UNIVERSIDADE ESTADUAL DO PIAUÍ

CAMPUS DRA. JOSEFINA DEMES

CURSO DE GRADUAÇÃO EM CIÊNCIAS DA COMPUTAÇÃO

YGOR FREITAS MEDEIROS DA SILVA

ANALISE DA RELEVÂNCIA DA DESINFORMAÇÃO EM FRAUDES VIRTUAIS: UM ESTUDO COM *DASHBOARD* INTERATIVO

FLORIANO

2024

YGOR FREITAS MEDEIROS DA SILVA

ANALISE DA RELEVÂNCIA DA DESINFORMAÇÃO EM FRAUDES VIRTUAIS: UM ESTUDO COM *DASHBOARD* INTERATIVO

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Ciências da Computação da Universidade Estadual do Piauí, como requisito parcial à obtenção do grau de bacharel em Ciências da Computação.

Orientador: Prof. Me. Filipe Fontinele de Almeida.

FLORIANO

2024

Análise da Relevância da Desinformação em Fraudes Virtuais: Um Estudo com *Dashboard* Interativo

Ygor Freitas Medeiros da Silva[1], **Filipe Fontinele de Almeida**[1]

[1]Universidade Estadual do Piauí (UESPI)

ygorsilva@aluno.uespi.br, filipedealmeida@frn.uespi.br

Abstract. *The advancement of technology and the expansion of social media have intensified the phenomenon of disinformation, facilitating the occurrence of virtual fraud. This study focuses on developing an interactive dashboard to analyze data related to disinformation in cyber fraud in the states of Piauí and Maranhão. The research conducted a bibliographic survey to understand crime patterns associated with disinformation and employed automated data collection from reliable sources between 2012 and 2023. The results obtained with the dashboard highlight the most frequent fraud types and the temporal and regional patterns of disinformation dissemination. This work contributes practical strategies for awareness and prevention, showcasing the role of technology in mitigating cybercrime.*

Keywords*: Disinformation, cyber fraud, interactive dashboard, digital security, social engineering.*

Resumo. *O avanço da tecnologia e a expansão das redes sociais intensificaram o fenômeno da desinformação, facilitando a ocorrência de fraudes virtuais. Com base nisso, este estudo tem como foco o desenvolvimento de um dashboard interativo para analisar dados relacionados à desinformação em fraudes cibernéticas nos estados do Piauí e Maranhão. A pesquisa realizou um levantamento bibliográfico para embasar a compreensão dos padrões de crimes associados à desinformação e utilizou coleta automatizada de dados de fontes confiáveis entre 2012 e 2023. Os resultados obtidos com o dashboard destacam as modalidades mais frequentes de fraude e os padrões temporais e regionais de disseminação da desinformação. O trabalho contribui com estratégias práticas de conscientização e prevenção, mostrando o papel da tecnologia na mitigação de crimes cibernéticos.*

Palavras-chave: *Desinformação, fraudes cibernéticas, dashboard interativo, segurança digital, engenharia social.*

1. Introdução

Nos últimos anos, o uso da internet e das redes sociais cresceu de forma acelerada, proporcionando uma plataforma ideal para o compartilhamento de informações. Contudo, essa facilidade também abriu espaço para a propagação de desinformação, que causa prejuízos em diversos contextos, especialmente em fraudes virtuais. Um exemplo relevante é o aumento de golpes de engenharia social, que utilizam informações enganosas para manipular indivíduos e obter dados sensíveis ou financeiros, configurando-se como uma ameaça crescente à segurança digital.

O impacto da desinformação vai além do âmbito pessoal, afetando também instituições públicas, empresas e a sociedade como um todo. No cenário digital, a rápida disseminação de conteúdos falsos é potencializada por algoritmos das redes sociais, que frequentemente priorizam informações sensacionalistas ou polarizadoras. Esse fenômeno não apenas prejudica usuários por meio de golpes, mas também compromete a confiança nas plataformas digitais e dificulta a implementação de medidas eficazes de segurança. No Brasil, onde a conectividade cresce rapidamente, a identificação e o combate à desinformação tornam-se ainda mais urgentes, exigindo ferramentas tecnológicas robustas que auxiliem na análise de dados e na conscientização da população.

Diante desse contexto, este trabalho propõe o desenvolvimento de um *dashboard* interativo que possibilite a análise e compreensão dos padrões de desinformação associados a crimes cibernéticos, com foco nos estados do Piauí e Maranhão. A abordagem combina coleta automatizada de dados por meio da biblioteca , organização em bases estruturadas e visualizações interativas. Essa ferramenta tem como objetivo não apenas identificar os padrões temporais, regionais e temáticos das fraudes virtuais, mas também subsidiar ações preventivas e conscientização sobre a segurança digital.

A análise proposta neste estudo busca explorar as relações entre desinformação e fraudes cibernéticas, utilizando dados coletados entre 2012 e 2023. Os resultados esperados incluem a identificação de modalidades mais frequentes de crimes, além da elaboração de estratégias baseadas em tecnologia para mitigar esses problemas. Este trabalho busca contribuir para a promoção da segurança digital e para a construção de uma sociedade mais consciente e resiliente frente aos desafios do ambiente virtual.

2. Trabalhos Relacionados

Nesta seção, são apresentados os estudos relacionados ao tema da desinformação e sua conexão com crimes digitais. A análise aborda pesquisas que exploram como a disseminação de informações falsas impacta o ambiente digital. Contribuindo para a ocorrência de direitos cibernéticos e ameaças à segurança *online*.

Oliveira (2023) investigou o impacto das fraudes no setor de turismo e hotelaria no Brasil, com foco no estelionato digital. A pesquisa revelou um aumento significativo dos casos de golpes no setor, com base em dados coletados por questionários e fontes jornalísticas. Como resultado, foi sugerida a necessidade de estratégias de prevenção e melhorias na segurança de sites voltados a esse mercado.

O trabalho de Nunes (2012) destacou o impacto da internet e do ciberespaço na sociedade contemporânea, com ênfase em áreas como comunicação, economia, política e cultura. Foi identificado que o ciberespaço, embora tenha promovido crescimento econômico e eficiência administrativa, introduziu novas vulnerabilidades, como ciberataques mais frequentes e severos. Além disso, foi reforçada a importância de estratégias nacionais de cibersegurança para proteger cidadãos e soberania, alertando sobre o risco da dependência em soluções estrangeiras.

Poiares (2019) analisou a cibersegurança sob a perspectiva da criminologia moderna, abordando os desafios sociais enfrentados no ciberespaço. O estudo salientou a relevância de uma abordagem multidisciplinar, incluindo ações preventivas desde a educação básica até o ensino superior como medida essencial no combate aos crimes cibernéticos.

A contribuição de Lime (2022) trouxe um programa acadêmico focado nas prioridades de segurança no ciberespaço, com destaque para o cenário africano. O estudo ressaltou a importância da colaboração entre setor privado, governos e sociedade civil no enfrentamento de ameaças cibernéticas, como espionagem e sabotagem de infraestruturas críticas. Também foi enfatizada a necessidade de políticas de cibersegurança que respeitassem os direitos humanos.

Serino e Rigo (2024) exploraram a virtualização de sistemas SCADA como estratégia para o aprimoramento da segurança cibernética em setores industriais críticos. Os autores demonstraram que a virtualização possibilitou avaliações contínuas de vulnerabilidades, otimizou a recuperação de dados e aprimorou o controle de incidentes.

Moraes (2016) examinou a evolução histórica e a legislação relacionada a crimes virtuais no Brasil. A análise abrangeu modalidades de delitos, como invasão de dispositivos e estelionato online, com destaque para marcos legais, como a Lei Carolina Dieckmann e o Marco Civil da Internet. Também foi discutida a necessidade de atualizações legislativas para acompanhar a evolução tecnológica.

Zacarias e Freire (2023) investigaram as dificuldades no combate aos crimes cibernéticos, analisando suas formas de ocorrência e as limitações das legislações nacionais e internacionais. Foi ressaltada a urgência de um acompanhamento legislativo mais rigoroso para garantir maior proteção aos usuários.

Cutti (2023) concentrou-se nos desafios jurídicos relacionados ao estelionato virtual, destacando as dificuldades na identificação dos criminosos e na aplicação de punições. O estudo evidenciou os impactos trazidos pelo aumento da conectividade e as implicações ao ordenamento jurídico.

Silveira, Realan e Amaral (2016) investigaram ataques de *phishing* no contexto da engenharia social, explicando como tais práticas exploraram vulnerabilidades dos usuários. Foram sugeridas medidas preventivas, como a ampliação da conscientização sobre segurança digital e a adoção de ferramentas *antiphishing*.

Cardoso (2023) analisou os impactos do estelionato virtual na população idosa, constatando que o aumento do uso da internet durante a pandemia tornou esse grupo mais vulnerável a fraudes. Entre as conclusões, foi proposta a criação de políticas públicas específicas para proteger os idosos contra crimes digitais.

Colli (2009) abordou os desafios enfrentados pelas investigações preliminares de cibercrimes no contexto policial brasileiro, discutindo limites jurídicos e tecnológicos. O trabalho reforçou a importância da interdisciplinaridade entre Direito e Tecnologia como meio de avançar na proteção dos direitos humanos e na eficiência das investigações cibernéticas.

Pauvels, Ramborger e Savgnago (2013) analisaram os cibercrimes de pedofilia e pornografia infantil sob a perspectiva constitucional e penal, destacando os desafios enfrentados no combate a esses delitos. A pesquisa ressaltou a necessidade de normas mais rígidas e medidas efetivas para proteger crianças e adolescentes, propondo soluções baseadas em proporcionalidade e razoabilidade.

Ramalho e Ameida (2024) discutiram a intersecção entre o Código de Processo Penal e a legislação voltada a crimes cibernéticos, com foco na apreensão de correios eletrônicos. O estudo apresentou as implicações legais e os desafios enfrentados pelas autoridades durante investigações digitais, além de apontar lacunas nas regulamentações vigentes.

Guedes, Santos e Aparecido (2023) investigaram a relação entre o uso da tecnologia pelos idosos e sua vulnerabilidade a crimes virtuais. A análise evidenciou que, embora a conectividade tenha trazido benefícios, esse grupo enfrenta dificuldades ao lidar com ameaças digitais. Como solução, foram sugeridas estratégias de conscientização e adaptações tecnológicas às necessidades dos usuários mais velhos.

3. Materiais e Métodos

Esta seção apresenta os principais componentes técnicos desenvolvidos neste trabalho: um *script* automatizado para a coleta de *URLs* notícias relacionadas a fraudes cibernéticas e desinformação, e um *dashboard* interativo para a visualização e análise dos dados coletados. Ambos foram desenvolvidos utilizando a linguagem de programação *Python*, escolhida por sua versatilidade, simplicidade e ampla gama de bibliotecas que suportam tarefas de automação, manipulação de dados e visualização. A mesma é amplamente reconhecida por sua aplicabilidade em projetos de ciência de dados e inteligência artificial, características que foram cruciais para atender aos objetivos do estudo. A seguir, são detalhadas a arquitetura, funcionalidades e objetivos de cada sistema.

3.1. *Script* de Captura de *URLs*

O *script* de coleta de *URLs* foi desenvolvido com a biblioteca *Selenium*, especializada em automação de navegadores. Essa ferramenta permite navegar em páginas web de forma programada e extrair informações estruturadas de maneira eficiente. O *script* foi projetado para buscar notícias relacionadas a fraudes cibernéticas e desinformação em fontes confiáveis, filtrando os dados de acordo com as regiões de interesse (estados do Piauí e Maranhão).

Arquitetura: Nesta subseção, será descrita a organização estrutural do sistema, destacando como os componentes interagem para viabilizar a coleta de dados de forma eficiente e segura.

1. **Configuração do *WebDriver*:** O *Selenium* é configurado com o *WebDriver* do navegador *Firefox*, operando em modo "*headless*", o que reduz o consumo de recursos e permite a execução sem interface gráfica.
2. **Busca de Dados:** Combina termos de busca como:" fraude bancária online "ou " *phishing* "com localizações específicas, como " Piauí "e " Maranhão ", para realizar buscas direcionadas no *Google*.
3. **Coleta de Informações:** Identifica elementos contendo *URLs* e metadados das páginas utilizando seletores *CSS* e implementa estratégias para capturar datas de publicação, analisando meta *tags* e elementos visíveis como $< time >$ e $< span >$.
4. **Armazenamento Estruturado:** Os dados coletados são salvos em um arquivo *CSV*, com as seguintes colunas: *Url*, Estado, modalidade do crime, data de coleta, data de publicação, período de busca.

Funcionalidades: Aqui serão apresentadas as principais capacidades do script, incluindo recursos que garantem a robustez e a confiabilidade durante o processo de coleta de informações.

1. **Resiliência a Erros:** Implementa tratamento de exceções para lidar com problemas como *CAPTCHA* ou elementos ausentes nas páginas.

2. **Padronização de Datas:** Realiza conversões automáticas para o formato dd/mm/aaaa, garantindo uniformidade nos dados armazenados.
3. **Evita Duplicidade:** Verifica *URLs* previamente coletadas no *CSV*, prevenindo redundâncias.

3.2. *Dashboard* Interativo

O *dashboard* interativo foi desenvolvido utilizando as bibliotecas *Dash* e *Plotly*, amplamente reconhecidas por oferecerem soluções robustas para a criação de interfaces web interativas e gráficos de alta qualidade. Ele serve como uma ferramenta analítica que permite aos usuários explorar os dados coletados de forma intuitiva e visualmente atraente.

Arquitetura:Serão detalhadas as técnicas e ferramentas utilizadas na implementação do *script*, abordando aspectos específicos da configuração e execução.

1. **Interface de Navegação:** Inclui uma *navbar* e uma *sidebar*, criadas com componentes do *Dash Bootstrap*, que organizam os gráficos por categorias, facilitando a navegação.
2. **Uso de Cache:** Implementa a biblioteca *Flask-Caching* para reduzir o tempo de resposta ao armazenar dados processados, otimizando a experiência do usuário.
3. **Componentes Visuais:** Gráficos interativos que fornecem *insights* detalhados sobre os dados, incluindo: Gráficos de Barras com as *URLs* mais mencionadas em publicações; mapas Coropléticos com a distribuição geográfica das fraudes; Gráficos de Área com padrões temporais das modalidades de crimes; Séries Temporais com ´´ *Seasonal Autoregressive Integrated Moving Average - SARIMA* ” em português ´´ Média Móvel Integrada Autorregressiva Sazonal ”, é uma técnica utilizada para previsão de tendências futuras.
4. **Previsões Temporais com Inteligência Artificial:** Para identificar padrões temporais e realizar previsões sobre o volume de publicações, foi implementado o modelo *SARIMA* . A escolha desse modelo se deu devido à sua capacidade de capturar componentes sazonais e não sazonais em séries temporais, sendo amplamente utilizado em cenários de dados que apresentam repetição periódica e tendências de longo prazo.

   Funcionamento do *SARIMA*: O modelo combina os seguintes componentes:

- **AR (*Autoregressive*):** Utiliza valores passados da série para prever os próximos.
- **I (*Integrated*)**: Aplica diferenciação nos dados para torná-los estacionários.
- MA (***Moving Average***): Ajusta o modelo com base nos erros das previsões anteriores.
- **Sazonalidade (S):** Incorpora padrões sazonais nos dados, como ciclos semanais ou mensais.

Implementação Técnica: Serão explorados os aspectos específicos da criação do *dashboard*, como a utilização de modelos estatísticos e integração de bibliotecas para visualização de dados.

1. **Pré-processamento:** Conversão das datas para o formato padrão dd/mm/aaaa e agrupamento dos dados em intervalos temporais (semanas ou meses).
2. **Análise de Estacionariedade:** Testes como ADF (*Augmented Dickey-Fuller*) foram aplicados para garantir que a série temporal fosse estacionária.
3. **Treinamento do Modelo:** Ajuste dos parâmetros sazonais e não sazonais (p, d, q, P, D, Q, S) utilizando métodos de busca automatizada, como *Grid Search.*

4. **Validação**: O modelo foi validado utilizando uma amostra dos dados históricos, e métricas como RMSE (*Root Mean Square Error*) foram aplicadas para avaliar sua precisão.
5. **Visualização**: As previsões geradas foram integradas ao *dashboard* em forma de gráficos interativos, permitindo ao usuário visualizar tendências futuras e picos de atividade.

Funcionalidades: Esta subseção detalhará os recursos disponibilizados pelo *dashboard*, incluindo a interatividade e as opções de personalização para os usuários.

1. **Exploração Dinâmica:** Permite que o usuário filtre informações por região, modalidade ou período de tempo.
2. **Previsões Avançadas:** Utiliza o modelo *SARIMA* para identificar sazonalidades e prever o volume de publicações nos próximos meses.
3. **Foco Regional:** Destaca as diferenças entre estados, ajudando na identificação de regiões mais vulneráveis a determinados tipos de crimes.
4. **Acessibilidade e Personalização:** Oferece *layouts* responsivos para diferentes dispositivos e permite personalização de parâmetros de visualização.

Diagrama de Sequência: A interação entre o usuário, o *script* de captura de *URLs*, o arquivo *CSV* e o *dashboard* interativo pode ser representada no seguinte diagrama de sequência presente na Figura 1:

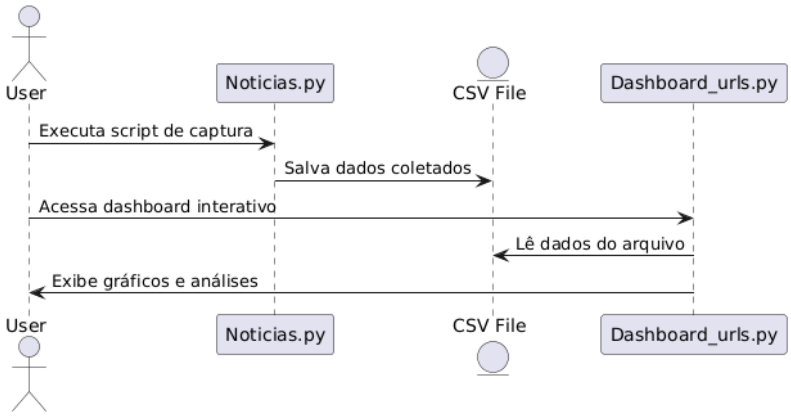

Figura 1. Diagrama de Sequencia

1. **Execução do *Script*:** O usuário inicia a execução do *script* de captura, fornecendo termos de busca e especificações regionais. Então, o mesmo coleta dados relevantes da internet.
2. **Armazenamento dos Dados:** As informações coletadas são processadas e salvas no arquivo *CSV* em formato padronizado, facilitando sua reutilização posterior.
3. **Acesso ao *Dashboard*:** O usuário acessa o *dashboard* interativo, que lê os dados armazenados no *CSV* para gerar visualizações.
4. **Exploração Visual:** O *dashboard* processa os dados e exibe gráficos interativos, permitindo ao usuário explorar padrões e tendências de maneira dinâmica. Este fluxo demonstra a integração eficiente entre os dois sistemas, permitindo a automação na coleta e análise de informações sobre desinformação e fraudes cibernéticas. Além disso, ele destaca o uso estratégico de *Python* para lidar com grandes volumes de dados e oferecer *insights* significativos.

4. Resultados

Nesta seção, apresentam-se os resultados obtidos a partir da análise dos dados, organizados em gráficos que evidenciam padrões temporais, geográficos e temáticos relacionados à desinformação e fraudes virtuais. Os gráficos foram desenvolvidos no *dashboard* interativo, permitindo visualizar as relações entre as variáveis analisadas. A seguir, explora-se o que cada gráfico revela sobre os dados coletados.

Um dos primeiros aspectos analisados foi a diferença em dias entre a coleta e a publicação das notícias, conforme mostrado na Figura 2. Esse intervalo é um fator crítico para avaliar a eficiência na disseminação de informações, com períodos de atraso significativo apontando gargalos em processos editoriais ou priorização inadequada de conteúdo.

Essa defasagem traz implicações práticas, pois atrasa o conhecimento público sobre crimes cibernéticos, reduzindo a capacidade de resposta da sociedade e dificultando a conscientização. Notou-se, por exemplo, que momentos de maior defasagem frequentemente precedem eventos sazonais, como feriados, quando a vulnerabilidade a fraudes é maior.

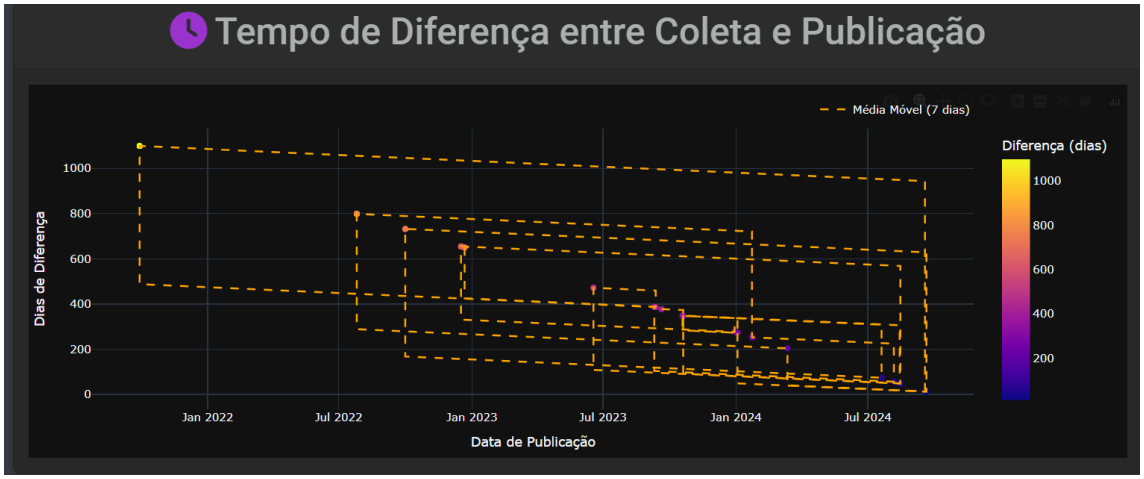

Figura 2. Diferença entre Coleta e Publicação

As modalidades de fraudes mais recorrentes foram organizadas em categorias, destacando crimes como *phishing*, roubo de identidade e falsificação de documentos. Na Figura 3, essas categorias foram apresentadas em um gráfico de barras empilhadas que permite identificar padrões regionais e temáticos.

Essa análise revelou que o *phishing* é amplamente utilizado em campanhas massivas que exploram a falta de informação imediata da população, conectando-se diretamente à defasagem temporal evidenciada anteriormente. Além disso, crimes específicos, como roubo de identidade, mostram concentrações em regiões com menor acesso à educação digital, evidenciando a necessidade de intervenções específicas.

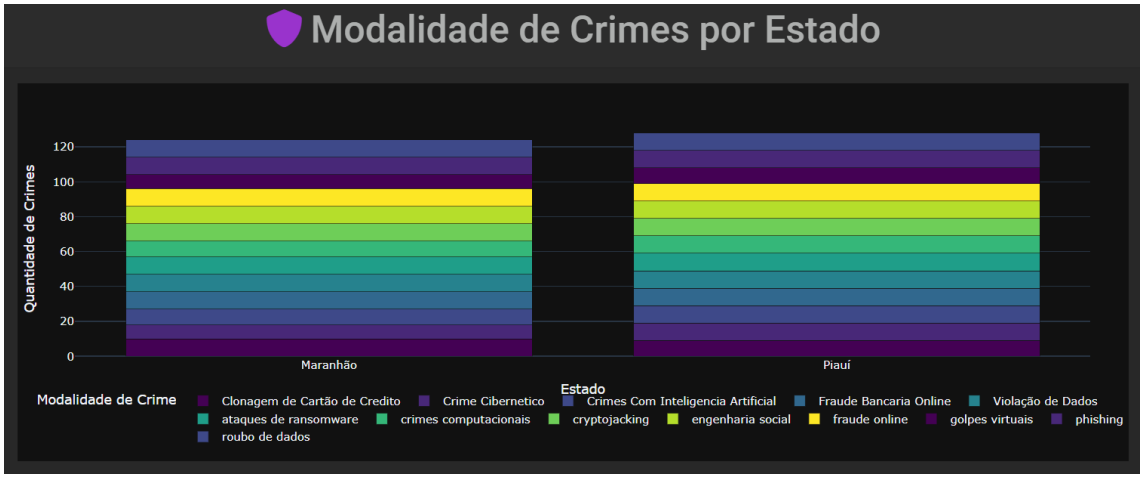

Figura 3. Frequência de Modalidades de Fraudes

Ao analisar a distribuição geográfica dos crimes, foi possível identificar padrões claros nos estados do Piauí e Maranhão, que aparecem como os mais impactados. A visualização na Figura 4, por meio de um mapa coroplético, sugere que a conectividade crescente nessas regiões, aliada à ausência de estratégias educativas, potencializa a vulnerabilidade local.

Esses dados, quando cruzados com as modalidades de fraudes, indicam que as regiões mais afetadas também apresentam maior diversidade de crimes. Isso reforça a necessidade de políticas públicas adaptadas às particularidades regionais para mitigar os riscos.

Figura 4. Distribuição Geográfica das Fraudes

Os padrões temporais das notícias sobre fraudes cibernéticas mostram picos evidentes em períodos críticos, como datas promocionais e feriados. A análise, ilustrada na Figura 5, demonstra como esses momentos de alta atividade digital são explorados pelos criminosos.

Os dados reforçam a sazonalidade dos crimes, com aumento expressivo em modalidades como fraudes em compras online durante o final de ano. Ao integrar esses resultados com a distribuição geográfica, é possível prever quais regiões são mais suscetíveis em determinados períodos, permitindo ações preventivas direcionadas.

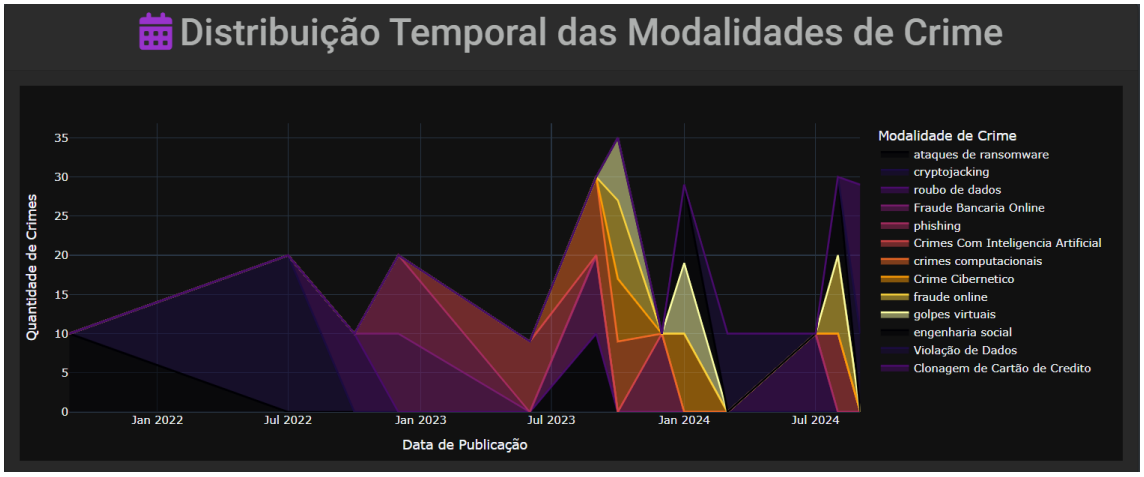

Figura 5. Relação entre Frequência de Notícias e Períodos Temporais

A correlação entre diferentes categorias de notícias e sua manipulação para disseminação de desinformação foi explorada com profundidade. A Figura 6 destaca que conteúdos relacionados à segurança financeira são os mais frequentemente utilizados para atrair vítimas.

Essa análise fornece *insights* sobre as estratégias de engenharia social empregadas pelos criminosos, que ajustam suas táticas com base no momento e na localização. Campanhas educativas direcionadas a essas temáticas podem reduzir significativamente os impactos dessas práticas.

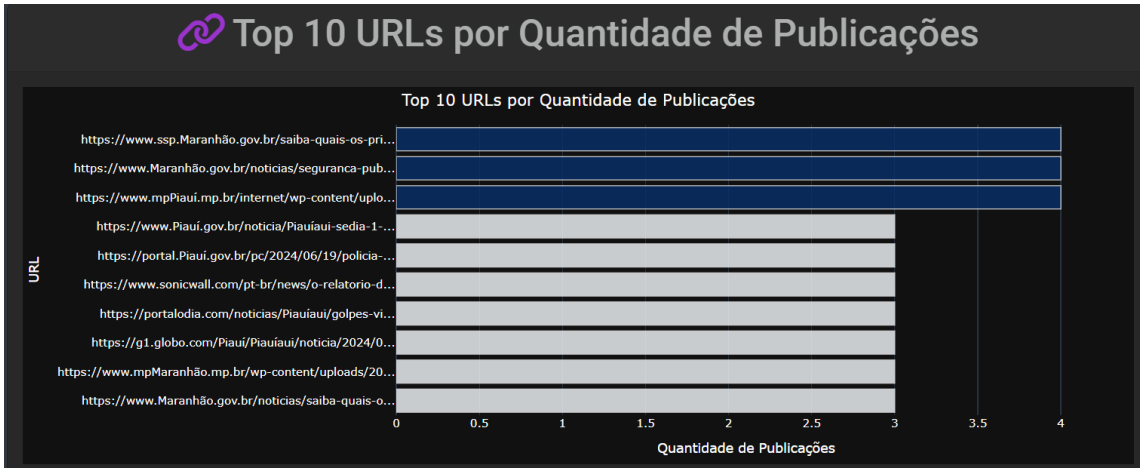

Figura 6. Correlação entre Categorias de Notícias e Desinformação

Para compreender as tendências futuras, foram geradas previsões utilizando o modelo *SARIMA*, que considera padrões sazonais e não sazonais. A Figura 7 apresenta essas projeções, indicando picos futuros de atividade criminosa, especialmente em datas críticas já identificadas, como feriados.

Além disso, o *SARIMA* mostrou-se eficiente ao modelar flutuações recorrentes e sazonais, resultando em previsões mais ajustadas à realidade observada. A análise temporal das fraudes cibernéticas possibilita uma compreensão profunda dos comportamentos criminosos, auxiliando no planejamento estratégico de combate e na alocação de recursos para os períodos mais vulneráveis.

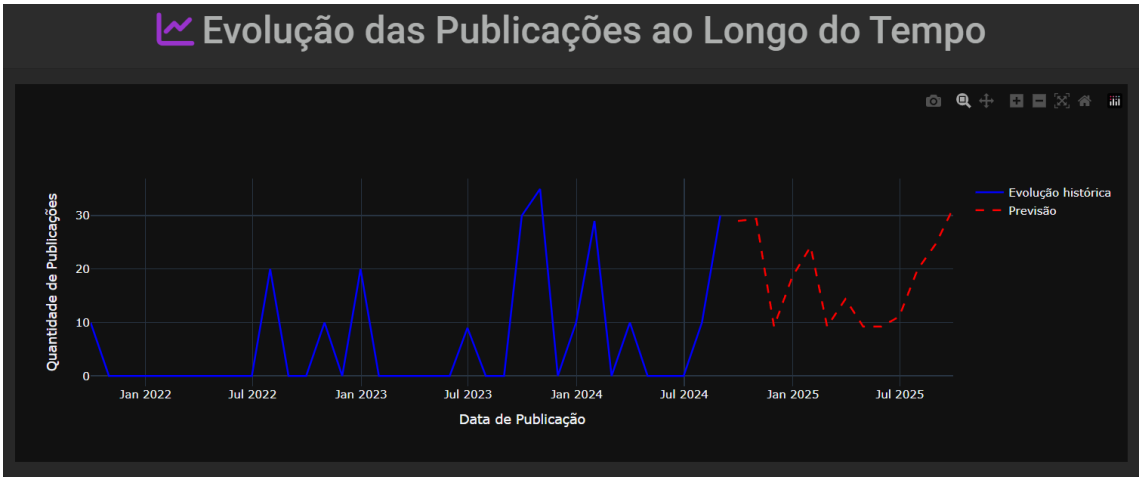

Figura 7. Evolução das Publicações ao Longo do Tempo

5. Conclusão

Este estudo destacou a relevância da desinformação como um dos principais vetores para a ocorrência de fraudes virtuais nos estados do Piauí e Maranhão. Por meio do uso de um *dashboard* interativo, foi possível identificar padrões temporais, regionais e temáticos que caracterizam a disseminação de informações falsas e sua relação com crimes cibernéticos. Essa abordagem não apenas demonstrou as modalidades de crimes mais frequentes, como também evidenciou a necessidade de estratégias preventivas fundamentadas na tecnologia e na educação digital.

Os resultados obtidos enfatizam que o combate às fraudes virtuais requer uma colaboração coordenada entre sociedade, setor privado e poder público. Este trabalho apresentou uma contribuição prática nesse contexto ao desenvolver uma ferramenta analítica capaz de promover a conscientização e subsidiar ações preventivas. Além disso, reforça-se a importância de políticas públicas que priorizem o acesso à educação digital, especialmente em regiões vulneráveis.

A integração dos dados coletados com previsões baseadas em modelos estatísticos, como o *SARIMA*, demonstrou ser uma estratégia eficaz para antecipar picos de atividade criminosa e apoiar a formulação de políticas públicas e empresariais. Essa abordagem, aliada à análise regional, permite um planejamento mais assertivo e adaptado às necessidades locais.

Futuras aplicações podem ampliar o escopo deste estudo, incluindo a expansão do *dashboard* para análise de dados em outras regiões do Brasil. Essa iniciativa possibilitará um entendimento mais abrangente dos padrões de desinformação e fraudes, promovendo soluções adaptadas às especificidades de cada contexto. Além disso, a inclusão de módulos educativos no *dashboard* pode potencializar sua eficácia, alcançando instituições de ensino, empresas e comunidades, e promovendo uma cultura de segurança digital.

Por fim, acredita-se que, ao expandir o uso de tecnologias de análise de dados e fortalecer a conscientização sobre os impactos da desinformação, será possível construir uma sociedade mais resiliente aos riscos do ambiente digital e mais preparada para enfrentar os desafios impostos pelo crescimento das fraudes virtuais.

Referências

CARDOSO, M. A. F. O estelionato virtual praticado contra o idoso e os reflexos jurídico-penais. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, v. 9, n. 5, p. 3385–3398, 2023. 3

COLLI. *Cibercrimes: limites e perspectivas para a investigação preliminar policial brasileira de crimes cibernéticos*. 2009. 3

CUTTI, M. C. *Crimes virtuais no ordenamento jurídico e as suas dificuldades da identificação do agente*. 2023. 3

GUEDES; SANTOS, M.; APARECIDO, R. Crimes e golpes virtuais: desafios enfrentados pelos idosos na era tecnológica. *OBSERVATÓRIO DE LA ECONOMÍA LATINOAMERICANA*, v. 21, n. 9, p. 14026–14040, 2023. 4

LIME, M. L. Prioridades de segurança do ciberespaço para os atores de segurança nacional de África: Programa acadêmico virtual. *Africa Center for Strategic Studies*, 2022. 3

MORAES, I. F. *Crimes virtuais*. 2016. 3

NUNES, P. F. V. A definição de uma estratégia nacional de cibersegurança. *Nação e Defesa*, Instituto da Defesa Nacional, 2012. 2

OLIVEIRA, A. Golpes no turismo e em hotelaria no brasil: Prevenção e conscientização. *Anais da Feira de Iniciação Científica e Extensão (FICE) Campus Camboriú*, 2023. 2

PAUVELS, C. M.; RAMBORGER, H.; SAVGNAGO, J. U. Cibercrimes sob o enfoque constitucional penal: Aspectos controvertidos da pornografia infantil e pedofilia. *IN: XV Seminário Internacional de Educação no Mercosul, Cruz Alta: Universidade de Cruz Alta*, 2013. 3

POIARES, N. C. L. d. B. A cibersegurança à luz da criminologia moderna. *Cyberlaw by CIJIC*, Faculdade de Direito da Universidade de Lisboa, Centro de Investigação, v. 7, 2019. 2

RAMALHO, J.; AMEIDA, F. Apreensão de correio eletrónico: Os regimes do código de processo penal e da lei do cibercrime. *Revista Jurídica Portucalense*, p. 261–276, 2024. 3

SERINO, D. G.; RIGO, A. Virtualização de sistemas SCADA como forma de atender a controles de segurança cibernética. In: *20th CONTECSI - International Conference on Information Systems and Technology Management Virtual*. [S.l.: s.n.], 2024. 3

SILVEIRA, L. A.; REALAN, M.; AMARAL, É. Engenharia social: Uma análise sobre o ataque de phishing. *Anais SULCOMP*, v. 8, 2016. 3

ZACARIAS, F.; FREIRE, L. Z. Crimes virtuais: análise das dificuldades e limitações ao combate. *Jures*, v. 16, n. 29, p. 29–61, 2023. 3