**FRAUDES VIRTUAIS EM TEMPOS DE INTELIGÊNCIA ARTIFICIAL**

Jossandra Victoria dos Santos Fontenele Andrade ¹

Estefane Gabriele Araújo de Oliveira ¹

Paulo Victor de Sousa Lopes ¹

Sérgio Ricardo Soares ²

**RESUMO**

O presente artigo tem por objetivo analisar a incidência da Inteligência Artificial na criação de novas práticas de fraudes virtuais, trazendo uma análise crítica de estudos acerca do tema para que se possa constatar a contribuição dessa nova ferramenta para a realidade criminosa. Nesse viés, a metodologia utilizada foi o método de pesquisa exploratório bibliográfico, buscando apoio na legislação brasileira, mais especificamente no Código Penal, projetos de lei em discussão e ainda na doutrina e artigos pertinentes ao tema, utilizando como base de dados o Google Acadêmico. Em vista disso, o trabalho aborda inicialmente a definição de fraude e sua migração para o meio virtual, além de deixar claro o conceito de Inteligência Artificial, para que se possa então estabelecer ligação entre ambos. Feito isso, são apresentados exemplos de fraudes em que se utiliza essa ferramenta tecnológica para fundamentar a pesquisa, além da atuação legislativa do Brasil perante o uso da inteligência artificial nesse meio. No que diz respeito a conclusão ficou evidenciado que a Inteligência Artificial é de grande influência para a prática de tais delitos de fraude, além de que ficou demonstrado a necessidade da regulamentação de tal ferramenta.

**Palavras-chave:** Crimes. Fraudes. Inteligência Artificial

¹Graduandos em direito- Christus Faculdade do Piauí

²Professor orientador- Christus Faculdade do Piauí

**1 INTRODUÇÃO**

É incontestável que as tecnologias trouxeram grandes avanços para a sociedade, sendo o processo de virtualização o qual se vive nos últimos anos um grande exemplo de praticidade para a vida humana. No entanto, ao passo que a sociedade adentra no mundo virtual, surge também a prática de crimes nesse ambiente, já que os conflitos tendem a acompanhar a vida social.

Nesse âmbito, cabe pontuar em destaque a prática da fraude, um dos crimes predominantes no ciberespaço que visa enganar o usuário para obter vantagens em relação a este. Diante de tal cenário, surge ainda a inteligência artificial, uma ferramenta tecnológica imprescindível para a sociedade, mas que tem sido vista pelos golpistas como uma nova arma para praticar esse delito, gerando assim golpes virtuais mais sofisticados e de difícil identificação pela vítima, já que o recurso traz uma falsa segurança para a fraude.

Em vista disso, faz-se necessária a análise sobre a incidência dessa ferramenta na prática de fraudes virtuais. Logo, o presente estudo justifica-se pelo seu relevante valor social, uma vez que as pessoas estão cada vez mais suscetíveis a sofrerem golpes no meio virtual do que fora dele. Espera-se contribuir para o conhecimento da comunidade acerca do uso da Inteligência Artificial para a realização desses crimes, servindo não apenas para título de conhecimento, mas também como um alerta para essa nova onda de golpes no meio virtual.

**2 OBJETIVO**

Como exposto anteriormente, apesar da inteligência artificial ser essencial para a sociedade em diversas áreas, há indivíduos que fazem uso dessa importante ferramenta para cometer diversos crimes, sobretudo as fraudes virtuais.

Nesse viés, podemos destacar que o objetivo geral do presente trabalho é analisar a incidência da inteligência artificial na criação de novas práticas de fraudes virtuais, buscando especificamente expor os golpes originados através do mau uso

dessa tecnologia e verificar se esta contribui para o aumento das fraudes, investigando apanhados concretos que corroborem para a validação da pesquisa.

**3 FRAUDE E SUA MIGRAÇÃO PARA O MEIO VIRTUAL**

Para compreender o tema com êxtase, é essencial esclarecer do que se trata uma fraude. Dessa forma, a fraude é uma prática que visa obter vantagens ilegítimas sobre alguém, agindo o fraudador com persuasão para convencer a vítima a entregar o que este deseja obter. Nesse âmbito, conceitua-se a fraude, de forma ampla, como um esquema criado e usado para obter ganhos pessoais (WENDT; JORGE, 2012, p.74).

Mediante o exposto, essa conduta pode ser praticada de várias formas, encontrando como principal tipificação no Código Penal Brasileiro o art. 171, que dispõe em seu caput: “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”, possuindo pena de reclusão, de um a cinco anos e multa (BRASIL, 1940).

Além disso, conforme a realidade social se modifica ao longo da história, os crimes também se adequam para acompanhar esse novo cenário, surgindo assim novos crimes e novas formas de comete-los. Desse modo, diante do cenário de entrada da sociedade para o mundo digital nos últimos anos, é compreensível que as fraudes tenham migrado para esse meio, visto que isso é um reflexo do novo contexto social.

Nesse enredo, as fraudes virtuais são os mesmos delitos citados anteriormente, mas efetuados através do ciberespaço, onde, muitas vezes, a própria vítima, sem perceber, acaba contribuindo para que o criminoso obtenha vantagem contra ela. Essa prática tem aumentado no país e sido realizada de diversas formas.

Cabe destacar que essa modalidade de fraude recentemente entrou como forma qualificada no Código Penal Brasileiro por meio do artigo 172, § 2°-A, que dispõe sobre a fraude eletrônica da seguinte forma:

§ 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.

Apesar do delito ter recebido punição mais severa no Código Penal, a investigação na esfera digital ainda é um desafio para as instituições policiais, que não dispõem de recursos e qualificação frente às técnicas de fraudes cada vez mais sofisticadas, havendo a necessidade de adaptações para refletir essa nova realidade.

**4 O QUE É INTELIGÊNCIA ARTIFICIAL?**

É certo dizer que hoje a inteligência artificial está mais em alta do que nunca, contudo o que poucos imaginam é que essa tecnologia já nos rodeia a muito tempo tendo seus primeiros passos por volta de 1950, fazendo dela hoje algo essencial e indispensável em nosso meio, visto que esta controla transações bancárias, sistemas de energia, sistemas de voo e transporte e demais fatores.

Pode-se afirmar que a maior qualidade da inteligência artificial é a capacidade de aprender sozinha, além de sempre estar em evolução, assim como um ser humano. Para aferir se uma máquina realmente está como um grau de inteligência comparado a de um humano, Alan Turing criou um teste que consiste em uma pessoa, chamado de interrogador, conversando com uma máquina e com uma outra pessoa sem que as veja. No momento em que o interrogador não conseguir distinguir quem é a máquina e quem é a pessoa a inteligência artificial é considerada inteligente por ter conseguido se passar por humano.

A vista disso, não é de se estranhar quem veja a inteligência artificial com maus olhos, seja por achar perigosa essa autonomia da máquina ou pelo medo de ser substituído por ela. Contudo, foi exatamente por esses dois pontos que ela foi inventada, para substituir o labor humano com o maior grau de eficácia e autonomia possível, dessa concepção nascendo o desejo de dar um cérebro às máquinas.

**5 CASOS DE FRAUDES VIRTUAIS COM O USO DA INTELIGÊNCIA ARTIFICIAL**

À proporção que a inteligência artificial trouxe grandes benesses e se tornou indispensável para nosso meio, também se transformou em uma grande arma na posse de golpistas, sendo utilizada de forma maliciosa para cometer crimes. Ocorre que o fácil acesso à ferramenta trouxe a oportunidade de criar aspectos mais sofisticado às fraudes, sendo pouco identificadas no campo cibernético.

As vítimas dificilmente conseguem distinguir a ocorrência do golpe, já que o recurso da inteligência artificial passa uma falsa sensação de segurança, fazendo com que sejam induzidas a cometer erros e o golpista obtenha êxito. Assim sendo, serão abordados a seguir os principais mecanismos de IA que vêm sendo utilizados para a prática fraudulenta no ciberespaço.

* 1. **Deep fakes**

As *deep fakes* são produzidas a partir do uso de técnicas de aprendizado profundo utilizando-se de Redes Neurais Generativas Adversariais (GANs), que são

um tipo de manipulação das máquinas para que estas venham a aprender habilidades. Nesse sentido, tal técnica é utilizada para cometer fraudes roubando dados da vítima, seja uma foto ou uma gravação de áudio. Em seguida, uma rede neural generativa adversarial é treinada com esses dados, criando imagens, áudios e vídeos falsos, sendo aperfeiçoados até que se pareçam tão realistas que o próprio programa não consegue distinguir qual imagem é verdadeira ou falsa.

Nesse sentido, o fraudador utiliza esse conteúdo para manipular a vítima e induzi-la ao erro, fazendo com que esta acredite estar conversando com um conhecido, com o intuito de conseguir algo em troca, seja dinheiro ou imagens comprometedoras. No Brasil, o caso ocorreu com o influenciador Dario Centurione, quando seu pai, acreditando estar falando com Dario, transferiu para o fraudador a quantia de R$600,00 (seiscentos) reais. Nesse viés, torna-se clara a importância de uma mudança significativa da legislação, para que crimes como este venham a ser punidos.

* 1. **ChatGPT**

O Chat GTP é uma ferramenta de IA desenvolvida pela OpenAI que se tornou bastante popular no ciberespaço, tendo objetivo de criar conteúdo de forma rápida e eficiente. A tecnologia usa algoritmo baseado em redes neurais, o que permite interagir em linguagem natural com o usuário a partir do processamento de uma grande quantidade de dados. Nesse âmbito, cabe destacar que a facilidade da ferramenta em criar conteúdo tem atraído também sua utilização para fins maliciosos,

onde cibercriminosos se valem do recurso para criar e aperfeiçoar golpes em grande escala, como é o caso da prática de *phishing*. Em vista disso, a citada tecnologia é capaz de criar sites fraudulentos, tornando-os mais realistas e confiáveis, trazendo assim maior efetividade nessa modalidade de fraude.

Para explicitar essa situação, de acordo com Roy (2023), o golpista passa várias solicitações ao Chat GTP projetadas de forma a contornar as medidas de filtragem da ferramenta, possibilitando a criação de um código-fonte para um site de *phishing* que seja muito parecido com o site de uma organização popular, o que traz uma falsa segurança ao usuário e o faz compartilhar seus dados sensíveis.

A partir da implantação do código-fonte em um domínio, o site fraudulento torna-se ativo, partindo o cibercriminoso para a criação de cadeias completas de e-mails enganosos também com o uso do ChatGPT, que proporciona textos aprimorados e sem erros gramaticais, o que torna a fraude muito mais convincente e eficaz. Logo, tal ferramenta demonstra a possibilidade da inteligência artificial não só de inovar nos golpes, mas também os tornar mais eficazes.

* 1. **Bots do Telegram**

O Telegram, aplicativo de mensagens que veio para competir com o Whatsapp, ganhou popularidade no Brasil por volta de 2015 por sua praticidade de uso e pelo seus Bots, abreviação de *robot*, robô em inglês, que são usados em sua maioria para piratear séries, filmes, livros, entre outras funcionalidades.

Ademais, muitas pessoas confundem um Bot com uma IA, porém são programas diferentes, já que a inteligência artificial é muito superior, uma vez que se

aproxima da inteligência humana, sendo ela capaz de evoluir cada vez mais. Já os Bots, só podem executar tarefas pré-estabelecidas, sendo uma ferramenta muito limitada em comparação com a IA, mas ainda sim tem suas utilidades.

Cabe destacar que junto com as benesses da tecnologia, também vêm os efeitos nocivos, uma vez que a internet é vista como uma terra sem lei por muitos, não seria então diferente dentro da plataforma de mensagens em questão. Os bots do Telegram são comumente usados para a aplicação de fraudes no ambiente digital, assim com afirma Botton, 2022:

[...] bots vêm assumindo nos últimos dois anos um papel essencial na dinâmica dos fraudadores, pois são amplamente utilizados nas fraudes por automatizarem inúmeras tarefas, como realização de consultas de informações pessoais, venda de números de cartões de crédito, testes de validade de dados de cartões de crédito, venda de checkers (testadores de logins de lojas ou cartões), entre outras funcionalidades, economizando

tempo e trabalho dos fraudadores, que utilizarão tais informações para posterior uso em compras on-line fraudulentas.

Logo, é evidente que a má utilização dessa tecnologia na plataforma venha a se agravar cada vez mais, juntamente com a evolução dessas ferramentas, pois apesar de ilícita, é um meio lucrativo e de pouco risco para o fraudador, uma vez que este dificilmente é identificado por ficar atrás de uma tela, o que dificulta sua localização e impede sua responsabilização por suas práticas ilegais, sendo necessário que ocorra a criação, modificação e endurecimento das leis que tratam sobre o tema.

**6 ATUAÇÃO LEGISLATIVA DO BRASIL PERANTE O USO DA INTELIGÊNCIA ARTIFICIAL**

A partir da evolução tecnológica e com a migração dos crimes para o meio virtual, faz-se necessária a modificação e criação de novas leis para que tais crimes não fiquem impunes. Desse modo, a partir da análise da legislação brasileira, percebemos que existem lacunas presentes na lei, que corroboram para que a prática de delitos virtuais ocorra com frequência.

Nesse sentido, o Projeto de Lei 3800/2023 elaborado pelo deputado Acácio Favacho tem como proposta a modificação do Código Penal Brasileiro, visando dobrar a penalidade imposta para o delito de fraude eletrônica, quando esta for cometida pelo uso de Inteligência Artificial, como demonstrado nos exemplos citados acima. Tal modificação pretende atuar como um meio para a diminuição de tais crimes. Logo, tal

alteração demonstra que existem lacunas que urgem ser preenchidas não somente no código penal, mas também em toda a legislação brasileira.

À vista disso, mesmo com recentes discussões acerca da criação de novas leis que visem fiscalizar o uso da inteligência artificial, não existe até o presente momento nenhuma lei que vise tipificar as fraudes cometidas por este meio. Ademais, além da criação de novas leis é necessário que ocorra também a modificação de leis já

existentes, como verifica-se no exemplo citado acima, para que desse modo a legislação encontre-se sempre em atualização, assim como a sociedade está em constante evolução.

**7 METODOLOGIA (OU DESCRIÇÃO DA EXPERIÊNCIA)**

Foi utilizado no presente trabalho o método de pesquisa exploratório bibliográfico para chegar na melhor solução possível para o problema em questão. Foram realizadas buscas por publicações que visassem a contemplar a problemática das Fraudes digitais em tempos de inteligência artificial. As bases de dados usados como referência foram Google Acadêmico, artigos pertinentes, a legislação competente, a jurisprudência e os projetos de lei ainda em discussão.

O estudo terá caráter exploratório do tipo qualitativo, uma vez que serão estudadas as informações obtidas das pesquisas feitas para que seja possível solucionar o problema do modo mais eficaz possível.

**8 RESULTADOS E DISCUSSÃO**

Relativo aos apanhados, utilizou-se como embasamento o Código Penal Brasileiro, em específico o título dos crimes contra o patrimônio. Trouxemos em questão a qualificadora do estelionato denominada fraude eletrônica, que tipifica o delito trabalhado no presente artigo. Contudo, observamos que o uso da inteligência artificial na prática desse crime não possui tipificação especifica, o que mostra a necessidade de atualização do referido código frente à nova realidade social.

Outrossim, buscou-se na doutrina da área penal explicação dos autores Ermeson Wendt e Igor Vinícius Nogueira Jorge, através do livro “Crimes Cibernéticos”, para explicitar o conceito de fraude. Assim como utilizou-se do conceito de I.A trazido

por Alan Turing, para melhor entendimento acerca dessa ferramenta. Foram ainda abordadas análises de casos de delitos cometidos com o uso da inteligência artificial, apresentando o caso ocorrido com o influenciador Dário Santurione, além das explicações de Sayak Sasha Roy e Fabiano Felício Botton, acerca dos casos com ChatGTP e bots do telegram. Ao final, buscou-se abordar a legislação, trazendo um

projeto de lei recente elaborado pelo senador Acácio Favacho, com o intuito de comprovar a atualidade e importância do projeto.

**9 CONCLUSÕES**

Diante dos fatores expostos, conclui-se que a inteligência artificial evidentemente é um recurso que pode contribuir para a prática de fraudes no meio virtual, sendo utilizada tanto na criação de novos golpes como também no aprimoramento das fraudes já existentes, como demostraram os aspectos analisados.

Apesar dessa realidade criminosa ser algo novo em nosso meio, o fácil acesso à inteligência artificial tornou a ferramenta bastante atrativa para os criminosos. Isso porque o poder de convencimento que esse recurso passa à vítima durante o golpe aliado à dificuldade de identificar as infrações no ciberespaço faz com que as fraudes sejam bem sucedidos.

Logo, é imprescindível que haja regulamentação acerca do uso da inteligência artificial, além de punição mais severa e efetiva para práticas criminosas que se utilizem dessa tecnologia, buscando barrar o provável crescimento das fraudes através desse novo recurso. Para tanto, é necessário que haja a devida qualificação informática e tecnológica da área policial, além da disponibilização de recursos materiais que viabilizem uma investigação mais eficaz acerca de crimes no ciberespaço.

**REFERÊNCIAS**

ALVES, Alan; DOS SANTOS, LAIZA PADILHA. Os Crimes Virtuais no Brasil. **JUSFARESC-Revista Jurídica Santa Cruz,** v. 9, n. 9, 2016. Disponível em: https://unisantacruz.edu.br/revistasold/index.php/JUSFARESC/article/view/1978 . Acesso em 15 Ago. 2023.

BOTTON, Fabiana Felicio. **"Roubamos sem dar um tiro"**: uma etnografia de grupos de fraudadores no espaço virtual. 2022. Dissertação (Mestrado em Antropologia Social) - Faculdade de Filosofia, Letras e Ciências Humanas, University of São Paulo, São Paulo, 2022. doi:10.11606/D.8.2022.tde-10062022-105118. p. 38-39. Acesso em: 02 de set. 2023.

BRASIL. **Código Penal.** Decreto-lei nº 2848, de 7 dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil\_03/decreto-lei/Del2848compilado.htm. Acesso em: 20 Ago. 2023. COMPROVA, D. P. Saiba o que é deepfake, técnica de inteligência artificial que foi apropriada para produzir desinformação. Disponível em:. Acesso em: 04 set. 2023.

COMPROVA, D. P. **Saiba o que é deepfake, técnica de inteligência artificial que foi apropriada para produzir desinformação**. Disponível em:<https://www.cnnbrasil.com.br/noticias/saiba-o-que-e-deepfake-tecnica-de-inteligencia-artificial-que-foi-apropriada-para-produzir-desinformacao/>. Acesso em: 04 set. 2023.

Favacho, acácio. **Projeto de lei n. 3800/2023**. Altera o art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para aumentar a pena do crime de fraude eletrônica quando a conduta for praticada com a utilização de inteligência artificial. Brasília: Câmara dos Deputados, 08 de ago. 2023. Disponívelmem: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao ?idProposicao=2376427&ref=nucleo.jor.br. Acesso em: 20 de ago. 2023.

JIMENEZ, cinta castillo. Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información. Huelva: Facultad de Derecho. Universidad de Huevas. **Derecho y Conocimiento**. v. 1. p. 35-48, 2001. Disponível em: https://rabida.uhu.es/dspace/bitstream/handle/10272/1565/b1205654.pdf. Acesso em 15 de set. 2023.

MARTINS, F. **Influenciador alerta sobre novo golpe do pix com IA que recria voz de qualquer pessoa**. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/influenciador-alerta-sobre-novo-golpe-do-pix-com-ia-que-recria-voz-de-qualquer-pessoa/>. Acesso em: 21 ago. 2023.

ROY, Sayak Saha; NARAGAM, Krishna Vamsi; NILIZADEH, Shirin. Generating Phishing Attacks using ChatGPT. **arXiv preprint arXiv:2305.05133**, 2023. Disponível em: https://arxiv.org/abs/2305.05133 . Acesso em: 05 Set. 2023.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos**. Ameaças e Procedimentos de Investigação. Rio de Janeiro. Brasport, 2012.