DOI 10.47402/ed.ep.c202321007201

CAPÍTULO 7

CASO DE CYBER FRAUD POR TELEFONE NO BRASIL E A INTELIGÊNCIA ARTIFICIAL: VÍTIMAS IDOSAS, SPOOFING ATÉ A MANIPULAÇÃO POR ENGENHARIA SOCIAL

Eduardo Martins Morgado
Docente e pesquisador do Programa de Pós-Graduação em Mídia e Tecnologia (Doutorado) na Universidade Estadual Paulista "Júlio de Mesquita Filho", Faculdade de Arquitetura, Artes, Comunicação e Design - Câmpus de Bauru.
Carla Gonçalves Távora
Discente do Programa de Pós-Graduação em Mídia e Tecnologia (Doutorado) na Universidade Estadual Paulista "Júlio de Mesquita Filho", Faculdade de Arquitetura, Artes, Comunicação e Design - Câmpus de Bauru.
Ana Claudia Pires Ferreira de Lima
Discente do Programa de Pós-Graduação em Mídia e Tecnologia (Doutorado) na Universidade Estadual Paulista "Júlio de Mesquita Filho", Faculdade de Arquitetura, Artes, Comunicação e Design - Câmpus de Bauru.
João Pedro Albino
Docente e pesquisador do Programa de Pós-Graduação em Mídia e Tecnologia (Doutorado) na Universidade Estadual Paulista "Júlio de Mesquita Filho", Faculdade de Arquitetura, Artes, Comunicação e Design - Câmpus de Bauru.
Ivany Bucchianico
Especialista pela Escola de Enfermagem de Ribeirão Preto (USP/SP). Bacharel em Enfermagem pela Universidade de São Paulo (USP), Ribeirão Preto/SP.

RESUMO
O objetivo é abrir discussão sobre medidas que possam ser tomadas para proteger as vítimas através da Inteligência Artificial. A metodologia é a descrição detalhada de um golpe digital de *spoofing* e manipulação com vítimas idosas, além da identificação da Inteligência Artificial para proteger as vítimas. O relato de caso retrata o golpe por meio do *spoofing,* programas que alteram a identificação do chamador em uma comunicação, junto da Engenharia Social para enganar a vítima para a realização de operações no aplicativo do banco, assim, incentivando a realização de transferências para a conta do golpista. A vítima acabou seguindo essas orientações e realizou agendamentos de envio de dinheiro para a golpista, porém, acabou suspeitando da situação, decidiu interromper aquela comunicação e procurar a agência do banco para o esclarecimento, assim, conseguindo cancelar os agendamentos e estornar os valores da transferência. Diante disso, a Inteligência Artificial pelo *Machine Learning* é uma forma de tratamento para essas situações, onde realiza o monitoramento e configuração para detectar ações irregulares dentro da conta bancaria e prevenir transações suspeitas, porém, sua aplicação está em fase de desenvolvimento e não há previsão de incorporação entre as instituições bancarias, no entanto, tem potencial em aprender sozinhos, estabelecer padrões, reconhecer mudanças dentro desses padrões e reportar ao um profissional para que realize o contato com os usuários. O *Machine Learning* proporciona monitoramento das contas por 24 horas, oportunizar mais vagas de empregos para atendimento ao público ora e dentro do expediente conforme o reconhecimento de um padrão desconhecido.
Palavras-chave: tecnologia; sociedade; inteligência artificial; fraude.

1 INTRODUÇÃO

O número de fraudes e golpes digitais associados a smartphones está aumentando vertiginosamente ao longo dos últimos anos. De acordo com o Indicador de Tentativas de

Fraude da Serasa Experian, em 2022, a **população brasileira sofreu uma tentativa de golpe a cada 8 segundos.** Somente no mês de junho de 2022, foram 322.219 tentativas de fraude em todo o território Brasileiro.

De acordo com a Federação Brasileira dos Bancos (Febraban), desde o início da Pandemia Covid 19, em 2019, houve alta de 165% em golpes baseados em smartphones. São muitos os tipos de golpes, como a extorsão, roubo de identidade, violação de dados pessoais, não pagamento ou não entrega

Segundo a Fintech (2021), no último ano as fraudes digitais aumentaram 33% no último ano. Não é um fenômeno Brasileiro, o mesmo está acontecendo em outros países, como o Reino Unido, onde a população é supostamente mais esclarecida e educada, mas onde o aumento foi de 25% no último ano (ONS.gov.uk, 2022).

As fraudes predominam junto aos usuários de smartphones, dado que eles foram adotados por quase toda a população. No Brasil, segundo censo IBGE de 2021, cerca de 84,4% dos brasileiros possuíam celular de uso pessoal; 90% deles com acesso à Internet e 79% desses brasileiros utilizavam algum tipo de “serviço de bancos digitais” (FORBES, 2022).

O objetivo é discutir sobre medidas que possam ser tomadas para proteger as vítimas através da Inteligência Artificial, que infelizmente, no Brasil, é composta por 30% de idosos (mais velhos que 60 anos).

A metodologia é o relato de caso de um golpe sob os pontos de vista da vítima com análise técnica do golpe, essa fraude ou golpe envolveu um grande Banco estatal Brasileiro, que da mesma forma que todos os envolvidos, não terá seu nome revelado, embora suas ações e comportamentos sejam analisados. E também realizar um levantamento bibliográfico sobre a aplicação da Inteligência Artificial para proteger as vítimas.

2 RELATO DE CASO: NARRATIVA DA VÍTIMA

Tenho 64 anos e sou cliente do Banco há mais de 15 anos e fui vítima de um golpe pelo telefone celular, do tipo que é chamado de "golpe de hacker”. Eu tenho um iPhone 11. Em uma Sexta-Feira, no final da manhã, o celular tocou mostrando na tela “Banco” – este é o nome da agência onde tenho minha conta já anos e estava cadastrado entre meus contatos há anos.

Para mostrar “Banco”, somente dois números que estariam ligados: o número XXXX XXXX, um celular corporativo da Agência de meu “Banco”, ou YYYY YYYY da mesma agência. Eram esses os números cadastrados em meus contatos há anos. Confiante e certa de

que falava com a minha Gerente, atendi falando “Oi Gerente!” e “ela” (já uma golpista) me cumprimentou alegremente, mas abriu a conversa me assustando, ao dizer que “possivelmente minha conta havia sido hackeada”.

Perguntou se eu havia feito algumas transferências naquele dia. Falei que não, mas a golpista “disse que sim”, e informou que “foram feitas para outro Banco”. Pediu para eu anotar um número de protocolo e disse que estava “rodando o sistema” para verificar os valores envolvidos nas transferências. Depois de segundos, a golpista pediu para eu anotar as “transferências” de R$4253,00; R$4050,00; R$4500,00 e R$4598,00; totalizando R$17.401,00.

Com voz calma, a golpista disse novamente que “as transferências foram feitas para o ‘outro Banco’”, mas que eu poderia ficar tranquila porque “ela já estava em contato simultâneo com a Gerente do Setor de Fraudes de “outro Banco’”, pediu para que eu anotasse o nome dessa “Gerente doutro Banco”. Quando eu perguntei como essas transações foram possíveis, já que ninguém tem minhas senhas e não as tenho anotado em agenda, a golpista respondeu que “era assim mesmo, eles invadem a conta e obtém facilmente as senhas”. E acrescentou que “já estava bloqueando minha conta”.

Apavorada, mas ainda confiante que estava conversando com a “Gerente de meu Banco”, perguntei se haviam entrado na conta do meu pai, da qual sou segunda titular. A golpista pediu alguns segundos para verificar e voltou dizendo que “sim, e que havia transferidos por volta de R$21.000,00 da conta dele”.

Perguntou, então, se eu havia feito empréstimos ao que respondi que não. A golpista então me orientou a entrar no App do Celular e contratar um empréstimo, porque esta seria a única forma dela verificar se eles (os supostos invasores) haviam contratado. Falei que não faria isso, já que não tinha sentido clicar em contratar empréstimo para fazer essa verificação. Vendo que não havia conseguido-me fazer contratar um empréstimo, a golpista rapidamente disse que “não seria preciso, pois eles (os invasores) haviam solicitado empréstimo, mas que não foi aprovado e que era para eu ficar tranquila”.

Mesmo apavorada, nesse meio tempo, verifiquei os extratos do meu e de meu pai, e visualizei que neles não apareciam qualquer saída ou transferência de valores. Comentei isso com a golpista, mas ela informou que “os golpistas congelam a tela de extrato por 48 horas para vítima não ter acesso ao saldo”. Começando a achar tudo muito estranho, eu questionei: “se

você havia bloqueado as contas, como foi que eu tive acesso ao App e ao extrato?". A golpista respondeu que havia desbloqueado para eu ter acesso, mas que estava bloqueando novamente.

A golpista então disse que me orientaria nos procedimentos para eu habilitar minhas transferências via App de Celular para que eu pudesse "receber os ressarcimentos que a Gerente do 'outro Banco' realizaria". Pensando nos ressarcimentos, fiz vários procedimentos na tela da App, clicando em pagar / receber, mas, ao mesmo tempo, me perguntava se eu não enviaria valores ao invés de me preparar para receber. A golpista disse que "estava tudo certo, que ela estava acompanhando o que eu fazia e garantia que eu estava mesmo habilitando o App para receber". Apavorada e nervosa, e sendo pressionada pela orientação de fazer tudo com urgência, mas ainda confiando que falava com a 'Gerente de meu Banco' fiz os procedimentos.

Nesse momento, a ligação ficaram muito ruim e eu pedi para ela me ligar no meu telefone fixo, o ZZZZ ZZZZ. A golpista relutou muito, mas enfim concordou, porém orientou para "que eu não saísse da tela do iPhone para não perder as transações". Ligou no meu telefone fixo, cujo identificador de chamada mostrou novamente o número XXXX XXXX.

Como há limites diários para transferências, ela insistiu que eu habilitasse outro tipo de transferência para eu poder receber. O que eu estava fazendo, na verdade, eram transferência e não percebi. Como há limites diários para transferências, em pouco tempo não podia fazer mais. Então ela orientou "que eu fizesse as habilitações, que eram na verdade, agendamentos de transferências para sábado e domingo".

Apavorada, nervosa e totalmente insegura com essas transações invertidas (saindo e não chegando), mesmo certa de que havia falado com a 'minha Gerente de Banco', interrompi as ligações e fui pessoalmente na Agência do Banco aqui de minha cidade. Fui prontamente atendida e informada que havia sido vítima de um golpe. As gerentes cancelaram os agendamentos e estornaram as transferências que foram possíveis. Porém, as transferências que foram feitas e sacadas na Agência Receptora não puderam ser recuperadas. As quadrilhas mantêm pessoas próximas às agências, para sacarem rapidamente o que foi transferido.

3 ANÁLISE TÉCNICA DO GOLPE

Do ponto de vista da Segurança Digital, a vítima foi inicialmente abordada por uma técnica chamada de "**spoofing**" e na sequência por uma estratégia chamada de "**Engenharia Social**".

> • **Spoofing**, em inglês "enganar ou falsificar", é o uso de programas que alteram a identificação do chamador em uma comunicação. Existem muitos tipos de "spoofing":

de DNS (Domain Name System ou nome de um site Web); de e-mail e, como foi nesse caso, de telefone.
O "spoofing" é uma estratégia de massa, onde um computador faz milhares de ligações – nesse caso, apenas uns poucos reagem positivamente à ligação – exatamente aqueles que tem o número cadastrado em seus contatos. Quando isso acontece, os golpistas passam para a fase seguinte.

- **Engenharia Social**, é uma estratégia complexa de manipulação de pessoas, onde uma quadrilha engana uma pessoa, explorando o seu emocional e esperando erros humanos que irão acontecer, para obter informações privadas, acessos ou objetos de valor. Sua aplicação segue uma metodologia onde uma quadrilha treinada, engana e manipula as vítimas, buscando obter informações ou induzir ações que as prejudiquem

Essa estratégia pode ser aplicada online (p.ex. Chats); por sistemas de troca de mensagens (p.ex. WhatsApp); por e-mail e, como foi nesse caso, por telefone.
Também é uma estratégia de massa – milhares são abordados.

Como a vítima foi atacada por "***spoofing***" seguido por "**Engenharia Social**", não faz sentido discutir se ela colaborou ou não colaborou com os fraudadores, pois a **Engenharia Social** busca exatamente isso – **conseguir colaboração**. A única forma de ajudar as vítimas a se defender é a informação, advertência ou aconselhamento prévio sobre os golpes que estão sendo aplicados no momento – eles mudam sempre. Informar é a obrigação dos Bancos.

Antes de tudo, precisamos destacar que todos esses golpes são aplicados por grupos de golpistas (quadrilhas) e são estratégias de massa – onde um computador faz muitas ligações para muitas pessoas, incansavelmente, dado que é uma máquina, redirecionando ou criando bancos de dados para outras ações de todos aqueles que reagiram à primeira rodada de ataques. Além do "*spoofing*", existem outras variações técnicas de ataques, como o "*fishing*", "*vishing*", "*smishing*" e "*pharming*", resumidamente descritos abaixo:

- ***Phishing***: ataque, normalmente por e-mail, onde se busca a obtenção de informações pessoais e sigilosas, geralmente seguidas por ataques via engenharia social.
- ***Vishing***: Semelhante ao phishing (Voice Phishing). Forma mais comum de ataque por chamadas de voz.
- ***Smishing***: Semelhante ao phishing (SMS Phishing), mas normalmente faz uso de mensagens de texto, tipo SMS enviadas para o celular. Geralmente acompanhadas de um link ou formulário.
- ***Pharming***: Parecido com o phishing, ele explora o tráfego a um site falso e previamente preparado, roubando informações confidenciais.

A **Engenharia Social** é a estratégia que sempre é utilizada depois de detectados os alvos, ou potenciais vítimas. Para entender melhor essa estratégia vamos descrever sua metodologia, que é exaustivamente treinada pelas quadrilhas de golpistas:

1. **Preparação**: quando a quadrilha reúne informações básicas sobre um alvo ou grupo de alvos em situação semelhante.
2. **Infiltração:** conexão e estabelecimento de relacionamento ou comunicação com a vítima. Começa pela construção de confiança.
3. **Desestabilização**: fornecimento de informações de impacto, avisos ou alertas que apavorem ou deixem a vítima nervosa e, portanto, sem capacidade de raciocínio claro.

4. **Pressão ou exploração:** por indução de pressa, urgência ou medo maior, a quadrilha convence a vítima a agir depressa, fazendo coisas ou passando informações, sem pensar.
5. **Dispersão:** sumiço, desconexão após objetivos serem atingidos.

A Engenharia Social é muito eficaz. As vítimas normalmente entregam tudo, aparentemente sem serem coagidas ou ameaçadas. Infelizmente, existe grande preconceito, que tende a considerar que o "usuário colaborou" e não que o "usuário foi vítima". Esse preconceito é, obviamente, maior entre aqueles que ainda não foram vítimas ou que não estudaram o problema (IC3, 2023).

Os smartphones são o alvo preferencial dos golpes, porque 88% dos Brasileiros tem celular com acesso à Internet, dos quais 75% faz uso de "recursos de bancos digitais". Sabemos que 30% das vítimas de fraudes digitais é composta por idosos com mais de 60 anos, que em sua maioria são vítimas de "spoofing" (FORBES, 2022; FINTECH, 2021).

Nesse ponto, dúvidas importantes surgem e vamos tentar respondê-las:

- **Como os golpistas sabiam que a vítima tinha conta no Banco?**

Eles não sabiam! Eles apenas sabiam que o número "XXXX XXXX" havia sido utilizado para ligar para os clientes no passado, mas que não era mais usado assim, embora ainda existisse para receber ligações.

> *Esse pequeno detalhe demonstra uma grande falha do Banco – se o número havia mudado de função, esse número deveria ter sido trocado por um novo número.*

Os golpistas fizeram "*spoofing*" do "XXXX XXXX" em milhares ou milhões de pessoas. *São máquinas que ligam e elas não se cansam. Quem reagir reconhecendo a ligação como sendo do Banco é transferido para o grupo da Engenharia.*

- **Por que a vítima tinha esse número XXXX XXXX nos contatos com o nome Banco já que o Banco afirma que esse número é das Agências, mas não é usado para ligações externas?**

Atualmente, esse número pode não ligar para fora da Agência, mas no passado ele ligava. E ele precisa sim, estar em meus contatos, porque é um dos números que podemos usar para falar com o Banco.

> *Essa é outra falha do Banco – o autor, que também é correntista do Banco, tenho esse número nos seus contatos do celular e pode ligar para ele, mas o que devo fazer se ele ligar para mim?*
> *No passado esse número ligou para a vítima e para mim, e nós o salvamos anos atrás. Não sabemos quando esse número parou de fazer ligações externas.*

Ao analisar as estratégias e ações do Banco em relação a esse golpe, há como evidenciar tecnicamente que foram negligentes ao gerenciar essa questão. Eles não informaram as pessoas que estavam correndo alto risco.

O Banco sabia de 88% dos Brasileiros tem celular com acesso à Internet, dos quais 75% faz uso de "recursos de bancos digitais". O Banco também sabia que 30% das vítimas de fraudes digitais é de idosos (> 60 anos), que em sua maioria são vítimas de "spoofing".

> *Mesmo sabendo disso tudo, pouco ou nada fez quando alterou o uso de seu número XXXX XXXX.*

O **Banco conhece esse golpe**, que ele chama de "falsa central de atendimento", há muito tempo. E o Banco o tem detalhadamente descrito em uma de suas páginas Web.

Mas para achar essa descrição eu tive de fazer uma busca via Google usando como palavras de busca "*spoofing*", "*phishing*" e "*Banco*", Encontrei as páginas e navegando por lá encontrei esse golpe descrito.

A busca que eu fiz foi a de um especialista em informática – um cliente comum dificilmente a faria. Dentro dessas páginas, me cadastrei para "Receber Newsletter" – agora recebo notícias regularmente.

- **O Banco também descreve esse golpe em um folheto ou *folder* muito bem elaborado.**

Paradoxalmente, esse folheto está disponível em mesas da Agência. Ou seja, quem usa o aplicativo do Banco no Celular, aqueles 75% dos donos de celular que usam algum tipo de "banco digital" vai raramente à Agência e, portanto, não vai ver esse folheto.

> *Temos aqui outra falha do banco. Esse folheto não foi enviado por correio para ninguém, nem para os clientes idosos.*

- **Por que os idosos predominam entre as vítimas?**

O Brasil, segundo o Censo 2017 (IBGE), conta com 30,2 milhões de pessoas maiores de 60 anos, sendo 56% mulheres e 44% homens. Até 2022, o número de idosos aumentou e o número de mulheres é superior ao de homens. E como já vimos, os idosos são 30% das vítimas de golpes digitais, notadamente de "spoofing" que foi a estratégia usada no golpe da "falsa central de atendimento" (FINTECH, 2021; KASPERSKY, 2022).

Verifica-se uma maior participação dos idosos no universo virtual para lazer e comunicação com seus familiares. Consequentemente, há um aumento do número deles como vítimas de crimes virtuais. A população idosa é uma classe social extremamente vulnerável a

tais crimes. Dentre as inúmeras causas dessa situação, citamos a redução das capacidades cognitivas e fisiológicas derivadas do aumento da idade; o desconhecimento e ingenuidade no uso adequado das tecnologias e dos riscos associados.

Idosos em sua maioria são aposentados, com grupos restritos de relacionamento social já que estão fora da vida profissional. Tem mais dificuldade de acesso às tecnologias que se atualizam a cada segundo. Desse modo tem muito menos chance de serem alertados sobre golpes.

Criminosos utilizam a estratégia da **Engenharia Social**, que afetam o psicológico dos idosos, afetando seu processo de tomadas de decisões pela emoção e pela sobrecarga de informações, bem como a ingenuidade no crer em reciprocidade de favores, em ofertas e na falsa construção de relacionamentos. Entre os idosos, os golpes mais comuns são:

- **Estelionato**: quadrilha engana a vítima para obtenção de vantagem, como por exemplo, venda de coisas alheias como sendo próprias;
- **Ligações mal-intencionadas**: golpistas passam-se por familiares, empresas e contas no geral, praticando a solicitação de dados e créditos;
- **Falsos empréstimos**: como depósitos antecipados para liberação de crédito ou empréstimos falsos para roubos de dados, onde os golpistas podem obter dinheiro e crédito em nome da vítima, assim como outros crimes de falsa identidade.

Um caso bem particular - o WhatsApp é um campeão no envolvimento com fraudes (NOIA, 2023)

Pesquisa feita com 14 mil entrevistados revela que a maior parte das pessoas que caíram em golpes foi enganada por meio de mensagens recebidas pelo WhatsApp, sendo que dos 65,1%, sofreram os seguintes tipos de golpes:

- Tiveram conta do aplicativo clonada (22,1%);
- Clicaram em links fraudulentos que receberam por mensagem de texto (20,7%
- Pagaram boletos falsos com o código de barras adulterado (20,8%).
- 49,5% transferiram dinheiro aos golpistas.

Infelizmente, 76,4% dos consumidores que foram vítimas de golpes não conseguiram reaver o prejuízo, e somente 24,7% registraram boletins de ocorrência. Cerca 30,1% passaram dados pessoais e bancários, 20,4% tiveram os CPFs e os nomes usados em compras de terceiros não autorizadas, e 49,5% fizeram transferências financeiras para os golpistas.

Segundo outra fonte, (SIQUEIRA, 2022), os golpes mais comuns com o uso do WhatsApp são descritos abaixo. Vemos também que o WhatsApp implementou medidas de segurança adicional, mas que não tem sido muito eficaz quando os golpistas usam também a **Engenharia Social**.

• **Clonagem**: Consiste na "cópia" do WhatsApp da vítima para o celular do golpista. Para cadastrar o aplicativo no seu celular, o golpista vai precisar do número do celular da vítima e de um código que é enviado por SMS pela WhatsApp para o número cadastrado na conta. Ou seja, esse código não é enviado para o golpista, e sim para a vítima. Os golpistas utilizam diferentes técnicas para obter este código, como pressão, promessas, ameaças, mas no final, a vítima colabora.
• **Links falsos**: Links maliciosos com boas propagandas para roubar dados pessoais. Os mais compartilhados no Brasil são: saque do FGTS, grandes promoções e vagas de empregos.
• **Contas falsas**: Utilização de nome e foto de perfil de outras pessoas para pedir dinheiro;
• **Fake News**: Técnica utilizada para fraudar dados de usuários ao confundir pessoas com notícias falsas e fora do contexto;
• **Spywares**: aplicativos espiões que permitem que golpistas monitorem atividades do celular da vítima remotamente. Esses aplicativos são instalados após a vítima clicar num link e dar diversas confirmações exigidas pela segurança do celular.

3.1 Informações relevantes, importantes e o absurdo dos absurdos

A instalação de um *spyware* é o máximo que um golpista consegue fazer, à distância, sem estar de posse do aparelho. A técnica é sempre a mesma, o usuário é incitado a clicar em um link, mas, como vimos, a instalação do *spyware* só vai acontecer depois de vários pedidos de confirmação pelo sistema operacional do celular.

Não existe a possibilidade de um golpista "capturar" ou "clonar" ou "copiar" o celular de outra pessoa. Isso é uma lenda urbana. Para conseguir algo parecido o celular tem que ser manuseado pelo golpista – ou seja passar um bom tempo na mão de um terceiro golpista. É uma operação complexa, que hoje é impossível no iOS (Apple) e muito difícil no Android.

O absurdo dos absurdos: Existem programas que se dizem *spyware* e seu marketing é prometer que instalando esse programa no celular de uma vítima, a pessoa que o instalou vai ter acesso a suas ligações e ações. Esse marketing visa parceiros desconfiados de seus parceiros e pais desconfiados de seus filhos. A venda desses programas é também um golpe – um golpe numa pessoa que sonha em dar um golpe em outra, invadindo sua privacidade. Alguns chegam ao absurdo de prometer que não é preciso estar com o celular na mão para instalar esse *spyware*. Outros chegam a prometer que "basta saber o número do telefone".

4 INTELIGÊNCIA ARTIFICIAL PARA PROTEGER AS VÍTIMAS

A Inteligência Artificial apresenta diferentes metodologias de *Machine Learning,* o *Machine Learning* apresenta evolução na área da educação, negócios, e principalmente para a segurança, uma metodologia de análise de dados para o desenvolvimento de modelos analíticos (JONES-ORTIZ e GUZMÁN–SERAQUIVE, 2022).

O *Machine Learning* atua entre as áreas de Ciência da Computação e a Estatística, com a evolução tecnológica e o avanço de aplicações financeiras por meio digital, a segurança é o principal setor que requer atenção. Assim, o *Machine Learning* realiza a coleta de dados, organização, resumo, analise, interpretação e tomadas de decisões, um sistema inteligente capaz de atuar em diferentes setores, principalmente para a segurança (MEDRI, 2011; JORDAN e MITCHELL, 2015).

As técnicas de *Machine Learning* estão sendo aplicadas para a detecção e previsão de fraudes através de algoritmos de classificação na detecção e redes neurais artificiais, onde algoritmos estatísticos, *Machine Learning,* regressão logística e redes neurais artificiais é capaz de detectar fraudes financeiras (LIMA, 2022).

Os algoritmos de *Machine Learning* permitem que um computador aprenda sozinho, há três categorias de algoritmos, como: Algoritmos supervisionados, Algoritmos semi-supervisionados e Algoritmos sem supervisão. Caldas (2019, p.18) explica que:

> Algoritmos supervisionados: aqui entram os modelos que são treinados com dados classificados, isto é, dados que possuem uma etiqueta a indicar a classe a que pertencem (por exemplo, fraude ou não fraude podem ser as classes de um modelo);
> Algoritmos semi-supervisionados: estes modelos possuem apenas uma etiqueta, ou seja, geralmente apenas são classificados os dados normais;
> Algoritmos sem supervisão: um modelo é treinado sem qualquer classificação prévia dos seus dados, desta forma, não existe a etiqueta (por exemplo, fraude ou não fraude) que ajude o modelo a classificar de maneira mais assertiva os dados.

Segundo Castro e Alonso (2022) para a detecção de fraudes de diversos tipos com soluções de aprendizado automático para a detecção de padrões de comportamento pode ser utilizado *Machine Learning* e mineração de dados com técnicas de aprendizado supervisionado para a extracção de conhecimento, detecção de padrões, automação de processos de trabalho e abordando diferentes fontes de dados. O modelo supervisionado é ideal para prever os valores de saída de determinado ambiente (HASTIE, 2009).

O uso de *Machine Learning* está em fase de teste para a área da segurança, Muller (2021) explica que essa técnica permite reconhecer padrões e aprender, assim, garantir que fraudadores sejam identificados, detectar variáveis de maior impacto e indicar com uma maior probabilidade as transações não legítimas. Essa aprendizagem é através de registros de fraudes já ocorridas, assim, detectando futuros padrões de comportamento dentro de uma conta e evitar que futuros usuários repitam erros de outros golpes.

O *Machine Learning* já está sendo aplicado para a prever ocorrência de fraudes em transações europeias de cartão de crédito, por isso, há a possibilidade de sua aplicação para a área de transações financeiras em contas bancarias (VIANA, 2021).

5 CONSIDERAÇÕES FINAIS

Atualmente, as fraudes são situações recorrentes e caracterizado como uma situação normal para os brasileiros, por isso, há a necessidade de adotar medidas que contribua para a proteção da vítima, o *Machine Learning* é uma forma de tratamento para essas situações, onde realiza o monitoramento e configuração para detectar ações irregulares dentro da conta bancaria e prevenir transações suspeitas.

O *Machine Learning* é uma alternativa de cuidado para a sociedade, porém, está em fase de desenvolvimento e não há previsão de incorporação entre as instituições bancarias, por enquanto, essa alternativa continua sendo um estudo e uma proposta de melhorias necessárias para a proteção das pessoas contra fraudes e golpes.

O *Machine Learning* tem potencial por conseguir aprender sozinhos os padrões de comportamento dos usuários dentro de uma instituição bancaria, processando todos os dados dos usuários para estabelecer padrões diferentes para cada padrão, assim, quando acontecer mudanças dentro desses padrões poderá reportar ao gerente/chefe da instituição, possibilitando que esse profissional entre em contato com os usuários para reconhecer a situação.

A aplicação do *Machine Learning* para o monitoramento das contas, proporciona aos usuários uma segurança por 24 horas, além de oportunizar mais vagas de empregos para a população no aspecto de secretário, gerente ou atendente, onde realizariam o contato com os usuários fora e dentro do expediente em casos de reconhecimento de um padrão desconhecido na conta bancaria.

REFERÊNCIAS

ALLOWME. **Device Fraud Scan**. 2022. Disponível em: <https://conteudo.allowme.cloud/e-book-device-fraud-scan-2022>. Acesso em: 17 fev. 2023.

ALLEASY. **O que é Phishing, Smishing e Vishing? Conheça as diferenças!** 2018. Acesso em 16 fev. 2023.

CALDAS, Luísa Lopes. **Deteção de fraude em telecomunicações através de machine learning**. Dissertação (Mestrado em Matemática e Computação) - Universidade do Minho, 2019.

CASTRO, Claudia Beatríz Martínez. ALONSO, Jose Alberto Vilalta. Métodos y técnicas de Machine Learning e Inteligencia Artificial para el enfrentamiento al fraude en las Telecomunicaciones: Técnicas de minería de datos aplicadas a las gestión del fraude. **Revista Cubana de Transformación Digital**, v. 3, n. 4, p. e182-e182, 2022.

CORREIO DO POVO. Disponível em: <https://www.correiodopovo.com.br/jornalcomtecnologia/mais-de-155-milhões-de-brasileiros-possuem-celular-para-uso-pessoal-aponta-ibge-1.891007>. Acessado em 16 fev. 2023.

DATAVISOR. **DIGITAL FRAUDTRENDS REPORT 2021.** 2021. Disponível em: <https://www.datavisor.com/wp-content/uploads/2021/11/DataVisor-Digital-Fraud-Trends-Report-2021-2.pdf>. Acesso em: 16 fev. 2023.

FINTECH. Disponível em: <https://fintechs.com.br/relatorio-o-estudo-de-fraude-de-identidade-de-2021/>. Acessado em 16 fev. 2023.

FORBES. Disponível em: <https://forbes.com.br/forbes-money/2022/10/brasileiros-se-dividem-entre-bancos-digitais-e-tradicionais-diz-pesquisa/#:~:text=Uma%20pesquisa%20do%20C6%20Bank,em%20instituições%20sem%20agências%20físicas>. Acessado em 16 fev. 2023.

HASTIE, T. TIBSHIRANI, R. FRIEDMAN, J. **The Elements of Statistical Learning:** Data Mining, Inference, and Prediction. 2. Ed. New York: Springer, 745 p., 2009.

HUESO, Lorenzo Cotino. Riesgos e impactos del Big Data, la inteligencia artificial y la robótica: enfoques, modelos y principios de la respuesta del derecho. **Revista general de Derecho administrativo**, n. 50, p. 1-37, 2019.

IC3. **Internet Crime Report.** 2021. Disponível em: <https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf>. Acesso em: 20 fev. 2023.

JONES-ORTIZ, Carlos Vicente. GUZMÁN–SERAQUIVE, Jomar Elizabeth. Análisis de las técnicas de machine learning aplicadas en la detección de fraudes bancarios. **Revista Científica Ciencia y Tecnología**, v. 22, n. 33, 2022.

JORDAN, M. I. MITCHELL, T. M. Machine learning: trends, perspectives, and prospects. Science, [S.L.]. American Association for the Advancement of Science (AAAS). v. 349, n. 6245, p. 255-260, jul. 2015.

KASPERSKY. **Boletim de Segurança Kaspersky**. 2022. Disponível em: <https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2022_en_final.pdf>. Acesso em: 10 fev. 2023.

LIMA, Lemonier Barbosa de. **O uso de técnicas de Machine Learning para melhorar a prevenção à fraude**. Dissertação (Mestrado) – Universidade de Brasília, 2022.

MANZZI, Ana Carolina. **Conheça os principais golpes na Internet e saiba como proteger os seus dados.** NIC.br, 2022. Disponível em: https://www.nic.br/noticia/na-midia/conheca-os-principais-golpes-na-internet-e-saiba-como-proteger-os-seus-dados/. Acesso em: 15 fev. 2023.

MAYBANK. **Top 4 most viral online scams right now.** 2022. Disponível em: <https://www.maybank.com/en/blogs/2022/11/14-scam-tactics.page>. Acesso em: 13 fev. 2023.

MEDRI, W. **Análise exploratória de dados**. Universidade Estadual de Londrina. Centro de Ciências Exatas (CCE). Curso de Especialização em Estatística. Londrina, Paraná, 2011.

MULLER, Bruna Luise. **Como o Machine Learning funciona na detecção de fraudes.** Linkedin, 2021. Disponível em: <https://pt.linkedin.com/pulse/como-o-machine-learning-funciona-na-detec%C3%A7%C3%A3o-de-fraudes-m%C3%BCller> Acesso em: 22 março 2023.

NASSIF, Tamara. G**olpes digitais colocam cibersegurança à prova; veja como se proteger.** CNN Brasil, 2022. Disponível em: <https://www.cnnbrasil.com.br/business/golpes-digitais-colocam-ciberseguranca-a-prova-veja-como-se-proteger/>. Acesso em: 12 fev. 2023.

NOIA, Julia. **WhatsApp é campeão de fraudes na internet, mostra pesquisa. Saiba como se proteger.** 2023. Disponível em: <https://extra.globo.com/economia-e-financas/whatsapp-campeao-de-fraudes-na-internet-mostra-pesquisa-saiba-como-se-proteger-25415122.html>. Acesso em: 16 fev. 2023.

ONS.gov.uk. **Office for National Statistics.** Gov,UK Office for National Statistics for England and Wales, Consultado em <https://www.ons.gov.uk/>. Acesso em: 13 fev, 2023.

PANCINI, Laura. **58% dos brasileiros sofreram crimes cibernéticos, aponta estudo da Norton.** Exame, 2022. Disponível em: <https://exame.com/tecnologia/58-dos-brasileiros-sofreram-crimes-ciberneticos-aponta-estudo-da-norton/>. Acesso em: 13 fev. 2023.

RATIER, Rodrido. **Grupos bolsonaristas têm ataques de golpe do pix, notas falsas e "gatonet".** UOL. 2022. Disponível em: <https://www.uol.com.br/ecoa/colunas/rodrigo-ratier/2022/06/13/grupos-bolsonaristas-no-whatsapp-tem-golpe-do-pix-nota-falsa-e-gatonet.htm>. Acesso em: 13 fev. 2023.

SERASA EXPERIAN. **Brasileiros sofreram mais de 375 mil tentativas de fraude em janeiro, revela Serasa Experian.** 2022. Disponível em: <https://www.serasaexperian.com.br/sala-de-imprensa/analise-de-dados/brasileiros-sofreram-mais-de-375-mil-tentativas-de-fraude-em-janeiro-revela-serasa-experian/>. Acesso em: 11 fev. 2023.

SERASA EXPERIAN. **Pessoas entre 36 e 50 anos são os principais alvos de golpistas, aponta pesquisa da Serasa Experian.** 2022. Disponível em: <https://www.serasaexperian.com.br/sala-de-imprensa/analise-de-dados/pessoas-entre-36-e-50-anos-sao-os-principais-alvos-de-golpistas-aponta-pesquisa-da-serasa-experian/>. Acesso em: 11 fev. 2023.

SIQUEIRA, Filipe**. Conheça os crimes digitais mais comuns praticados no Brasil e saiba se proteger** R7, 2022. Disponível em: <https://noticias.r7.com/tecnologia-e-ciencia/conheca-os-crimes-digitais-mais-comuns-praticados-no-brasil-e-saiba-se-proteger-22042022#/foto/1>. Acesso em: 16 fev. 2022.

TRANSUNION. **Tentativas de fraude digital migram para novos segmentos globalmente.** 2022. Disponível em: <https://newsroom.transunion.com.br/tentativas-de-fraude-digital-migram-para-novos-segmentos-globalmente/>. Acesso em: 11 fev. 2023.

VIANA, Wesley Muller Oliveira**. Comparativo de alguns modelos de machine learning utilizando dados de domínio público e a linguagem python**. Trabalho de Graduação (Engenheiro Eletricista) - Universidade Estadual Paulista, 2021.

WOJAHN, A. S.; MICHAEL, C. da P.; VEIGA, D. J. S. da; LENZ, R.; SILVA, S. G. da; ROSSETTO, T. P.; SANTOS, M. L. dos. The social vulnerability of the elderly against scams in the digital scope. **Research, Society and Development,** [S. l.], v. 11, n. 11, p. e452111133652, 2022. DOI: 10.33448/rsd-v11i11.33652.