UNIVERSIDADE DE BRASÍLIA
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas Departamento de Administração
MBA em Gestão e Governança de Segurança Pública

Fábio Henrique de Souza

Ivana Peres de Melo

Leobino Pereira da Silva

PRODUTO TÉCNICO-TECNOLÓGICO:

Software (*chatbot*)

INA – INTELIGÊNCIA NACIONAL DE ATENDIMENTO

Brasília, DF

2025

UNIVERSIDADE DE BRASÍLIA
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas Departamento de Administração
MBA em Gestão e Governança de Segurança Pública

Fábio Henrique de Souza

Ivana Peres de Melo

Leobino Pereira da Silva

PRODUTO TÉCNICO-TECNOLÓGICO:

Software (*CHATBOT*)

INA – INTELIGÊNCIA NACIONAL DE ATENDIMENTO

Trabalho de Conclusão de Curso (TCC) sob o formato de Produto Técnico-Tecnológico (PTT) apresentado como requisito para à obtenção do grau de especialista no MBA em Gestão e Governança em Segurança Públicade Pessoas, da Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas da Universidade de Brasília.

Orientadora: Profª. Dra. Marina Figueiredo Moreira

BANCA EXAMINADORA

_____

Profª. Dra. Marina Figueiredo Moreira – Orientadora

_____

Dr. Rodrigo de Souza Carvalho

_____

Dra. Eloisa Gonçalves da Silva Torlig

UNIVERSIDADE DE BRASÍLIA
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas Departamento de Administração
MBA em Gestão e Governança de Segurança Pública

Dedicamos este trabalho às nossas famílias, que sempre nos apoiaram incondicionalmente, oferecendo incentivo em cada etapa dessa jornada.

Aos professores, por todo o conhecimento compartilhado, pela orientação e incentivo ao longo desta jornada.

AGRADECIMENTOS

Primeiramente, agradecemos a Deus por nos conceder força e sabedoria.

À nossa orientadora, Profa. Dra. Marina, expressamos nossa profunda gratidão por sua dedicação, paciência e valiosas orientações, que foram fundamentais para a realização deste trabalho. Seu compromisso e conhecimento foram essenciais para nosso crescimento acadêmico e profissional.

Aos professores por compartilharem seus conhecimentos e contribuírem para nossa formação.

UNIVERSIDADE DE BRASÍLIA
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas
Departamento de Administração
MBA em Gestão e Governança de Segurança Pública

RESUMO

O Brasil enfrenta um aumento significativo nos crimes virtuais, principalmente nas chamadas fraudes eletrônicas, conhecidas popularmente como “golpes”, tipificadas no Código Penal no Artigo 171, §2º-A, CP. Este trabalho propõe a criação de um Produto Técnico-Tecnológico, um software, que possa efetuar, de forma simples e prática, os registros que atualmente sobrecarregam todo o efetivo da Polícia Civil, instituição legalmente responsável por investigar tais crimes. Trata-se de um chatbot, a ser disponibilizado via aplicativo de mensagens, como o WhatsApp (e outros), que coletará dados fundamentais para a posterior investigação. Com esse produto, espera-se que seja possível reduzir subnotificações de crimes de fraudes eletrônicas geradas pela alta demanda nas delegacias e reduzido efetivo. Bem como padronizar a coleta de dados essenciais para o combate a esse tipo de crime e, também, instituir ações preventivas.

Palavras-Chave: Crimes virtuais; Fraude eletrônica; Estelionato; Chatbot; Inteligência Artificial; Registro de ocorrências; Investigação criminal; Prevenção ao crime.

UNIVERSIDADE DE BRASÍLIA
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas
Departamento de Administração
MBA em Gestão e Governança de Segurança Pública

ABSTRACT

Brazil is experiencing a significant rise in cybercrimes, particularly in so-called electronic frauds, commonly known as "scams," which are classified under Article 171, §2º-A of the Penal Code. This study proposes the development of a Technical-Technological Product, a software solution designed to streamline the registration process for such crimes, which currently overwhelms the entire workforce of the Civil Police the institution legally responsible for investigating these offenses.

The proposed software is a chatbot that will be made available through messaging applications such as WhatsApp (among others) to collect essential data for subsequent investigations. This product aims to reduce the underreporting of incidents caused by long queues at police stations, enhance the operational capacity of the current police force, standardize the collection of critical data for combating this type of crime, and implement preventive measures.

Keywords: Cybercrimes;Electronic fraud; Scam; Chatbot; Artificial Intelligence; Incident reporting; Criminal investigation; Crime prevention.

UNIVERSIDADE DE BRASÍLIA
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas
Departamento de Administração
MBA em Gestão e Governança de Segurança Pública

SUMÁRIO

INTRODUÇÃO

Este trabalho aborda o aumento dos crimes virtuais no Brasil. Os números do Anuário Brasileiro de Segurança Pública (2024) demonstram que o crime de estelionato tem crescido ano após ano no país. Em 2023, foram registrados quase 2 milhões de casos de estelionato, representando um aumento de 8,2% em relação ao ano anterior. Entre esses crimes, destaca-se a modalidade de fraude eletrônica, ou seja, estelionato cometido por meio de dispositivos eletrônicos. Observa-se que muitas organizações criminosas têm alterado seus *modus operandi*, migrando para crimes virtuais e investindo fortemente em tecnologia para praticar suas ações de forma digital (Anuário Brasileiro de Segurança Pública, 2024). Neste trabalho, o foco está exclusivamente no crime de estelionato, com ênfase na modalidade eletrônica.

Com esse aumento, as delegacias ficam saturadas de registros de ocorrências, e o efetivo se dedica apenas ao atendimento primário do registro, não tendo efetivo suficiente para analisar caso a caso, criar padrões criminais e promover uma investigação eficaz que consiga responsabilizar os culpados e ressarcir as vítimas, bem como inibir esse tipo de crime.

Vale destacar que em algumas situações a dificuldade em se registrar a ocorrência, ou até mesmo o constrangimento que a vítima sente ao admitir que caiu em um golpe, faz com que vítimas sequer registrem o fato, gerando também uma subnotificação considerável.

Diante o exposto, o ambiente gerado torna-se propício para o aumento da criminalidade na modalidade eletrônica, visto que nesse tipo de crime os autores ficam menos expostos a riscos físicos, têm a capacidade de aplicar golpes em um volume maior e possuem uma maior probabilidade de permanecerem impunes.

Os dados indicam um aumento expressivo nos casos de estelionato entre 2018 e 2020, com um crescimento de aproximadamente 125% nesse período, seguido por uma estabilização em patamares elevados até 2023. Em contraste, o efetivo das polícias civis apresentou uma redução entre 2018 e 2020 e, desde então, manteve-se relativamente estável em um nível inferior ao inicial (Anuário Brasileiro de Segurança Pública, 2024). Esse descompasso entre a crescente demanda por investigação e a

redução da força de trabalho sugere a necessidade de investimentos estratégicos, tanto na recomposição e ampliação do efetivo policial quanto no aprimoramento de tecnologias que possam otimizar a investigação e o combate aos crimes de estelionato. Dada a indisponibilidade de aumento orçamentário, surge a necessidade de optar por soluções de baixo custo para reduzir o déficit entre a demanda crescente por atendimentos e a capacidade operacional das Polícias. Entretanto, este trabalho visa propor uma solução viável e de baixo custo no auxílio ao combate ao crime, em especial o crime de fraude eletrônica, visando um atendimento via chatbot, onde a vítima consegue ser atendida imediatamente, de forma eficaz, sem se sentir constrangida. Adicionalmente, geram-se dados indispensáveis para a investigação e o efetivo poderá se dedicar as investigações, visto que os registros serão feitos de forma virtual, disponibilizando mais tempo aos policiais para sua atividade fim, que é a investigativa. Trata-se, portanto, de uma proposta para uso de tecnologia como recurso para redução

O produto técnico-tecnológico proposto é um chatbot, um programa de computador projetado para simular uma conversa com usuários humanos, utilizando técnicas de processamento de linguagem natural e inteligência artificial para fornecer respostas automáticas a consultas de maneira eficiente e em tempo real (Caldarini; Jaf; McGarry, 2022). O sistema denominado INA (Inteligência Nacional de Atendimento) engloba a ideia de usar ferramentas tecnológicas e estratégias inovadoras para oferecer um serviço de atendimento nacional, simplificando o registro de ocorrências de maneira virtual. Atualmente, alguns estados já oferecem o registro de ocorrências de forma virtual, por meio de sites, mas esses serviços são baseados em formulários que apresentam dificuldades no preenchimento, complexidade de acesso em dispositivos móveis e exigem que o histórico seja escrito manualmente. Isso dificulta o processo para parte da população que não possui conhecimento tecnológico básico ou habilidades de escrita. Este relatório, portanto, apresenta o estudo técnico que embasa a criação do INA, seguindo as recomendações internacionais e as melhores práticas para sua concepção e implementação.

A proposta é que o chatbot INA possa ser feito pelo celular, via a aplicativo de mensagem, onde o áudio explicativo da vítima se transforme em texto e os campos

possam ser preenchidos de maneira interativa e eficiente. Esse mesmo chatbot, acessível a qualquer celular, também poderá ser desenvolvido em totens, nas respectivas delegacias de atendimento ao público, visando assim, atender parte da população que não tem acesso à tecnologia, celular, internet, dentre outros.

Nesse contexto, este estudo busca propor uma solução tecnológica baseada em Inteligência Artificial considerando o *benchmarking* internacional para otimizar o registro de ocorrências de crimes cibernéticos, em especial o estelionato por fraude eletrônica, contribuindo para a eficiência das investigações e a redistribuição de recursos humanos na Polícia Civil. Além de:

- Reunir o *bechmarking* teórico internacional sobre boas práticas para a proposição de Chatbots para atendimento a cidadãos;
- Prototipar, com telas projetadas, o atendimento ao cidadão a partir do INA para as principais ocorrências policiais;
- Descrever as potencialidades futuras, em termos de predição de crimes, para composição de uma base de dados a ser gerada a partir das variáveis-chave coletadas com os atendimentos ao INA.

JUSTIFICATIVA

A partir da implementação do INA, espera-se que seja possível reduzir subnotificações de crimes de fraudes eletrônicas geradas pela alta demanda nas delegacias e reduzido efetivo. O chatbot INA tem como objetivo padronizar e otimizar a coleta de informações relevantes para o registro de estelionatos eletrônicos. Algumas variáveis fundamentais que poderão ser coletadas incluem:

a) Dados da Vítima:

- Nome completo
- CPF
- Endereço
- Contato (telefone e e-mail)

- Faixa etária e perfil socioeconômico

b) Dados do Crime:

- Tipo de fraude eletrônica (phishing, golpe do boleto etc.)
- Data e horário do ocorrido
- Valor financeiro envolvido
- Método utilizado pelo criminoso (mensagens fraudulentas, links maliciosos, sites falsos etc.)

c) Dados do Criminoso:

- Nome ou pseudônimo usado
- Número de telefone, e-mail ou redes sociais utilizadas
- Conta bancária de destino
- Domínio e IP associado

d) Comportamento da Vítima e Reações ao Golpe:

- Como a vítima foi abordada
- Tempo de resposta até perceber o golpe
- Ações tomadas após o golpe (tentativa de contato com o criminoso, denúncia ao banco etc.)

e) Dados Complementares para Investigação:

- Evidências fornecidas pela vítima (prints, áudios, mensagens trocadas)
- Relatos sobre comportamento suspeito prévio ao golpe
- Grau de recorrência do golpe na região

1. PANORAMA DO ESTELIONATO ELETRÔNICO

Os avanços tecnológicos e a crescente digitalização conectaram o mundo de maneira sem precedentes, mas também abriram caminho para o aumento exponencial dos crimes cibernéticos. As organizações contemporâneas estão amplamente direcionadas para o uso de tecnologias emergentes, de modo que criminosos aproveitam as fragilidades em sistemas, redes e infraestruturas online, causando impactos econômicos e sociais significativos em governos, empresas e indivíduos ao redor do mundo. A ameaça inclui práticas como *phishing, ransomware* e vazamentos de dados, além do surgimento constante de novas modalidades de cibercrimes, que são cada vez mais sofisticadas, organizadas e adaptadas ao uso de tecnologias emergentes (Baset, 2021; INTERPOL, 2025).

A transnacionalidade dos crimes cibernéticos – com criminosos, vítimas e infraestruturas técnicas frequentemente distribuídos por várias jurisdições – apresenta desafios significativos para investigações e processos judiciais. O Brasil ocupa a segunda posição no ranking global de ataques cibernéticos, ficando atrás apenas dos Estados Unidos, segundo o *Panorama de Ameaças para a América Latina 2024*. No período de 12 meses, foram registradas mais de 700 milhões de tentativas de ataques, o que equivale a uma média de 1.379 por minuto (Agência Senado, 2024).

Diante dessa realidade, o Brasil tem aprimorado seu arcabouço jurídico para enfrentar os desafios dos crimes digitais. A Lei nº 12.737/2012, conhecida como *Lei Carolina Dieckmann*, tipificou a invasão de dispositivos informáticos e estabeleceu agravantes para casos envolvendo divulgação de dados sigilosos ou prejuízos à administração pública. Em complemento, a Lei nº 14.155/2021 aumentou as penas para crimes como invasão de dispositivos, furto e estelionato eletrônico, considerando agravantes específicos, como o uso de servidores no exterior ou a vitimização de pessoas idosas e vulneráveis. Essas medidas evidenciam o avanço legislativo na tentativa de mitigar os impactos dos crimes cibernéticos e garantir maior proteção aos usuários (Brasil, 2012; Brasil, 2021).

Entretanto, como destaca a pesquisa de Siqueira, Contin, Barufi e Lehfeld (2021), os consumidores ainda permanecem vulneráveis devido à falta de

regulamentações efetivas e ao baixo nível de conhecimento técnico para proteger seus dados. Essa vulnerabilidade é agravada pela sofisticação das práticas criminosas e pela ausência de estratégias educativas e tecnológicas integradas. A *Lei Geral de Proteção de Dados* (LGPD), embora represente um marco importante, não acompanha totalmente a velocidade das transformações tecnológicas, o que evidencia a necessidade de um alinhamento mais robusto entre legislação, governança e educação digital.

Em linha com essa análise, Nolasco e Silva (2022) ressaltam que a chamada "sociedade da informação" trouxe benefícios como a globalização e a valorização dos dados digitais, mas também desafios complexos, como a violação de direitos fundamentais, incluindo a privacidade. A desmaterialização dos bens e a globalização das infraestruturas digitais dificultam a rastreabilidade e a responsabilização de criminosos. Nesse contexto, o fortalecimento da cibersegurança, aliado ao desenvolvimento de tecnologias como a Inteligência Artificial, emerge como essencial. Ainda assim, sua eficácia depende de marcos regulatórios sólidos que garantam tanto a proteção de dados quanto a segurança jurídica, promovendo avanços tecnológicos responsáveis e alinhados às necessidades sociais.

Nos últimos anos, o Brasil tem enfrentado um aumento significativo nos casos de estelionato, especialmente em fraudes eletrônicas. Dados do Observatório Nacional de Segurança Pública mostram que, entre 2018 e 2024, os casos de estelionato cresceram aproximadamente 360%, passando de 426.799 registros em 2018 para 870.320 em 2023. Esse crescimento exponencial é reflexo de uma mudança no perfil da criminalidade, que migrou de crimes tradicionais, como furtos e roubos, para crimes eletrônicos, mais difíceis de rastrear e punir.

Figura 1 – Infográfico 2024

Fonte: Anuário Brasileiro de Segurança Pública, 2024.

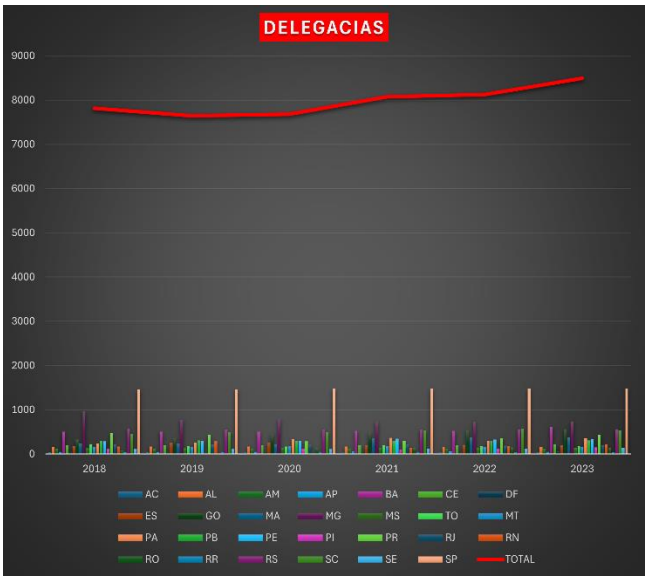
Antes de 2018, a categorização de crimes contra o patrimônio não destacava o estelionato, sendo o foco voltado para furtos e roubos de veículos, estabelecimentos comerciais e residências, dentre outros. No entanto, com o avanço das tecnologias de rastreamento, como leitura de placas e rastreio de dispositivos móveis, houve uma redução nesses crimes. Essa mudança forçou as organizações criminosas a adaptarem seus métodos, migrando para o ambiente digital, onde a anonimidade e a abrangência nacional oferecem maior segurança para os criminosos e mais desafios para as forças de segurança. Conforme demonstrado em mapa abaixo.

Figura 2 – Evolução dos Roubos e Estelionatos no Brasil, 2018-2023

Fonte: Anuário Brasileiro de Segurança Pública, 2024.

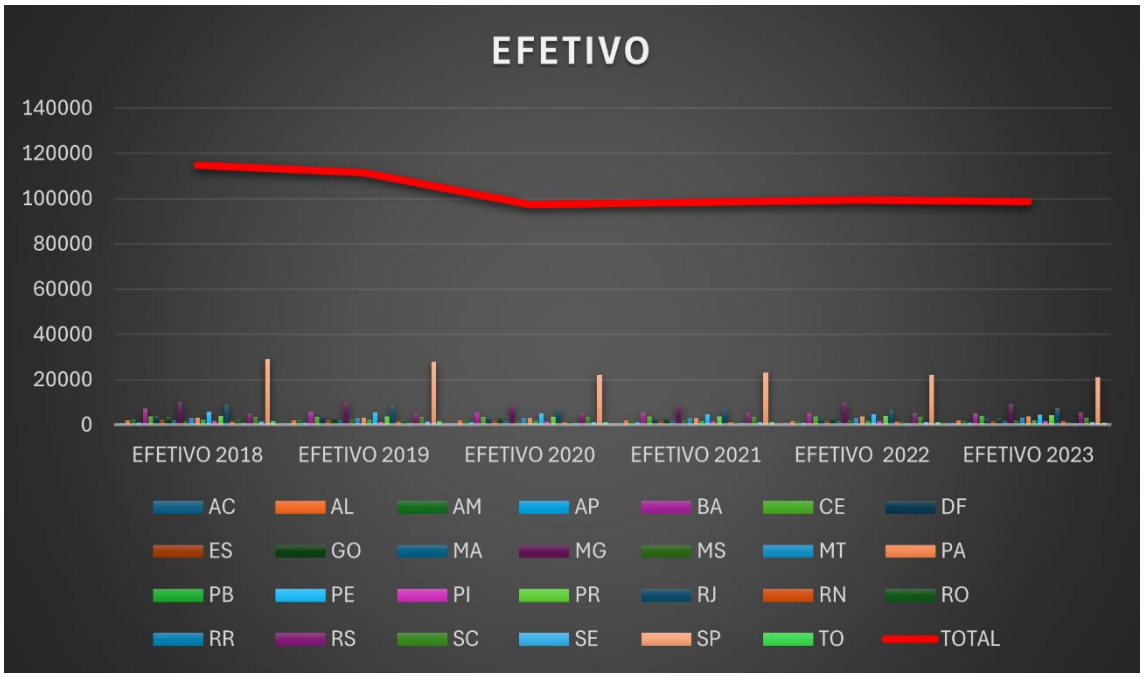
Ao mesmo tempo, o efetivo policial no Brasil tem enfrentado uma redução significativa. Em 2018, o país contava com 114.706 policiais, número que caiu para 98.596 em 2023. Essa redução é causada por fatores diverso como aposentadorias, falecimentos e abandono da carreira, muitas vezes devido às condições de trabalho e à falta de incentivos. A diminuição do efetivo contrasta com o aumento dos crimes, criando um cenário de dificuldade operacional para a segurança pública. Além disso, o número de delegacias no país permaneceu praticamente estagnado, ampliando a sobrecarga nas estruturas existentes.

Figura 3 – Número de Unidades de Atendimento da Polícia Civil



Fonte: Anuário Brasileiro de Segurança Pública, 2024.

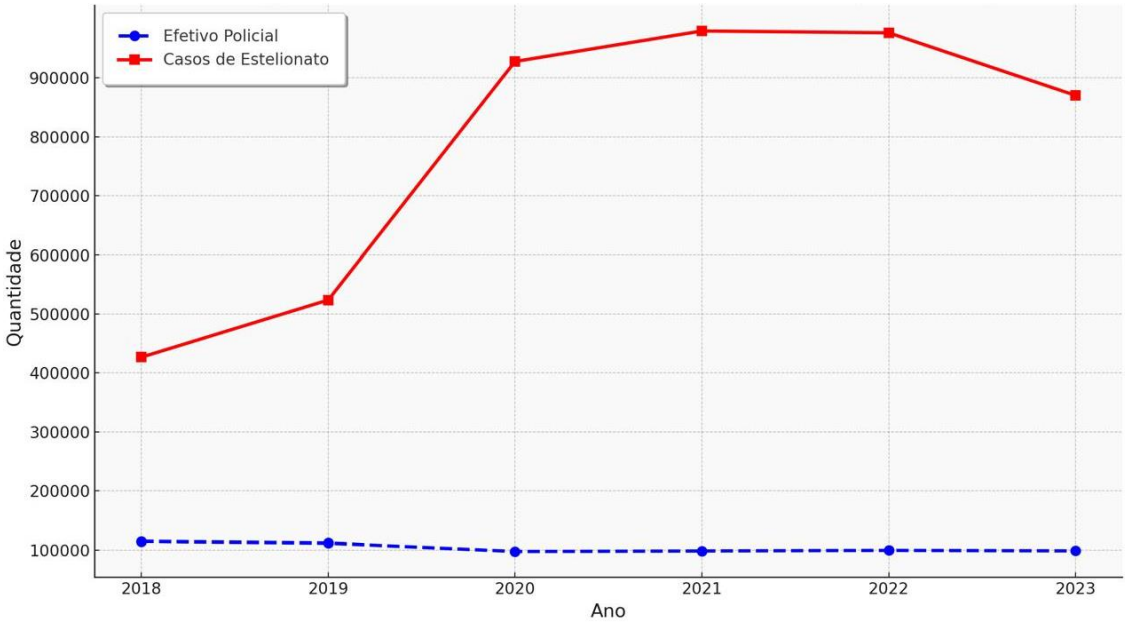
Figura 4 – Efetivo Policial por Estado Brasileiro



Fonte: Anuário Brasileiro de Segurança Pública, 2024.

Esse panorama revela que, enquanto os crimes eletrônicos evoluem rapidamente, as estruturas de segurança pública enfrentam dificuldades para acompanhar essas mudanças. As vítimas de estelionato muitas vezes não conseguem registrar os casos devido a delegacias sobrecarregadas, falta de integração entre estados e, em alguns casos, à vergonha ou desmotivação para relatar os crimes e admitir que forma vítimas de um golpe. O registro incompleto ou a subnotificação enfraquecem ainda mais o combate ao crime eletrônico, dificultando a identificação de padrões e a desarticulação de organizações criminosas.

Figura 5 – Comparativo: Efetivo Policial x Casos de Estelionato (2018-2023)



Fonte: Anuário Brasileiro de Segurança Pública, 2024.

Uma solução para esse cenário seria a adoção de tecnologias inovadoras que auxiliem no registro e análise desses crimes. Um exemplo é o desenvolvimento do chatbot INA (Inteligência Nacional de Atendimento), uma ferramenta que permitiria às vítimas registrarem ocorrências de forma rápida e eficiente. O INA coletaria dados essenciais, como contas bancárias, CPFs, números de telefone e perfis de redes sociais usados nos golpes, alimentando uma base de dados nacional que facilitaria as investigações e possibilitaria a criação de estratégias preventivas. Essa iniciativa visa não apenas suprir a carência de efetivo policial, mas também aumentar a acessibilidade e a eficiência no registro de crimes eletrônicos, contribuindo para o combate ao estelionato no Brasil.

O Brasil ainda enfrenta a ausência de dados específicos sobre estelionato digital, o que dificulta a compreensão da real dimensão desse tipo de crime. Nesse contexto, a implementação do INA (Instrumento Nacional de Atendimento) poderia desempenhar um papel fundamental, ao parametrizar a forma de registro de crimes virtuais e não virtuais. Essa padronização é crucial para que o país possa obter dados

confiáveis, possibilitando análises e a projeção de cenários futuros com base em informações reais.

Esse cenário evidencia a necessidade de modernizar as forças de segurança pública, o que requer investimentos em tecnologia, capacitação e uma integração nacional robusta. Essas medidas são uma possibilidade de acompanhamento da evolução dos crimes digitais.

2. BENCHMARKING INTERNACIONAL: COMO FAZER UM BOM CHATBOT?

A próxima etapa desse trabalho tem o objetivo de avaliar as boas práticas sobre a criação de um chatbot seguindo as literaturas internacionais.

Benchmark refere-se a um padrão de referência utilizado para avaliar e comparar o desempenho de um sistema ou modelo. No caso dos chatbots, benchmarks como GLUE - General Language Understanding Evaluation e SuperGLUE são amplamente utilizados para medir a compreensão geral da linguagem dos modelos, abrangendo métricas de medição, desenvolvimento, treinamento e avaliação de modelos de linguagem (Banerjee et al., 2023). Benchmarking, por outro lado, é o processo contínuo de comparação e análise dos resultados obtidos em relação a esses benchmarks, com o objetivo de identificar oportunidades de melhoria e otimização dos chatbots. Dessa forma, o benchmarking permite que desenvolvedores e pesquisadores ajustem seus modelos com base nos padrões estabelecidos.

O benchmarking da criação de um chatbot é essencial para aprimorar o serviço oferecido aos usuários, pois permite trazer novos elementos junto com ideias essenciais de padronização internacional. Esse processo possibilita identificar e adotar as melhores práticas do setor, sendo a melhor forma de aperfeiçoar e ampliar essa nova ferramenta proposta por esse Projeto Técnico Tecnológico.

A recente evolução tecnológica, com um mundo cada vez mais conectado à internet e os avanços na criação de sistemas de informação com software baseado em Inteligência Artificial, tornou o cenário propício para a popularização de chatbots. Por isso, é essencial avaliar seu desempenho. Segundo a literatura, existem dois

fatores importantes a serem considerados na avaliação de um chatbot: precisão e utilidade. A precisão do chatbot mede a veracidade dos fatos sem erros, enquanto a utilidade avalia até que ponto um chatbot atende às necessidades do usuário, contribuindo para um bom relacionamento e satisfação do cliente (Banerjee et al., 2023).

O estudo feito por Banerjee et al. (2023) explora como deve ser avaliada a aplicação de um chatbot. O primeiro teste consiste em fornecer informações ao chatbot e, em seguida, analisar o resultado gerado, com o objetivo de medir métricas relevantes, sua integridade e precisão. Tudo isso deve ser feito considerando o propósito do chatbot, seja para vendas, informações sobre saúde ou atendimento ao usuário.

Os chatbots devem ser precisos, relevantes e úteis, garantindo a satisfação dos usuários. A precisão indica a quantidade de respostas corretas fornecidas, enquanto a relevância é geralmente medida por meio da avaliação humana. Nesse contexto, é importante diferenciar dois conceitos fundamentais: benchmark e benchmarking.

O INA, como um chatbot voltado para o registro de ocorrência policial em casos de crimes de estelionato, pode ter como benchmark de avaliação central do usuário o End to End (E2E), que compara a resposta fornecida pelo chatbot com a melhor resposta que um humano poderia oferecer, conhecida na literatura como "resposta de ouro". A avaliação humana desempenha um papel essencial na qualificação e otimização dos chatbots, porém, pode ser subjetiva, propensa a viéses e ter um alto custo em larga escala.

O benchmark E2E visa simular cenários da vida real e avaliar o desempenho do chatbot no tratamento de diversas consultas dos usuários. Esse processo combina métricas objetivas, como precisão e exatidão, com avaliações subjetivas feitas por humanos, que fornecem classificações e feedbacks. Dessa forma, o benchmarking permite uma análise mais ampla e estratégica, garantindo que o chatbot atenda aos critérios de relevância, correção, precisão e utilidade de forma eficaz.

Assim, ao longo deste trabalho, os dois termos são utilizados de forma complementar: benchmark como um padrão de referência para avaliação de desempenho e benchmarking como o processo sistemático de comparação e

aprimoramento baseado nesses padrões (Banerjee et al., 2023).

Quadro 1: Abordagem teórico-conceitual

Boas práticas	Definição constitutiva e operacional	Origem teórica
Utilizar a metodologia (Machine Learning) que tem a função de receber os dados mencionados pelos usuários para analisar a melhor resposta sem uma resposta pré-programada, isso com a ajuda da Inteligência Artificial.	"Isso deu origem a uma nova seção de chatbots conhecidos como chatbots baseados em ML (Machine Learning) que não são pré-programados com regras, mas sim aprendem de grandes quantidades de dados e responder à entrada do usuário analisando os dados mencionados."	(Banerjee et al., 2023)
Benchmarking para garantia de qualidade	"Ajuda a verificar se as respostas do modelo são precisas, contextualmente apropriadas e livres de erros factuais ou equívocos. Ele verifica se o modelo pode entender e gerar texto de uma maneira que atenda às expectativas para uma conversa humana."	(Ray, 2023)
Conformidade ética com o benchmarking	"Os desenvolvedores podem garantir que o modelo lide com tópicos sensíveis de forma adequada, respeite a privacidade do usuário e cumpra as diretrizes para IA responsável."	(Ray, 2023)
General Language Understanding Evaluation (GLUE), SuperGLUE	"são benchmarks projetados para avaliar o desempenho de modelos em uma ampla gama de tarefas de PNL (processamento de linguagem	(Ray, 2023)

	natural). GLUE consiste em nove tarefas, incluindo resposta a perguntas, análise de sentimentos e implicação textual. SuperGLUE se baseia em GLUE e inclui tarefas mais desafiadoras, expandindo os limites dos modelos de PNL.”	
SQuAD	“Stanford Question Answering Dataset (SQuAD) é um benchmark popular para modelos de resposta a perguntas.”	(Ray, 2023)
Resposta a perguntas conversacionais (CoQA)	“Foi desenvolvido para avaliar modelos quanto à sua capacidade de lidar com respostas a perguntas conversacionais, o que requer a compreensão do histórico da conversa.”	(Ray, 2023)
Benchmark E2E	Usa um conjunto de “Respostas de Ouro” para medir com precisão o desempenho do chatbot.	(Banerjee et al., 2023)
Pesquisa de satisfação do cliente	Conforme a revisão da literatura, os autores propuseram um sistema baseado em nove critérios: segurança, velocidade, capacidade de resposta, satisfação, confiabilidade, garantia, tangibilidade, engajamento e empatia.	(Ilieva, 2025)
Pesquisa de satisfação do cliente	Tem destaque na literatura um sistema que incorpora 12 critérios, incluindo influência social, prazer, desempenho, facilidade de uso, utilidade, confiança e risco de privacidade.	(Ilieva, 2025)

2.1 Uso de Chatbots na Segurança Pública

Um chatbot, conforme definição da OpenAI, é um programa de computador projetado para simular conversas humanas por meio de processamento de linguagem natural (NLP). Esses sistemas são amplamente utilizados em diversas áreas, como atendimento ao cliente, educação e saúde, variando de funcionalidades simples baseadas em regras até soluções avançadas que utilizam inteligência artificial, como o ChatGPT.

No cenário dos crimes cibernéticos, os chatbots têm gerado impactos significativos. Por um lado, ferramentas maliciosas baseadas em chatbots têm sido utilizadas para atividades ilícitas, como campanhas de *phishing*, envio de mensagens fraudulentas e automação de ataques de engenharia social. Esses sistemas podem se passar por entidades confiáveis para enganar usuários e facilitar a execução de fraudes cibernéticas. Por outro lado, chatbots também têm contribuído para mitigar e combater tais crimes. Eles são capazes de monitorar comunicações, identificar padrões suspeitos e responder em tempo real a possíveis ameaças (OpenAI, 2025).

Além disso, os chatbots podem ser aliados importantes no combate a crimes, desempenhando papéis como a detecção de ameaças por meio da análise de comportamentos atípicos, a educação de usuários sobre segurança digital e boas práticas para evitar armadilhas virtuais, e o suporte inicial a vítimas, oferecendo orientação e encaminhamento para autoridades competentes. Esses sistemas também têm auxiliado as forças de segurança, processando grandes volumes de dados, identificando redes criminosas e otimizando análises forenses (OpenAI, 2025).

3. PROTOTIPAÇÃO DO INA À LUZ DAS MELHORES PRÁTICAS INTERNACIONAIS

A implementação do chatbot INA visa otimizar a coleta de informações essenciais para investigações, reduzindo a subnotificação e aprimorando a experiência do usuário. Antes de apresentar o protótipo, é fundamental contextualizar seus principais objetivos e funcionalidades. O INA foi projetado para padronizar a coleta de dados, garantindo registros mais completos e organizados, além de facilitar

o atendimento às vítimas, eliminando barreiras como o deslocamento até uma delegacia ou o receio de relatar o crime. O sistema também auxilia investigações policiais, fornecendo informações estruturadas que permitem identificar padrões criminosos e associações entre diferentes golpes, e possibilita a predição de tendências criminais por meio da análise de variáveis coletadas.

Utilizando técnicas de processamento de linguagem natural (PLN), o chatbot interage com as vítimas de forma eficiente, convertendo relatos em textos estruturados e preenchendo automaticamente campos essenciais para a investigação. A arquitetura do chatbot segue boas práticas internacionais de design de chatbots, garantindo que suas respostas sejam precisas e úteis, promovendo uma interação intuitiva e eficiente. Além disso, as informações coletadas são protegidas em conformidade com a Lei Geral de Proteção de Dados (LGPD), garantindo a segurança e privacidade dos usuários. Assim, a prototipação do INA é apresentada a seguir, destacando suas principais funcionalidades e aplicações para o combate ao crime de fraude eletrônica.

As primeiras telas de Interação como o chatbot procuram estabelecer um contato com a vítima forma clara, acessível, com uma linguagem popular, dando opções de ser via texto ou áudio, proporcionando assim maior adesão a esse tipo de registro e tentando evitar a desistência do registro por falta de entendimento ou por dificuldades operacionais.

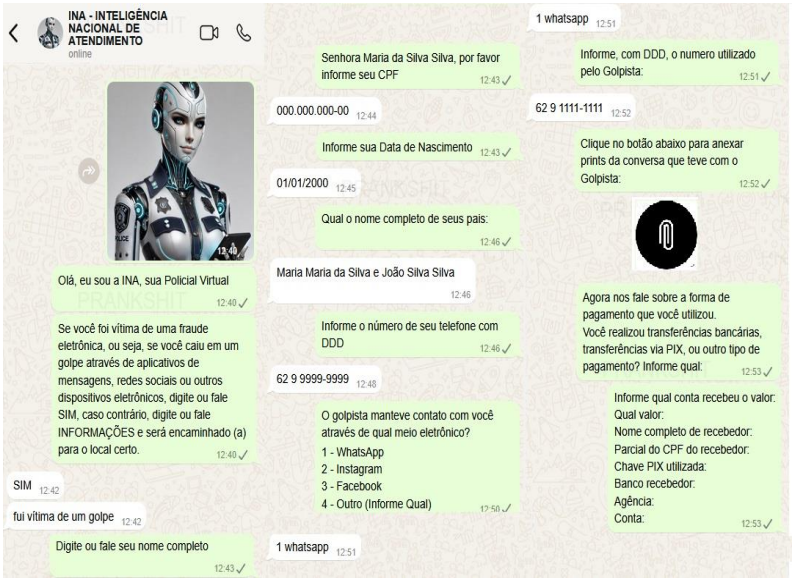
A seguir, têm-se a coleta de dados fundamentais que possibilitarão uma posterior investigação e também a construção de bases de dados essenciais no combate às fraudes eletrôncias, bem com na instituição de futuras ações preventivas.

Por fim, por se tratar de um crime de ação pública condicionada, ou seja, para que seja investigado é necessáro que a vítima deixe expresso sua vontade de representar criminalmente contra os possíveis autores, têm-se uma coleta dessa informação, sendo que a vítima pode expressar essa vontade no momento do registro, caso contrário será orientada que terá até seis meses para fazê-lo. Conforme preconiza o Código de Processo Penal.

Em ambas as situações, representando ou não, os dados serão coletados e irão compor a base de dados do INA. A vítima também receberá, em

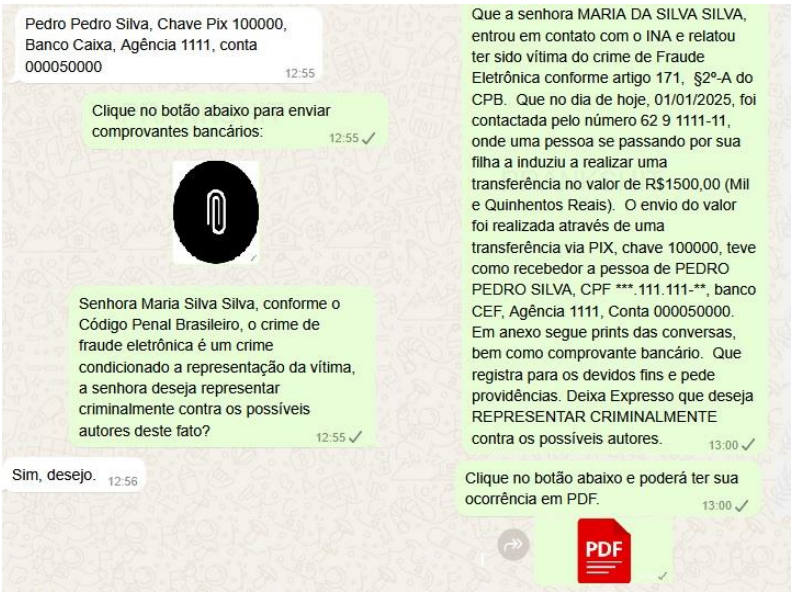
formato PDF a ocorrência. Entretanto, caso ela decida pela representação, a autoridade policial terá condições de dar andamento imediato às medidas cabíveis e representações judiciais necessárias.

Figura 7 – Tela de Interação com Usuário 1



Fonte: Desenvolvido pelos autores, 2025.

Figura 8 – Tela de Interação com Usuário 2



Fonte: Desenvolvido pelos autores, 2025.

4. PRINCIPAIS VARÍÁVEIS A SEREM COLETADAS PELO INA

Categoria	**Variável**	**Descrição**
Identificação dos suspeitos	Nome, CPF, RG, e-mail	Informações pessoais usadas nos golpes
Contatos utilizados	Números de telefone	Telefones usados para contato com as vítimas
Redes sociais e logins	Login e identificação dos usuários	Perfis em redes sociais, e-mails e outras credenciais
Transações bancárias	Contas bancárias	Contas utilizadas para recebimento do dinheiro fraudulento
Identificação do recebedor	Nome, CPF/CNPJ vinculado à conta	Pessoa ou empresa que recebe o dinheiro da fraude
Modus operandi	Tipo de golpe, padrão de abordagem	Estratégias e métodos utilizados pelo criminoso
Geolocalização	IP, localização da transação	Possíveis localizações do fraudador ou da vítima
Representação criminal	Vítima quer representar criminalmente?	Indicação se a vítima deseja formalizar a queixa
Valor do prejuízo	Montante financeiro envolvido	Valor perdido pela vítima
Histórico de denúncias	Ocorrências anteriores	Se há registros semelhantes vinculados ao suspeito
Correlação entre casos	Ligações com outros BOs	Possíveis conexões entre diferentes fraudes

5. AGENDA DE TRABALHO

Este trabalho, INA CHATBOT, tem como objetivo apenas uma prototipação, sendo que a implementação do software dependerá de etapas subsequentes, para as quais se oferece uma agenda de trabalho a título de planejamento.

Tempo	Órgão	Operacionalização	Demanda	Prazo revisional
Três Meses	Reunião no ministério da justiça com operadores de segurança pública	Reunião com delegados gerais das polícias judiciárias junto com os corpos técnicos de implementação	Promover o design thinking para aproximar os órgãos de segurança pública da ideia central do INA CHATBOT	**Um Mês**
Um Mês	Ministério da justiça / ministério público	Análise técnica da implementação de um protótipo	Programadores, alinhar com as unidades de tecnologia das polícias civis e polícia federal métodos de implementar o INA	**Um Mês**
3 mêses	Corpo Técnico	Prototipar	Desenvolver o protótipo do INA	**Um Mês**
3 mêses	Corpo Técnico	Desenvolvimento de um plano de implementação de do INA CHATBOT	Delinear as exigências das polícias, definir os objetivos do projeto, delimitar as responsabilidades dos órgãos	**Um Mês**
3 meses	Corpo Técnico	Fase de programação	Programar o chatbot	**1 mês**

6 meses	Polícias Civil	Fase de incorporação do INA CHATBOT em seus sistemas, divulgação para a população	Criar mecanismos de divulgação dos novos métodos de registros de ocorrências para dar escalabilidade a implementação	**1 mês**
2 meses	Policias Civis	Criar pareceres do uso do CHATBOT INA para registro de ocorrências nos estados	Criar elementos que possam melhorar o uso do CHATBOT INA	**1 mês**
Doze Meses	Reunião ministério da justiça, policiais civis e corpo técnico	Corpo técnico das polícias civis irá apresentar dados da eficiência, falhas do sistema, pontos a melhor no CHATBOT INA	Criar relatórios, apresentações de como foi a adaptação da sociedade ao registro de ocorrências via INA, apresentar pontos a serem melhorados no chatbot INA	**Um Mês**
Doze Meses	Corpo Técnico	Fase de programação 2	Corrigir erros apresentados pelos órgãos de segurança público, aperfeiçoar os chatbot de acordo com as demandas	**Um Mês**

6. CONSIDERAÇÕES FINAIS

O presente estudo abordou a necessidade de modernizar o registro de ocorrências policiais diante do crescimento expressivo das fraudes eletrônicas no Brasil. A partir da análise de dados do Anuário Brasileiro de Segurança Pública (2024) e da revisão das melhores práticas internacionais para o desenvolvimento de chatbots, foi elaborado o projeto do INA (Inteligência Nacional de Atendimento). O chatbot foi concebido para preencher lacunas no atendimento às vítimas, tornando o registro de ocorrências mais acessível, rápido e eficiente. Sua implementação também contribuirá para reduzir a subnotificação e melhorar a qualidade das investigações policiais, organizando e analisando os dados de forma estruturada.

A adoção de um chatbot na segurança pública traz impactos significativos. O sistema promove a eficiência no registro de ocorrências, reduzindo barreiras burocráticas e agilizando o atendimento. Permite a criação de uma base de dados nacional que auxilia na detecção de padrões e na identificação de organizações criminosas especializadas em fraudes eletrônicas.

Com base nas variáveis coletadas pelo INA, há um grande potencial para a geração de bases de dados estratégicas para a segurança pública. Uma ferramenta poderosa de inteligência policial na qual a centralização e análise dessas variáveis podem otimizar investigações, prevenir novos golpes e fortalecer a cooperação entre órgãos de segurança e instituições financeiras. Além disso, com a automação e integração dessas informações, é possível acelerar o processo de identificação e responsabilização dos criminosos, tornando o combate ao estelionato eletrônico mais eficaz.

Outro impacto é a otimização do trabalho das forças de segurança, liberando policiais para atuar diretamente nas investigações. O INA também atende a padrões internacionais, sendo desenvolvido com base em benchmarks como GLUE e E2E para garantir sua eficácia e qualidade.

Os próximos passos envolvem a implementação de um projeto-piloto, a coleta de feedback dos usuários e a realização de ajustes para aprimorar a experiência e a eficiência do chatbot. A longo prazo, o INA poderá ser expandido para o registro de outros tipos de crimes, ampliando seu impacto no combate à criminalidade digital no

Brasil. Este estudo reforça que a aplicação de tecnologia inovadora, alinhada às melhores práticas internacionais e à segurança de dados, pode transformar a forma como a sociedade lida com crimes cibernéticos, tornando o sistema de segurança pública mais ágil e acessível.

REFERÊNCIAS

18º ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA. Anuário brasileiro de segurança pública. 2024. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/253. Acesso em: 10 out. 2024.

AGÊNCIA SENADO. Panorama de ameaças para a América Latina *2024*. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/10/31/criacao-de-agencia-contra-ataques-ciberneticos-ganha-forca-em-subcomissao#:~:text=De%20acordo%20com%20o%20levantamento,atr%C3%A1s%20apenas%20dos%20Estados%20Unidos. Acesso em: 15 nov. 2024.

BANERJEE, Debarag; SINGH, Pooja; AVADHANAM, Arjun; SRIVASTAVA, Saksham. Benchmarking LLM powered chatbots: methods and metrics. **ArXiv,** [s.l.], p. 1-8, ago. 2023. Disponível em: https://arxiv.org/pdf/2308.04624. Acesso em: 30 jan. 2025. DOI: http://dx.doi.org/10.48550/ARXIV.2308.04624.

BASET – SUBGRUPO 4 – SEGURANÇA CIBERNÉTICA. Manual de conscientização em segurança cibernética na aviação civil. Brasília: ANAC, 2021.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 3 dez. 2012. Acesso em: 15 nov. 2024.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Código Penal e o Código de Processo Penal para tornar mais graves os crimes cibernéticos. Diário Oficial da União: seção 1, Brasília, DF, p.1, 28 mai. 2021. Acesso em: 16 nov. 2024.

CALDARINI, Guendalina; JAF, Sardar; MCGARRY, Kenneth. A literature survey of recent advances in chatbots. **Information**, [s.l.], v. 13, n. 1, p. 41, 15 jan. 2022. MDPI AG. Disponível em: https://www.mdpi.com/2078-2489/13/1/41. Acesso em: 27 jan. 2025. DOI: http://dx.doi.org/10.3390/info13010041.

DEPARTMENT OF COMPUTER APPLICATIONS, Sikkim University, Gangtok, Sikkim 737102, India. Benchmarking, ethical alignment, and evaluation framework for conversational AI: advancing responsible development of ChatGPT. Disponível em: https://www.sciencedirect.com/science/article/pii/S2772485923000534?via%3Dihub. Acesso em: 10 jan. 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA (São Paulo). Raio-X das forças de segurança pública no Brasil: resumo executivo. 2024. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/237. Acesso em: 10 out. 2024.

ILIEVA, Galina. Extension of Interval-Valued Hesitant Fermatean Fuzzy TOPSIS for Evaluating and Benchmarking of Generative AI Chatbots. **Electronics**, [S.L.], v. 14,

n. 3, p. 555, 30 jan. 2025. MDPI AG. DOI: http://dx.doi.org/10.3390/electronics14030555. Acesso em: 10 fev. 2025.

INTERPOL. Cybercrimes cross borders and evolve rapidly. Disponível em: https://www.interpol.int/Crimes/Cybercrime. Acesso em: 6 jan. 2025.

NOLASCO, Loreci Gottschalk; SILVA, Bruno Dutra Maciel. Crimes cibernéticos, privacidade e cibersegurança. **Revista Quaestio Iuris**, [s.l.], v. 15, n. 4, p. 2353-2389, 31 dez. 2022. Universidade do Estado do Rio de Janeiro. DOI: http://dx.doi.org/10.12957/rqi.2022.67976. Acesso em: 6 nov. 2024.

OPENAI. ChatGPT and AI: Empowering communication through advanced AI technologies. Disponível em: https://openai.com. Acesso em: 6 jan. 2025.

RAY, Partha Pratim. Benchmarking, ethical alignment, and evaluation framework for conversational AI: advancing responsible development of ChatGPT**. BenchCouncil Transactions on Benchmarks, Standards and Evaluations**, v. 3, n. 3, p. 1-19, 2023. DOI: https://doi.org/10.1016/j.tbench.2023.100136. Acesso em: 20 fev. 2025.

SILVA, Lorena Abbas da; FRANQUEIRA, Bruna Diniz; HARTMANN, Ivar A. Que os olhos não veem, as câmeras monitoram. **Revista Digital de Direito Administrativo**, [s.l.], v. 8, n. 1, p. 171-204, 29 jan. 2021. Universidade de São Paulo, Agência USP de Gestão da Informação Acadêmica (AGUIA). DOI: http://dx.doi.org/10.11606/issn.2319-0558.v8i1p171-204. Acesso em: 6 nov. 2024.

SIQUEIRA, Oniye Nashara; CONTIN, Alexandre Celioto; BARUFI, Renato Britto; LEHFELD, Lucas de Souza. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD. **Revista Eletrônica Pesquiseduca**, [s.l.], v. 13, n. 29, p. 236-255, 21 mar. 2021. Universidade Católica de Santos. DOI: http://dx.doi.org/10.58422/repesq.2021.e1029. Acesso em: 6 nov. 2024.