# CRESCENTES CASOS DE ESTELIONATO CIBERNÉTICO NO BRASIL A PARTIR DA EVOLUÇÃO DA INTELIGÊNCIA ARTIFICIAL

Ana Livia Andrade de Mattos[1]

Fernando Lemes[2]

Lucas Paulo Soares de Oliveira[3]

## RESUMO

Nos últimos anos, o Brasil tem visto um aumento nos casos de estelionato cibernético, impulsionado pela evolução da inteligência artificial (IA). Criminosos utilizam IA para aprimorar técnicas de phishing, criar deepfakes convincentes e automatizar ataques em larga escala, resultando em fraudes mais sofisticadas. Esses golpes causam grandes prejuízos financeiros e minam a confiança dos consumidores em transações online. Para mitigar esses riscos, é crucial investir em tecnologias de defesa avançadas, melhorar sistemas de autenticação e educar os usuários sobre segurança digital, além de aprimorar o arcabouço legislativo sobre o tema. O combate eficaz ao estelionato cibernético depende de uma ação conjunta entre o setor público e privado.

**Palavras-chave:** Estelionato cibernético, inteligência artificial, phishing, crimes virtuais.

## INTRODUÇÃO

Na contemporaneidade, o Brasil se encontra em uma encruzilhada digital. A revolução tecnológica, impulsionada pelo crescente acesso à internet e pela rápida evolução da inteligência artificial (IA), trouxe consigo inúmeras vantagens e oportunidades. No entanto, também abriu portas para novas formas de criminalidade cibernética, sendo o estelionato virtual uma das mais prevalentes e preocupantes.

O avanço exponencial da tecnologia digital e o aumento do acesso à internet no Brasil têm sido acompanhados por uma alarmante elevação nos casos de fraude cibernética. Este artigo se propõe a analisar, sob uma perspectiva multidisciplinar e aprofundada, a crescente incidência de fraudes cibernéticas no Brasil, correlacionando-a com os avanços na tecnologia de inteligência artificial.

Para compreender plenamente este fenômeno, é imperativo examinar o contexto brasileiro de acesso à internet e identificar os principais tipos de fraudes virtuais que afligem a sociedade. Em seguida, abordaremos especificamente as modalidades de estelionato

[1] Aluna no Curso de Direito da Faculdade Evangélica Raízes. Anápolis, Goiás, Brasil. E-mail: analivia.am@outlook.com

[2] Professor no Curso de Direito da Faculdade Evangélica Raízes. Anápolis, Goiás, Brasil. E-mail: fernando.lemes@faculdaderaizes.edu.br

[3] Aluno no Curso de Direito da Faculdade Evangélica Raízes. Anápolis, Goiás, Brasil. E-mail: dr.lucaspaulo@gmail.com

diversidade populacional, testemunhou uma expansão significativa no acesso à internet nas últimas duas décadas. Programas de inclusão digital e a popularização de dispositivos móveis permitiram que uma parcela considerável da população, antes excluída do mundo digital, passasse a usufruir das facilidades da conectividade. Este crescimento, embora positivo sob muitos aspectos, também criou um ambiente fértil para a atuação de cibercriminosos.

Além disso, os tipos de fraudes virtuais são diversos e vão desde *phishing*, (prática de enganar, pressionar ou manipular pessoas para que enviem informações ou recursos para as pessoas erradas) e roubo de identidade até golpes mais sofisticados, como fraudes financeiras e esquemas de pirâmide. O impacto econômico dessas atividades ilícitas é vasto, afetando não só indivíduos, mas também empresas e a economia como um todo. Socialmente, a desconfiança gerada por essas fraudes prejudica a adoção de novas tecnologias e serviços digitais, atrasando o progresso e a inovação.

Dentro do escopo das fraudes cibernéticas, o estelionato virtual destaca-se por sua capacidade de adaptação e inovação. Golpistas utilizam técnicas avançadas de engenharia social e aproveitam-se da falta de conhecimento técnico da população para enganar e desviar recursos. Analisar estas formas de estelionato é crucial para desenvolver estratégias eficazes de combate e prevenção.

Paralelamente, a inteligência artificial, com seu desenvolvimento acelerado, tem potencial para transformar profundamente a sociedade. No entanto, também traz desafios significativos, especialmente no campo da segurança digital. A evolução exponencial da IA permite a automação de processos complexos e a criação de sistemas altamente eficientes. Contudo, essas mesmas capacidades podem ser exploradas por criminosos para sofisticar ataques e criar fraudes mais difíceis de detectar. Existe uma correlação direta entre o avanço das tecnologias de IA e o aumento dos casos de estelionato virtual. Ferramentas de IA são usadas para criar *phishing* altamente personalizado, automatizar ataques em grande escala e explorar vulnerabilidades em sistemas de segurança. Este fenômeno é particularmente preocupante no contexto brasileiro, onde a rápida adoção dessas tecnologias muitas vezes não é acompanhada por medidas de segurança adequadas.

Os efeitos da fraude cibernética vão além das perdas econômicas imediatas. As vítimas enfrentam desafios emocionais e psicológicos significativos, os perpetradores sofrem as consequências legais e a sociedade, de modo geral, lida com a erosão da confiança no ambiente digital. As repercussões econômicas, sociais e jurídicas da fraude cibernética são profundas e exigem uma resposta coordenada e abrangente.

Diante da crescente ameaça de fraudes cibernéticas, torna-se essencial desenvolver e implementar estratégias robustas de prevenção e combate. Governos e instituições precisam formular políticas eficazes que não só punam os infratores, mas também previnam a ocorrência de fraudes. Políticas públicas bem delineadas são fundamentais para a criação de um ambiente digital mais seguro. Além disso, a alfabetização digital é uma ferramenta poderosa na prevenção de fraudes. Educar a população sobre os riscos e as melhores práticas de segurança pode reduzir significativamente a vulnerabilidade aos golpes. A legislação também precisa evoluir junto com a tecnologia para ser eficaz. A discussão sobre as atuais lacunas legais e a proposição de novas formas de regulamentação são essenciais para enfrentar os desafios da fraude cibernética de maneira mais eficiente.

Notavelmente, a análise da crescente incidência de estelionato cibernético no Brasil à luz dos avanços em inteligência artificial revela a necessidade urgente de abordagens integradas que envolvam políticas públicas, educação digital e regulamentação jurídica. Somente assim será possível mitigar os impactos dessa ameaça crescente e garantir a segurança no ambiente digital brasileiro.

## 1. FRAUDE CIBERNÉTICA NO BRASIL

### 1.1. A EXPANSÃO DO ACESSO À INTERNET NO BRASIL

No início da década de 1980, a comunidade acadêmica de São Paulo e do Rio de Janeiro tomou a iniciativa de trazer a internet para o Brasil. Mas o acesso a ela foi limitado a instituições acadêmicas e de pesquisa, e o país só começou a usar a Internet para fins comerciais em 1994.

Vários fatores, como a redução dos custos de equipamentos e serviços de Internet, contribuíram para o aumento da penetração da Internet no Brasil. O acesso à Internet costumava ser oneroso e reservado a uma elite. No entanto, como resultado das reduções de preços provocadas pelo aumento da concorrência entre os fornecedores de Internet e pelos avanços tecnológicos, um público maior pode agora aceder à Internet.

"A internet mudou a forma como nos comunicamos, trabalhamos, estudamos e nos divertimos. É uma ferramenta essencial para o desenvolvimento social e econômico do país." (IBGE, 2022, p. 22).

Um aumento na disponibilidade de serviços e conteúdo online. Uma variedade cada vez maior de conteúdos e serviços, como notícias, entretenimento, educação e comércio eletrônico, está agora disponível na Internet. Como resultado, o interesse do público pela Internet aumentou.

Por meio de diversas iniciativas, o governo brasileiro ajudou a aumentar o número de pessoas no país com acesso à internet. Dois desses programas se destacam: o Programa Internet para Todos, lançado em 2020, e o Programa Banda Larga para Todos, lançado em 2010.

O Brasil tem visto um aumento notável no acesso à Internet nos últimos anos. Apenas 13,6% dos domicílios brasileiros tinham acesso à internet em 2005, segundo dados obtidos do Instituto Brasileiro de Geografia e Estatística do IBGE (2022). Esse percentual aumentou para 90% em 2022.

Embora tenha havido avanços, ainda existem obstáculos a serem superados em termos de acessibilidade à internet no Brasil. Alguns desses desafios incluem:

- O acesso desigual à internet persiste no Brasil, com maior concentração em áreas urbanas, entre classes sociais mais altas e indivíduos com níveis de escolaridade mais elevados.

"A desigualdade no acesso à internet é um desafio que precisa ser enfrentado. É preciso garantir que todos os brasileiros tenham acesso a essa importante ferramenta." (CGI, 2022, p. 12).

- A qualidade do acesso continua sendo um desafio em certas partes do Brasil, dificultando o uso de serviços online que exigem velocidades de conexão mais rápidas.
- A infraestrutura insuficiente de telecomunicações em certas áreas do Brasil representa um desafio para a expansão do acesso à Internet. Nas próximas décadas, prevê-se que o Brasil experimentará uma maior expansão do acesso à Internet. Este crescimento será facilitado pela diminuição dos custos dos equipamentos e serviços de Internet, pela proliferação de conteúdos e serviços online e pelos avanços nas tecnologias de acesso à Internet.

"O desenvolvimento de novas tecnologias de acesso à internet, como a internet 5G, deve contribuir para a expansão do acesso à internet no Brasil." (PwC Brasil, 2023, p. 14).

Até 2025, a projeção é que aproximadamente 20% da população brasileira desfrutará dos benefícios da internet 5G, conforme afirma a PwC Brasil. Esta tecnologia avançada

proporcionará velocidades de ligação muito mais rápidas, desempenhando assim um papel crucial na melhoria da acessibilidade à Internet em áreas mal servidas.

Outros fatores, além dos discutidos anteriormente, desempenharam um papel significativo no crescimento da disponibilidade de internet no Brasil. Esses fatores incluem:

- O advento da telefonia móvel na década de 1990, a acessibilidade da Internet tornou-se omnipresente, permitindo aos indivíduos ligarem-se online a partir de qualquer local.
- A ascensão da literacia digital, que começou na década de 2000, desempenhou um papel significativo na promoção de uma sensação de facilidade e confiança entre os indivíduos quando se trata de utilizar a Internet.
- O aumento da acessibilidade e popularidade da internet pode ser atribuído à ascensão dos smartphones, que começaram a surgir na década de 2010.Os benefícios sociais resultantes do aumento da disponibilidade de acesso à Internet no Brasil são numerosos, podemos notar:
- O advento da Internet facilitou uma melhor conectividade entre os indivíduos, permitindo uma comunicação rápida e sem esforço, independentemente das barreiras geográficas.
- A Internet revolucionou a forma como acessamos e obtemos informações, tornando-as mais prontamente disponíveis e facilmente acessíveis aos indivíduos.
- A Internet proporcionou aos indivíduos a oportunidade de se envolverem mais ativamente na sociedade, expandindo o seu envolvimento em áreas como o ativismo, a política e a educação. Este aumento da participação social é resultado direto da influência da Internet.
- As empresas e os trabalhadores registaram um aumento na produtividade graças à Internet.

A Internet desempenhou um papel importante no aumento do consumo, com atividades como compras online e streaming de conteúdo contribuindo para esse aumento.

O avanço positivo da acessibilidade à internet no Brasil é um empreendimento transformador, pois confere inúmeras vantagens à sociedade. Melhorando a comunicação, a disseminação de informações, a educação e o entretenimento, a Internet permite que os indivíduos se envolvam nessas atividades com maior eficiência. Além disso, a Internet desempenha um papel fundamental na promoção do progresso económico e social da nação.

## 1.2. PRINCIPAIS TIPOS DE FRAUDES VIRTUAIS E SEU IMPACTO ECONÔMICO E SOCIAL

Consoante noção cediça, desde o advento da internet e do grande aumento do número de seus usuários, a incidência de crimes virtuais cresceu consideravelmente. Nesse sentido, Oliveira (2022), argumenta que as fraudes virtuais são uma ameaça crescente para a sociedade, causando danos econômicos e pessoais às vítimas. De mais a mais, estes crimes têm se tornado cada vez mais sofisticados, fato que se justifica, em parte, pela facilidade de manuseio dos meios virtuais, pelos avanços tecnológicos, bem como pela dificuldade em se punir os criminosos, tendo em vista a dificuldade em descobrir suas identidades e a ausência de legislações específicas sobre o tema.

A fraude virtual refere-se a atos criminosos que utilizam a Internet como meio para enganar as vítimas e obter benefícios financeiros ou outros. Estes crimes trazem sérios problemas à sociedade, uma vez que causam não apenas perdas econômicas e materiais, mas geram também danos mentais às vítimas.

Acredita-se que o fenômeno é devido, principalmente, ao crescimento exponencial do uso da internet na rotina dos brasileiros desde a pandemia do vírus Covid19. “Isso criou um ambiente propício para que criminosos explorassem as vulnerabilidades nesses sistemas”, disse David Marques, sociólogo e coordenador do Fórum Brasileiro de Segurança Pública.

Por assim ser, segundo o Podcast Segurança Digital (2023), as fraudes virtuais estão evoluindo rapidamente, uma vez que os fraudadores estão sempre desenvolvendo novas técnicas para enganar as vítimas. Dessa forma, conclui-se que as modalidades de crimes com o uso da internet são variadas — e só vêm crescendo.

Os crimes cibernéticos baseiam-se em três fundamentos principais:

- Confiança: A fraude virtual baseia-se frequentemente na confiança da vítima na instituição e nas pessoas com quem interage online.
- Lacunas: As fraudes online exploram frequentemente os pontos fracos das vítimas, como a falta de conhecimentos sobre segurança cibernética ou a falta de oportunidade de prestar atenção.
- Oportunidade: A fraude virtual é muitas vezes mais comum em momentos de oportunidade, como durante uma crise econômica ou evento de impacto.

Para Santos (2023), os fraudadores estão sempre inovando, desenvolvendo novas técnicas para enganar as vítimas. Um exemplo recente é o uso de *deepfakes*, vídeos ou áudios falsos criados por meio de inteligência artificial que podem ser usados para criar vídeos de pessoas famosas fazendo declarações falsas ou comprometedoras.

Como se depreende, existem muitos tipos de golpes cibernéticos, sendo estes os principais:

- *Phishing* (pesca) – é uma forma de fraude que envolve o envio de mensagens falsas, muitas vezes por e-mail, fingindo ser uma instituição ou pessoa confiável. O objetivo é enganar as vítimas para que forneçam informações pessoais ou financeiras;
- Software malicioso (Malware) – é um software malicioso que pode ser instalado no dispositivo da vítima sem o conhecimento da vítima. O malware pode ser usado para roubar dados, assumir o controle do dispositivo da vítima ou espalhar outras formas de malware;
- Roubo de identidade: Criminosos obtêm informações pessoais, como números de CPF, RG e dados bancários, para se passarem por outra pessoa, realizando transações fraudulentas em nome da vítima;
- Clonagem de cartões: Obtêm-se dados de cartões de crédito ou débito para replicá-los em um novo cartão, utilizado para realizar compras fraudulentas ou saques indevidos;
- Fraude no comércio eletrônico – refere-se a crimes que ocorrem durante compras online. Os fraudadores podem se passar por lojas ou vendedores legítimos para induzir as vítimas a obterem seus dados financeiros, ou até mesmo criam anúncios falsos ou sites fraudulentos são criados para vender produtos inexistentes ou de baixa qualidade, enganando o consumidor e induzindo-o a erro.

De maneira geral, as fraudes virtuais custaram à economia global cerca de US$ 6 trilhões em 2022, um aumento de 10% em relação ao ano anterior. Sob tal ambulação, cumpre ressaltar que o Brasil é um dos países mais afetados por esse tipo de crime, com perdas estimadas em R$ 10 bilhões, afirma Forbes (2023).

## 1.3. AS FORMAS DE ESTELIONATO CIBERNÉTICO NO BRASIL

A realidade anteriormente abordada não é diferente no que se refere ao estelionato cibernético, conduta criminosa na qual o agente faz uso da internet e de meios digitais para enganar vítimas em benefício próprio, ao passo em que se utiliza da ingenuidade, da confiança ou da ausência de saber tecnológico das vítimas para obter vantagem ilícita para si.

Este crime pode ser cometido por meio de diversas técnicas e estratégias fraudulentas, e tem se tornado uma questão significativa no Brasil. Isso pois o estelionato virtual atingiu números surpreendentes no ano de 2022. Com base na 17ª edição do Anuário Brasileiro de Segurança Pública foram mais de 1,8 milhão de ocorrências, o que significa um crescimento de 326,3% em quatro anos nessa modalidade.

Nesse espeque, criminosos criam páginas fictícias, por meio das quais fazem propostas chamativas e, em muitos casos, enviam mensagens por *WhatsApp* se passando por outros indivíduos, o que acaba por ludibriar as vítimas mais vulneráveis. Essas fraudes aplicadas caracterizam o crime de estelionato virtual.

A caracterização do crime de estelionato requer quatro pressupostos, quais sejam: a obtenção de vantagem ilícita; que seja causado o prejuízo a outra pessoa; o uso de meio de ardil ou artimanha; e que esteja demonstrada a intenção do agente em enganar alguém ou a induzir ao erro, de forma se ilude e/ou engana a vítima, a fim de que ela, por vontade própria, entregue bens ou objetos, por ter sido induzida a uma visão distorcida dos fatos.

A respeito da expressão "vantagem ilícita", Fernando Capez (2020) ensina que se trata do objeto material do crime e, caso o agente esteja agindo em razão de uma vantagem devida, a conduta é tipificada como exercício arbitrário das próprias razões, delito previsto no art. 345, do Código Penal.

Na mesma perspectiva, os golpes cometidos através das redes sociais também cresceram significativamente. Nessa esfera, inúmeros golpes, como por exemplo pedidos de doações enganosas e a disseminação de informações fraudulentas vêm sendo aplicados por meio de perfis falsos, visando adquirir valores materiais ou roubar dados pessoais e financeiros dos usuários.

Sob esse ângulo, uma das formas com maior incidência de estelionato virtual é o *phishing*, na qual os agentes criam e-mails, mensagens ou sites falsos que imitam instituições legítimas para induzir as vítimas a compartilhar informações confidenciais, como senhas bancárias, números de cartão de crédito ou dados pessoais. Esses dados são então usados para cometer fraudes financeiras.

Outra prática comum é o golpe de clonagem de cartões, em que os criminosos obtêm os dados de um cartão e os replicam em outro, geralmente para efetuar compras fraudulentas ou saques indevidos.

Da mesma forma, o comércio eletrônico também é um terreno fértil para o estelionato virtual. Os golpistas aproveitam-se de sites falsos ou de anúncios fraudulentos para vender produtos inexistentes ou de qualidade inferior, ludibriando consumidores desavisados.

Além disso, há os esquemas de pirâmide financeira, em que os criminosos prometem altos retornos sobre investimentos, mas na verdade estão apenas redirecionando o dinheiro dos novos investidores para pagar os antigos, sem nenhum sustento financeiro real.

De forma evidente, as modalidades de estelionato virtual são diversas e continuamente evoluem, adaptando-se aos avanços tecnológicos e às mudanças nos comportamentos das pessoas online. Além das já mencionadas, outras práticas vêm ganhando destaque.

Um exemplo são as práticas de engenharia social que têm se destacado, onde os criminosos se aproveitam da persuasão e manipulação psicológica para convencer as vítimas a agirem contra seus próprios interesses, fornecendo informações confidenciais ou executar ações que resultam em prejuízo financeiro.

Outro aspecto importante é o uso de falsos sites de leilões, onde bens são anunciados para venda, mas o produto não existe ou não é entregue após o pagamento. Isso afeta não apenas consumidores individuais, mas também empresas que confiam nesses mecanismos para realizar transações comerciais.

Em conclusão, o estelionato virtual no Brasil apresenta diversas modalidades que exploram a vulnerabilidade das pessoas na era digital. A prevenção, a educação e o fortalecimento das leis e da capacidade de aplicação delas são fundamentais para mitigar esse tipo de crime e proteger os cidadãos e instituições contra essas práticas fraudulentas cada vez mais sofisticadas e prejudiciais.

## 2. A EVOLUÇÃO DA INTELIGÊNCIA ARTIFICIAL E SUAS CONSEQUÊNCIAS

### 2.1. CARACTERÍSTICAS E DESAFIOS DA EVOLUÇÃO DA INTELIGÊNCIA ARTIFICIAL

A pesquisa sobre inteligência artificial (IA) tem crescido rapidamente desde sua criação na década de 1950, segundo Russell e Norvig (2016). E, de acordo com Poole e Mackworth (2017), a inteligência artificial é definida como a capacidade de um sistema de computador de realizar tarefas que normalmente exigem inteligência humana, como planejamento, aprendizado, compreensão de linguagem natural e reconhecimento de voz.

Como resultado, a Inteligência Artificial (IA) está se tornando cada vez mais prevalente em nossas vidas, com aplicações como reconhecimento de voz e tomada de decisões complexas. O Brasil, assim como muitos outros países, tem visto o uso da IA em uma variedade de setores, como saúde, educação, finanças, transporte e muito mais. Por exemplo, a indústria de saúde tem usado a IA para diagnosticar doenças com mais precisão, criar tratamentos personalizados e acelerar a pesquisa médica. O setor financeiro tem usado algoritmos de IA para fazer previsões e analisar grandes quantidades de dados, fornecendo informações que os humanos normalmente não conseguiriam identificar.

Primeiramente destaca-se o que foi afirmado por Goodfellow, Bengio e Courville (2016), a inteligência artificial é composta por uma variedade de capacidades essenciais. Para começar, a IA possui a capacidade de aprender e adaptar-se a novas circunstâncias. Técnicas de aprendizado de máquina são frequentemente usadas para fazer isso. Essas técnicas ensinam os sistemas de IA a trabalhar com grandes conjuntos de dados e aprender a fazer previsões ou tomar decisões com base nesses dados.

Em segundo lugar, Chen, Min, Yu, Chen e Hao (2020) afirmam que a inteligência artificial pode processar grandes volumes de dados muito mais rapidamente do que os humanos. A análise de grandes conjuntos de dados e a condução de veículos autônomos são algumas das muitas aplicações da IA que podem ser feitas com isso.

Assim, a IA oferece várias vantagens. A principal é a eficiência operacional. A IA pode aumentar a eficiência operacional in várias áreas, como a manufatura e os serviços financeiros. As organizações também podem tomar decisões mais fundamentadas e precisas analisando grandes quantidades de dados com algoritmos de IA avançados. A IA também pode melhorar.

Apesar de seu potencial a IA tem muitos problemas apesar de seu potencial. A privacidade e a ética são os principais problemas. Afirmam Cath, Wachter, Mittelstadt, Taddeo e Floridi (2018) que devido à frequência com que a IA é empregada no processamento de grandes volumes de dados, muitas vezes pessoais, há dúvidas sobre como esses dados são usados e protegidos. Outro desafio significativo é a deslocação de postos de trabalho é uma

preocupação importante porque a automatização da IA pode resultar em desemprego e deslocação de postos de trabalho, especialmente em setores onde a automatização de tarefas repetitivas é fácil de fazer. Uma desvantagem adicional da IA é sua dependência de dados.

Além dos supracitados a transparência e a aplicabilidade da IA são outros grandes desafios, além dos mencionados anteriormente. De acordo com Rudin (2019), uma grande quantidade de algoritmos de IA são considerados "caixas-pretas" devido ao fato de serem difíceis de entender o processo pelo qual eles tomam suas decisões. Quando as decisões tomadas pelo IA precisam ser justificadas, isso pode ser um problema.

Portanto, a adoção da IA está tendo um impacto significativo e duradouro na humanidade. A IA vem alterando nossa comunicação, aprendizado, trabalho e até mesmo nossas mentes. Mas junto com os benefícios, também há questões. A IA tem o potencial para aumentar as desigualdades existentes, pois aqueles com acesso à tecnologia colhem os benefícios, enquanto aqueles sem acesso são abandonados. Além disso, a IA também levanta questões éticas complexas, como a justiça e a transparência na tomada de decisões.

Em suma, a inteligência artificial é uma força poderosa que está transformando nosso mundo. Para maximizar os benefícios e minimizar os riscos desta tecnologia, é fundamental que continuemos estudando-a. Como sociedade, devemos colaborar para garantir que a IA seja usada de maneira justa e responsável, e que todos tenham a chance de participar e se beneficiar de suas promessas.

## 2.2. A RELAÇÃO ENTRE O AVANÇO DA INTELIGÊNCIA ARTIFICIAL E O CRESCIMENTO DOS CASOS DE ESTELIONATO VIRTUAL NO BRASIL

A inteligência artificial (IA) tem sido tornado uma tecnologia revolucionária em várias áreas, trazendo tanto vantagens quanto problemas. O aumento preocupante nos casos de estelionato virtual no Brasil tem acompanhado o avanço da IA.

Surgindo na década de 1950, a IA tem sua origem praticamente confundida com a própria origem do computador. Sobre o entendimento Russell e Norvig (2016) atualmente, estamos atravessando um período de otimismo sobre os possíveis benefícios que a IA pode prover. A inteligência artificial está usada em uma variedade de produtos e serviços, incluindo, mas não limitado a buscas na internet, compras do comércio eletrônico, serviços bancários virtuais, aplicativos para *smartphones* e outros. No entanto, embora a IA possa oferecer várias vantagens, como praticidade, velocidade e qualidade dos serviços, também traz questões

éticas, morais e sociais, bem como riscos, caso seja usada de forma irresponsável ou para fins desfavoráveis.

No Brasil, os casos de estelionato virtual estão aumentando in conjunto com o desenvolvimento da inteligência artificial. O estelionato virtual envolve a utilização de meios eletrônicos para enganar e fraudar pessoas, causando danos financeiros e à segurança digital. Como demonstrado por pesquisas realizadas no Brasil sobre o aumento do estelionato virtual, os criminosos cibernéticos têm se aproveitado das vulnerabilidades encontradas em sistemas automatizados e algoritmos de inteligência artificial para perpetrar golpes cada vez mais sofisticados.

Destaca-se que o número de estelionatos no Brasil mais que quadruplicou nos últimos cinco anos, segundo a pesquisa do site G1 (2023). Em 2022, foram registrados 1.819.409 casos, 326% a mais que em 2018, quando foram registrados 426.799 casos. Além disso, como resultado da pandemia de COVID-19, o país viu um aumento ainda mais expressivo no crime eletrônico. Em 2021, foram registrados 120.470 casos; em 2022, foram 200.322 casos, aumentando 66,2%.

É notável que vínculo entre o aumento dos casos de estelionato virtual no Brasil e o desenvolvimento da inteligência artificial está complexo. Por outro lado, a IA pode detectar e prevenir fraudes analisando padrões de comportamento e identificando atividades suspeitas. No entanto, estudos sobre as aplicações da IA em crimes cibernéticos mostram que os criminosos também têm explorado a IA para aprimorar suas técnicas de engenharia social e *phishing*, tornando mais difícil a detecção de fraudes.

É entendido pela Forbes Brasil (2023) que o aumento do estelionato virtual impulsionado pela IA tem um efeito significativo na sociedade brasileira. Além de sofrer perdas financeiras substanciais, as vítimas desses golpes podem sofrer danos à sua reputação e ao seu bem-estar emocional. Ademais, o estelionato virtual pode prejudicar a confiança do sistema financeiro como um todo e nas transações online.

Vê-se que a IA foi empregada para automatizar e melhorar uma variedade de processos, incluindo aqueles utilizados por criminosos para cometer estelionato. A IA permitiu que os golpistas usassem ferramentas mais complexas para enganar e cometer fraudes. Por exemplo, eles podem usar IA para enganar sistemas de segurança, criar sites e e-mails que parecem verdadeiros, ou até mesmo imitar vozes humanas em chamadas telefônicas.

Também segundo a Forbes Brasil (2023) sabe-se que o aumento do estelionato virtual impulsionado pela IA tem um efeito significativo na sociedade brasileira. Além de sofrer perdas financeiras substanciais, as vítimas desses golpes podem sofrer danos à sua reputação e ao seu bem-estar emocional. Além disso, a estelionato virtual tem o potencial de diminuir a confiança nas

Além disso, o Senado Federal (2023) afirma que para combater o estelionato virtual, governos, empresas e organizações civis devem trabalhar mais juntos. Isso inclui investigar e punir os infratores, compartilhar informações sobre ameaças e desenvolver novas tecnologias de segurança.

É importante salientar que a IA em si não é inerentemente perigosa. Como toda tecnologia, sua influência depende de como é usada. Assim, embora alguns indivíduos possam utilizar a IA para cometer delitos, outros indivíduos estão empregando a mesma tecnologia para detectar e prevenir fraudes. Assim, para garantir que a IA seja usada de maneira ética e responsável, é essencial criar e aplicar regulamentos e medidas de segurança sólidas, conforme Bostrom (2014).

## 2.3. O IMPACTO ECONÔMICO, SOCIAL E JURÍDICO DA FRAUDE CIBERNÉTICA NAS VÍTIMAS, NOS PERPETRADORES E NA SOCIEDADE EM GERAL

A fraude cibernética é problema crescente que afeta a segurança digital, além de impactar de forma ampla e profunda os aspectos sociais, econômicos e jurídicos no Brasil.

No Brasil, este tipo de fraude tem um grande impacto na economia, causando perdas financeiras para empresas e indivíduos. A recuperação de dados, a reparação de sistemas comprometidos e a compensação por danos causados por fraudes cibernéticas são todos custos financeiros significativos. Além disso, segundo Santos e Lima (2022) a perda de confiança dos consumidores e investidores devido a incidentes de fraude cibernética pode afetar a reputação e a credibilidade das empresas, resultando em impactos econômicos a longo prazo.

A respeito das vítimas individuais na ótica de Anderson (2013), a perda direta de dinheiro pode ser devastadora para as vítimas individuais. Além disso, as empresas enfrentam despesas substanciais como resultado da detecção, prevenção e resposta a incidentes de fraude cibernética na análise de Moore, Clayton e Anderson (2009). Segundo Choo (2008), a fraude cibernética tem o potencial de desestabilizar os mercados financeiros e diminuir a confiança dos consumidores. Os investimentos em cibersegurança do Brasil estão projetados para atingir

8,3 bilhões de reais (1,7 bilhões de dólares) em 2023 e podem chegar a 10,8 bilhões de reais (2,2 bilhões de dólares) até 2026 (Evolving Threats: The State of Personal Data Protection in Brazil).

Já no aspecto social, no Brasil, a fraude cibernética tem consequências que vão além da economia. As consequências sociais da fraude cibernética incluem violação da privacidade dos cidadãos, roubo de informações pessoais e disseminação de fake News e desinformação online. Essas práticas prejudicam a confiança na segurança digital e na veracidade das informações online, tendo um efeito na sociedade como um todo. Além disso, Oliveira (2021) relata que a exposição a golpes cibernéticos pode causar estresse, ansiedade e desconfiança entre os usuários da internet, o que afeta o bem-estar social.

Ainda no âmbito social, a perda de confiança nas instituições digitais pode ser causada pela fraude cibernética. Isso, segundo Button, Lewis e Tapley (2014) pode fazer com que as pessoas se absterem de participar da economia digital, o que, por sua vez, torna mais difícil obter serviços essenciais. Além disso, Brenner (2010) ressalta que as vítimas de fraude cibernética geralmente enfrentam um alto grau de estresse psicológico e emocional. No Brasil, um estudo de Lemos (2023) do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação revelou que 42% dos brasileiros estão "muito preocupados" com seus dados quando fazem compras online.

Do ponto de vista jurídico, A fraude cibernética no Brasil levanta questões complicadas sobre responsabilidade legal, punição de criminosos cibernéticos e proteção dos direitos dos cidadãos. A aplicação eficaz da lei está desafiada por falta de legislação específica e dificuldades para rastrear e identificar os autores de crimes cibernéticos. Além disso, Silva (2023) mostra que a cooperação internacional para investigar e processar crimes cibernéticos torna o aspecto jurídico da fraude cibernética no Brasil mais complicado.

Além do ressaltado, a fraude cibernética apresenta desafios únicos do âmbito jurídico. Nesse sentido, Wall (2007), argumenta que a aplicação eficiente das leis existentes é dificultada pela natureza transnacional da internet e pela rapidez com que os crimes cibernéticos podem ser cometidos. Além disso, a falta de harmonização das leis de cibercrime em todo o mundo complica ainda mais os esforços de aplicação da lei. No Brasil, muitas mudanças regulatórias foram conduzidas nos últimos anos, levando à consolidação de uma política de cibersegurança e ao desenvolvimento do projeto 5G após a conclusão do lance público em bandas de frequência em 2021 como Carapeto (2022) relatou.

No Brasil e no mundo houve vários casos notáveis de fraude cibernética. Segundo a BBC (2018) em 2018, a Cambridge Analytica, uma empresa de análise de dados, obteve acesso indevido aos dados pessoais de 87 milhões de usuários do Facebook sem o consentimento deles. As informações foram utilizadas para fins políticos, incluindo a campanha eleitoral de Donald Trump nos Estados Unidos. O escândalo abalou a confiança dos usuários na plataforma e gerou um debate global sobre privacidade online.

Já pela Polícia Federal (2023), o denominado "golpe do *Whatsapp*", que explora a engenharia social para roubar dados pessoais e financeiros das vítimas, se tornou um dos principais crimes digitais da atualidade. Através de mensagens falsas que se passam por familiares ou amigos, os criminosos induzem as vítimas a fornecerem informações confidenciais, como senhas bancárias ou números de cartão de crédito. O golpe, que afeta pessoas de todas as idades e classes sociais, já causou prejuízos milionários em diversos países, incluindo o Brasil.

Concluindo, a fraude cibernética no Brasil tem impactos profundos nos aspectos econômico, social e jurídico da sociedade. Para enfrentar esse desafio crescente, é essencial adotar medidas preventivas, como a implementação de políticas de segurança cibernética robustas, a conscientização dos usuários da internet e a atualização constante da legislação para lidar com crimes cibernéticos. A colaboração entre setores público e privado, a cooperação internacional e o investimento em tecnologias de segurança são fundamentais para mitigar o impacto da fraude cibernética e proteger a economia, a sociedade e a justiça no Brasil.

## 3. SEGURANÇA DIGITAL: MEIOS DE PREVENÇÃO E COMBATE À FRAUDE CIBERNÉTICA

### 3.1. POLÍTICAS PÚBLICAS EM COMBATE AO ESTELIONATO VIRTUAL

O estelionato virtual emerge como uma preocupação contemporânea, demandando ações coordenadas e eficazes por parte das políticas públicas. Este estudo propõe uma análise das estratégias adotadas pelo Estado no enfrentamento desse fenômeno, com foco na proteção dos cidadãos frente aos riscos inerentes ao ambiente digital.

De acordo com Smith (2018), o estelionato virtual se caracteriza pela utilização de meios eletrônicos para a prática de fraudes, envolvendo desde a obtenção ilegal de

informações pessoais até a manipulação de transações financeiras. Nesse contexto, a abordagem tradicional das políticas públicas se mostra inadequada, exigindo uma revisão e adaptação constantes para lidar com as novas formas de crime.

Uma das principais estratégias adotadas pelos governos é a implementação de legislações específicas para o combate ao crime cibernético. Conforme observado por Jones (2020), leis que criminalizam práticas como *phishing*, clonagem de cartões e invasão de sistemas têm sido fundamentais para dissuadir potenciais infratores e fortalecer a punição aos responsáveis.

Além da esfera legal, as políticas públicas também se voltam para a educação e conscientização da população sobre os riscos do estelionato virtual. Campanhas de mídia e programas de educação digital são essenciais para capacitar os usuários a reconhecerem e evitarem tentativas de fraude online, reduzindo assim o número de vítimas.

Outra frente importante de atuação é o fortalecimento da cooperação internacional no combate ao crime cibernético. Como salientado por Johnson (2021), o estelionato virtual muitas vezes transcende fronteiras, exigindo uma abordagem global que envolva a troca de informações entre países, a harmonização de legislações e a cooperação em investigações.

Por fim, é crucial destacar o papel das tecnologias de segurança na proteção dos usuários contra o estelionato virtual. Autores como García (2017) apontam para a importância do desenvolvimento contínuo de ferramentas de criptografia, autenticação multifatorial e detecção de anomalias, como forma de mitigar os riscos associados às transações online.

Em síntese, as políticas públicas em combate ao estelionato virtual devem abranger uma gama ampla de medidas, desde a criação de legislações específicas até a promoção da educação digital e o investimento em tecnologias de segurança. Somente por meio de uma abordagem abrangente e coordenada será possível enfrentar eficazmente esse desafio crescente no mundo digital.

## 3.2. A NECESSIDADE DE EDUCAÇÃO DIGITAL NO BRASIL

Os crimes virtuais têm se tornado uma preocupação crescente no Brasil, exigindo abordagens eficazes por parte das políticas públicas e da sociedade em geral. Neste contexto, a educação digital emerge como uma ferramenta fundamental para capacitar os cidadãos a reconhecerem e evitarem potenciais ameaças no ambiente online.

De acordo com Silva (2019), a falta de conhecimento sobre os riscos cibernéticos contribui para a vulnerabilidade dos usuários brasileiros, tornando-os alvos fáceis para criminosos virtuais. Diante disso, investir em programas de educação digital se apresenta como uma medida essencial para conscientizar a população e reduzir a incidência de crimes como *phishing*, roubo de identidade e fraudes financeiras.

A importância da educação digital também é destacada por Souza (2020), que ressalta a necessidade de promover uma cultura de segurança cibernética desde a educação básica. Ao incorporar o ensino de habilidades como proteção de dados, verificação de fontes online e uso seguro de dispositivos eletrônicos nas escolas, é possível preparar as futuras gerações para enfrentar os desafios do mundo digital.

Além disso, a educação digital pode desempenhar um papel crucial na inclusão digital e na redução das desigualdades sociais. Conforme apontado por Oliveira (2018), o acesso à informação e à formação em tecnologia da informação pode empoderar grupos historicamente marginalizados, tornando-os menos suscetíveis a golpes e fraudes online.

É importante ressaltar que a educação digital não se limita apenas aos indivíduos, mas também deve englobar as empresas e instituições governamentais. Segundo Santos (2021), programas de treinamento e conscientização voltados para funcionários e gestores são essenciais para fortalecer as defesas cibernéticas das organizações e evitar ataques de cunho financeiro e de vazamento de dados.

Em suma, a necessidade de educação digital no Brasil em combate aos crimes virtuais é inegável. Por meio do desenvolvimento de programas abrangentes e acessíveis, é possível capacitar os cidadãos a navegarem com segurança no mundo digital, reduzindo assim a incidência e o impacto dos delitos cibernéticos.

## 3.3. LEGISLAÇÃO E FRAUDE: NOVAS FORMAS DE REGULAMENTAÇÃO DA FRAUDE CIBERNÉTICA NO BRASIL

A crescente incidência de fraudes cibernéticas no Brasil tem impulsionado a necessidade de atualização e criação de novas formas de regulamentação para lidar com esse fenômeno. Neste estudo, investigamos as tendências emergentes na legislação brasileira relacionada à fraude cibernética, bem como seu impacto na prevenção e punição desses crimes.

A Lei nº 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, representa um marco inicial na legislação brasileira sobre crimes cibernéticos. Esta lei criminaliza a invasão de dispositivos eletrônicos, prevendo penas para aqueles que violarem indevidamente sistemas informáticos, furtarem dados ou prejudicarem o funcionamento de computadores alheios.

Além da Lei Carolina Dieckmann, outras iniciativas legislativas têm buscado ampliar o escopo de combate à fraude cibernética no Brasil. Um exemplo notável é a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), que estabelece diretrizes para o tratamento de informações pessoais por parte de empresas e organizações, visando proteger a privacidade e a segurança dos dados dos cidadãos.

No entanto, apesar dos avanços legislativos, ainda persistem lacunas na regulamentação da fraude cibernética no Brasil. Como apontado por Silva (2020), a falta de uma legislação específica para crimes como *phishing*, *ransomware* e fraude online dificulta a investigação e punição dos responsáveis, deixando os cidadãos vulneráveis a ataques virtuais.

Diante desse cenário, propostas de novas leis e regulamentações têm sido discutidas no âmbito legislativo brasileiro. Uma delas é o Projeto de Lei nº 2.630/2020, conhecido como Lei das *Fake News*, que visa combater a disseminação de informações falsas e a manipulação digital, crimes frequentemente associados à fraude cibernética.

Além das iniciativas legislativas, é fundamental fortalecer os mecanismos de cooperação entre órgãos governamentais, instituições financeiras e empresas de tecnologia na prevenção e combate à fraude cibernética. Como destacado por Oliveira (2019), a colaboração entre diferentes atores é essencial para identificar e neutralizar ameaças virtuais em tempo hábil, protegendo assim a segurança e integridade do ambiente digital no Brasil.

Em resumo, a regulamentação da fraude cibernética no Brasil está em constante evolução, refletindo a necessidade de adaptação às novas ameaças e tecnologias. A implementação de leis mais abrangentes e eficazes, aliada à cooperação entre setores público e privado, é essencial para enfrentar esse desafio complexo e proteger os cidadãos contra os riscos do mundo digital.

## CONCLUSÃO

A presente pesquisa, ao investigar a crescente incidência de estelionato cibernético no Brasil à luz da evolução da inteligência artificial, oferece uma visão aprofundada e

multifacetada dos desafios contemporâneos enfrentados pela sociedade brasileira. Ao longo desta análise, delineamos não apenas o panorama atual das fraudes cibernéticas, mas também as dinâmicas que impulsionam essa modalidade criminosa em um contexto de rápida transformação tecnológica. É imperativo, portanto, sintetizar as principais conclusões deste estudo e discutir as implicações para futuras políticas públicas, medidas de segurança e o arcabouço jurídico.

Em primeiro lugar, a expansão do acesso à internet no Brasil, um fenômeno observado nas últimas duas décadas, embora tenha democratizado o uso da tecnologia, também expôs uma parcela significativa da população a riscos cibernéticos. O aumento exponencial de usuários conectados criou um terreno fértil para a proliferação de fraudes virtuais, evidenciando a necessidade de estratégias de segurança robustas e inclusivas. O estudo revelou que a falta de conhecimento técnico e a ausência de uma cultura de segurança digital tornaram os usuários mais vulneráveis aos ataques de estelionatários cibernéticos, que se aproveitam dessas lacunas para perpetrar seus crimes.

Ademais, a pesquisa detalhou os principais tipos de fraudes cibernéticas, incluindo *phishing*, roubo de identidade, fraudes financeiras e esquemas de pirâmide, destacando o impacto econômico e social devastador dessas atividades ilícitas. As perdas financeiras sofridas por indivíduos e empresas são apenas a ponta do iceberg; o verdadeiro dano reside na erosão da confiança na economia digital e no retardamento do progresso tecnológico. A inovação, que deveria ser um motor de crescimento e inclusão, encontra-se ameaçada pela desconfiança e pela insegurança digital.

Paralelamente, a evolução da inteligência artificial foi identificada como um fator crucial na sofisticação das fraudes cibernéticas. A IA, com suas capacidades avançadas de aprendizado de máquina e análise de big data, não apenas potencializou a eficiência e a precisão dos ataques, mas também tornou mais complexa a tarefa de detecção e prevenção por parte das autoridades e das vítimas. A correlação entre o avanço das tecnologias de IA e o aumento dos casos de estelionato virtual sublinha a necessidade urgente de desenvolver tecnologias de segurança igualmente avançadas e adaptativas.

Nesse contexto, o impacto econômico, social e jurídico das fraudes cibernéticas foi exaustivamente explorado. As vítimas não enfrentam apenas perdas financeiras, mas também sofrem danos psicológicos e emocionais profundos. Por outro lado, os perpetradores, quando identificados e processados, revelam as falhas e as necessidades de atualização no sistema

jurídico. Além disso, a sociedade como um todo lida com as consequências da crescente desconfiança no ambiente digital, o que demanda uma resposta coordenada e multidisciplinar.

Por conseguinte, a pesquisa enfatiza a importância de políticas públicas bem delineadas e eficazes no combate ao estelionato virtual. Estas políticas devem não apenas focar na punição dos infratores, mas também na prevenção das fraudes, por meio de campanhas de conscientização e educação digital. A alfabetização digital emerge como um pilar fundamental para mitigar a vulnerabilidade dos usuários e fortalecer a resiliência contra os golpes cibernéticos.

Além disso, a legislação precisa acompanhar a velocidade das transformações tecnológicas. As lacunas legais identificadas durante a pesquisa indicam a necessidade de uma regulamentação mais ágil e adaptativa, capaz de responder prontamente às novas formas de fraude que surgem com o avanço da IA. Propostas legislativas inovadoras e a revisão contínua do marco jurídico são essenciais para garantir a proteção dos cidadãos e a integridade do ambiente digital.

Em suma, a presente pesquisa não apenas elucida as complexas interações entre a expansão do acesso à internet, a evolução da inteligência artificial e o aumento das fraudes cibernéticas, mas também propõe um conjunto de recomendações práticas e estratégicas para enfrentar esse desafio multifacetado. É evidente que a segurança digital no Brasil depende de uma abordagem integrada que englobe políticas públicas eficazes, educação digital abrangente e uma legislação atualizada e robusta. Somente através de uma resposta coordenada e proativa será possível mitigar os impactos dessa ameaça crescente e assegurar um ambiente digital seguro e confiável para todos os brasileiros.

## GROWING CASES OF CYBER FRAUD IN BRAZIL DUE TO THE EVOLUTION OF ARTIFICIAL INTELLIGENCE


## ABSTRACT

In recent years, Brazil has seen an increase in cases of cyber fraud, driven by the evolution of artificial intelligence (AI). Criminals use AI to improve phishing techniques, create convincing deepfakes and automate large-scale attacks, resulting in more sophisticated scams. These frauds cause huge financial losses and undermine consumer confidence in online transactions. To mitigate these risks, it is crucial to invest in advanced defense technologies, improve authentication systems and educate users about digital security, in addition to improving the legislative framework on the subject. Effectively combating cyber fraud depends on joint action between the public and private sectors.

## REFERÊNCIAS


ALLAHRAKHA, Naeem. **Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age. Legal Issues in the Digital Age**, v. 4, n. 2, p. 78121, 28 Jul. 2023.

ANDERSON, R. et al. **Measuring the cost of cybercrime. In: THE economics of information security and privacy** (pp. 265-300). Berlin, Heidelberg: Springer, 2013.

BRENNER, S. W. **Cybercrime: criminal threats from cyberspace**. Santa Barbara, CA: ABCCLIO, 2010.

BUTTON, M.; LEWIS, C.; TAPLEY, J. Not a victimless crime: The impact of fraud on individual victims and their families. **Security Journal**, v. 27, n. 1, p. 36-54, 2014.

**BBC Brasil**. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 12 maio 2024.

BOSTROM, N**.** Superintelligence: Paths, Dangers, Strategies. Oxford: **Oxford University Press**, 2014.

BRASIL. **LEI 12.737, DE 30 DE NOVEMBRO DE 2012.** Dispõe sobre a Tipificação Criminal de Delitos Informáticos e dá outras providências. Brasília, 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20112014/2012/lei/l12737.htm; Acesso em: 10 dez. 2023.

BRASIL. 2021. **LEI 14.155, DE 27 DE MAIO DE 2021**. Brasília, 27 de maio de 2021; 200o da Independência e 133o da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm#:~:text=Altera%20o%20Decreto%2DLei%20n%C2%BA,Penal)%2C%20para%20definir%20a%20compet%C3%AAncia. Acesso em: 10 dez. 2023.

CAPEZ, Fernando. Parte Especial arts. 121 a 212. **Coleção Curso de direito penal**. V. 2, 20. ed. São Paulo: Saraiva Educação, 2020.

CAPEZ, Fernando. Parte Especial arts. 213 a 359-h. **Coleção Curso de Direito Penal**. v. 3 - 18. ed. - São Paulo: Saraiva Educação, 2020.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. Rio de Janeiro: Brasport, 2014.

CHOO, K. K. R. **Organised crime groups in cyberspace: a typology**. Trends in Organized Crime, v. 11, n. 3, p. 270-295, 2008.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Relatório de Monitoramento da Internet no Brasil 2022**. São Paulo, 2022. Disponível em: https://cetic.br/media/docs/publicacoes/2023/relatorio_monitoramento_internet_brasil_2022.pdf. Acesso em: 10 dez. 2023.

Carapeto, R., Calil, A.L. **Cybersecurity regulation in Brazil and Latin America: an overview. Int. Cybersecur. Law Rev**. 3, 385–410. 2022. Disponível em: https://doi.org/10.1365/s43439022-00055-w. Acesso em: 12 maio 2024.

**Forbes Brasil.** Por que a IA pode tornar os crimes digitais mais eficientes. 22 fev. 2024. Disponível em: https://forbes.com.br/forbesmoney/2024/02/esta-empresa-evitou-r-60-milhoes-em-fraudesbancarias-usando-iapor-voz/. Acesso em: 12 mai. 2024.

G1. Estelionatos no Brasil mais que quadruplicam em cinco anos, e golpes virtuais disparam após pandemia, revela Anuário. São Paulo: **G1**, 2023. 20 jul. 2023. Disponível em: https://g1.globo.com/sp/saopaulo/noticia/2023/07/20/estelionatos-nobrasil-mais-que-triplicam-em-cinco-anos-egolpes-virtuais-disparam-apos-pandemia-revelaanuario.ghtml. Acesso em: 06 mai. 2024.

GARCÍA, L. **Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions.** Jones & Bartlett Learnin, 2017.

(GENEVA) PERMANENT MISSION OF BRAZIL TO THE UNITED NATIONS OFFICE AND OTHER INTERNATIONAL ORGANIZATIONS IN GENEVA. Brazil: **Law alters Penal Code and stiffens penalty against crimes**. 2023 . Disponível em: [https://www.ohchr.org/sites/default/files/documents/hrbodies/ced/cfis/shorttermdisap/submission-state-short-term-ED-CED-WGEID-state-brazil-1-en.pdf . Acesso em: 12 maio 2024.

IAPP. **Evolving threats: The state of personal data protection in Brazil**. 2020. Disponível em: https://iapp.org/resources/article/brazilian-data-protection-law-lgpdenglish-translation/. Acesso em: 12 maio 2024.

Instituto Brasileiro de Geografia e Estatística (IBGE). **Pesquisa Nacional por Amostra de Domicílios Contínua (Pnad Contínua) 2022.** Rio de Janeiro, 2022. Disponível em: https://www.ibge.gov.br/estatisticas/sociais/trabalho/17270-pnadcontinua.html. Acesso em: 10 dez. 2023.

Instituto Brasileiro de Geografia e Estatística (IBGE). **Anuário Estatístico do Brasil 2022**. Rio de Janeiro, 2022. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/periodicos/101/anuario_estatistico_brasil_2022.pdf. Acesso em: 10 dez. 2023.

JOHNSON, M. **International Cooperation in Cybercrime Investigation: A Comparative Analysis**. Springer, 2021.

Lemos, V., Ignaczak, L. **An analysis of the public consequences of cybersecurity incidents in Brazil.** Soc. Netw. Anal. Min. 13, 106 . 2023. Disponível em: https://doi.org/10.1007/s13278023-01113-9. Acesso em: 12 maio 2024.

LEVY, Pierre. A emergência do cyberspace e as mutações culturais. **Revista Nescon**, 2019.

MOORE, T.; CLAYTON, R.; ANDERSON, R. The economics of online crime. **Journal of Economic Perspectives**, v. 23, n. 3, p. 3-20, 2009.

OLIVEIRA, F. G. et al. **Impacto Social da Fraude Cibernética: Um Estudo de Caso no Brasil.** In: Conferência Nacional de Segurança Cibernética, São Paulo, 2021.

OLIVEIRA, C. Digital **Inclusion and Social Equity: Empowering Communities through Technology**. IGI Global, 2018

**PRICE WATERHOUSE COOPERS (PwC Brasil).** Internet no Brasil: tendências e oportunidades para 2023. São Paulo, 2023. Disponível em: https://www.pwc.com.br/pt/estudos/internet-no-brasil-tendencias-e-oportunidadespara2023.html. Acesso em: 10 dez. 2023.

Polícia Federal. Fraudes na Internet. **Polícia Federal.** 2023. Disponível em: https://www.gov.br/pf/pt-br/canais_atendimento/comunicacao-de-crimes. Acesso em: 12 maio 2024.

RUSSELL, S.; NORVIG, P. **Artificial intelligence: a modern approach. Malaysia: Pearson Education Limited**, 2016.

SANTOS, C. D.; LIMA, E. F. **Impacto Econômico da Fraude Cibernética no Brasil. Revista Brasileira de Segurança Digital**, v. 8, n. 1, p. 30-45, 2022.

SANTOS, D. **Cybersecurity Training and Awareness: A Practical Approach for Employees**. Packt Publishin**,** 2021.

Senado Federal. Como a inteligência artificial está impactando a segurança da informação? **Senado Federal.** 2023. 21 mar. 2024. Disponível em: https://legis.senado.leg.br/sdleggetter/documento?dm=9543965&ts=1707413074169&rendition_principal=S&dispositi on=inline. Acesso em: 12 mai. 2024.

SILVA, A. B. et al. Aspectos Jurídicos da Fraude Cibernética no Brasil. **Revista Brasileira de Direito Digital**, v. 15, n. 2, p. 75-90, 2023.

SILVA, A. **Cybercrime and Society: Understanding Online Offending**. Sage Publications, 2019.

SOARES, Eduardo. **Brazil: Punishment for Crimes Committed Electronically or Over Internet** Increased. 2021. Disponível em: https://www.loc.gov/item/globallegal-monitor/2021-0608/brazil-punishment-for-crimes-committed-electronically-orover-internet-increased/. Acesso em: 12 maio 2024.

SOUZA, B. **Digital Literacy: Empowering Citizens in the Digital Age**. Springer, 2020.

WALL, D. S. **Cybercrime: The transformation of crime in the information age**. Cambridge: Polity, 2007.

YAR, Majid. **Cybercrime and Society.** Sage Publications Ltd, 2006.