consumir conteúdo digital.

Em resumo, o futuro dos deepfakes é promissor em termos de avanços tecnológicos, mas também exige no que diz respeito às questões éticas e de segurança que ele suscita. Portanto, à medida que nos adentramos nesse território em constante evolução, é essencial que a sociedade esteja preparada para lidar com as complexidades que surgem, buscando um equilíbrio entre a inovação tecnológica e a ética.

3. Considerações Finais

Com o presente trabalho, conclui-se que apesar da tecnologia ter mudado o mundo de uma forma muito positiva, apresenta perigos à sociedade. Isso porque há muitos crimes cometidos via internet e por falta de informação as pessoas acabam sendo vítimas de tais delitos. Dessa forma, a informação previne e ajuda a combater ações de criminosos e de grupos organizados que são especialistas em cibercimes. Por fim, a sociedade tem que sempre ter em mente que os grupos vulneráveis precisam de auxílio em diversos aspectos, inclusive no que diz respeito à conscientização e ensino da tecnologia a pessoas idosas, com o intuito de protegê-las de golpes e demais crimes cometidos na internet.

Referências

BONIFÁCIO, Trevis. O que é inteligência artificial. *Tecnoblog.* Acesso em: 22 ago. 2023. Disponível em <https://tecnoblog.net/responde/o-que-e-inteligencia-artificial/&gt>

CAVALCANTE, Marcos André Lopes. Lei 14.155/2021: promove alterações nos crimes de violação de dispositivo informático, furto e estelionato. *Dizer o Direito*. Acesso em: 29 ago. 2023. Disponível em

<https://www.dizerodireito.com.br/2021/05/lei-141552021-promove-alteracoes-nos.html#:~:text=A%20pena%20%C3%A9%20de%20reclus%C3%A3o,qualquer%20outro%20meio%20fraudulento%20an%C3%A1logo.>
Correio Brasiliense. Acesso em 22 ago. 2023. Disponível em <<https://www.correiobraziliense.com.br/cidades- df/2022/12/5057594-suspeitos-de-desviar-rs-338-mil-de-contas-bancarias-sao-alvos-de- operacao.html&gt>

GARIBE, Adriana. Os crimes cibernéticos no Direito Digital. *Conjur.* Acesso em: 29 ago. 2023. Disponível em < https://www.conjur.com.br/2022-set-29/adriana-garibe-direito-digital-crimes-ciberneticos#:~:text=Os%20crimes%20cibern%C3%A9ticos%20no%20Direito%20Digital&text=Os%20crimes%20digitais%20podem%20ser,de%20um%20novo%20tipo%20penal>

KOVACKS, Leandro. O que é um crime cibernético? 3 casos populares. *Tecnoblog.* Acesso em 27 ago. 2023. Disponível em < https://tecnoblog.net/responde/o-que-e-um-crime-cibernetico-3-casos-populares/>

LÉVY, Pierre. Publicação, reprodução, execução: direitos autorais. In: FESTIVAL Usina de Arte e Cultura, Portos Alegre, outubro 1994.

MENDES, Paz. Crimes Cibernéticos no Brasil: conheça os tipos, suas penas e agravantes. *Paz Mendes.* Acesso em 28 ago. 2023. Disponível em <https://www.pazmendes.com.br/crimes-ciberneticos-no-brasil/>

PEREIRA, Maria Fernandes. Deepfake: como funciona e o que seu futuro reserva. *Politize.* Acesso em 22 ago. 2023. Disponível em: << https://www.politize.com.br/deepfake-como-funciona/&gt>.

Polícia Civil do Distrito Federal. Acesso em 22 ago. 2023. Disponível em <https://www.pcdf.df.gov.br/noticias/11362/pcdf-deflagra-operacao-deep-fakel >

PUCRS. Acesso em: 22 ago. 2023. Disponível em <https://www.pucrs.br/blog/inteligencia-artificial-na-medicina&gt>

SANTOS. Oito anos após mulher ser espancada até a morte em SP, fake news segue fazendo vítimas como o turista queimado vivo no México. Acesso em 22 ago. 2023. Disponível em <https://g1.globo.com/sp/santos-regiao/noticia/2022/06/15/oito-anos-apos-mulher-ser- espancada-ate-a-morte-em-sp-fake-news-segue-fazendo-vitimas-como-o-turista-queimado- vivo-no-mexico.ghtml>.