Me Deixe em Paz: Detecção e bloqueio de chamadas spam no Android com base em critérios comportamentais

Victor Giudice Tavares da Cruz[1] **e Silvana Rossetto**[1]

[1]Instituto de Computação – Universidade Federal do Rio de Janeiro (UFRJ)
Cidade Universitária – Rio de Janeiro – RJ

victorgtdacruz@outlook.com, silvana@ic.ufrj.br

Abstract. *The significant growth of unwanted phone calls has negatively affected the user experience, privacy, and security of mobile device users. This work presents the development of an Android mobile application, named "Me Deixe em Paz", designed to identify and block calls classified as spam through the analysis of behavioral criteria observable in call records. The results indicate that a behavioral rule-based approach has the potential to reduce unwanted calls, suggesting that lightweight and interpretable solutions can be a viable alternative for mitigating phone spam.*

Resumo. *O aumento expressivo de chamadas telefônicas indesejadas tem impactado negativamente a experiência, a privacidade e a segurança de usuários de dispositivos móveis. Este trabalho apresenta o desenvolvimento de um aplicativo móvel para Android, denominado "Me Deixe em Paz", para identificação e bloqueio de chamadas classificadas como spam por meio da análise de critérios comportamentais observáveis em registros telefônicos. Os resultados obtidos indicam que a abordagem baseada em regras comportamentais apresenta potencial para reduzir chamadas indesejadas, demonstrando que soluções leves e interpretáveis podem constituir uma alternativa viável para a mitigação de spam telefônico.*

1. Introdução

Nas últimas décadas, a popularização dos dispositivos móveis mudou completamente o modo como as pessoas se relacionam, trabalham e consomem informação. No Brasil, segundo o Instituto Brasileiro de Geografia e Estatística (IBGE), a posse de telefone celular entre as pessoas com 10 anos ou mais subiu de 77,4% em 2016 para 88,9% em 2024 (cerca de 167,5 milhões de pessoas no total) [IBGE 2025]. Esse cenário favorece a integração digital, mas também expõe os usuários a grandes quantidades de informação, incluindo propagandas e fraudes. Entre estas, uma das mais comuns são as chamadas telefônicas indesejadas, conhecidas popularmente como "chamadas spam".

Essas chamadas podem ter diversas motivações, como campanhas de *telemarketing*, cobranças e tentativas de golpe, e representam um fenômeno em escala global. Segundo relatório da TrueCaller [Truecaller 2022], em 2021, assim como nos três anos anteriores, o Brasil manteve a primeira posição do mundo em chamadas *spam*, com uma média de $32,9$ chamadas por usuários por mês.

A maioria dos golpes digitais são feitos por meio de ligações telefônicas e causam impactos emocionais significativos às vítimas. Segundo pesquisa sobre golpes digitais

realizada no Brasil em 2024 pela Global Anti-Scam Alliance [Gasa 2024] cerca de 82% dos 1.322 entrevistados foram abordados por golpistas através de ligações nos 12 meses anteriores à pesquisa, muito mais que em outras formas de comunicação. Dos entrevistados, 35% perderam dinheiro em golpes (apenas 4% das vítimas recuperaram todo o valor perdido) e 45% das vítimas de golpe relataram um forte impacto emocional.

A popularização das técnicas de inteligência artificial (IA) tem contribuído com a sofisticação dos golpes, uma vez que criminosos a utilizam para conquistar a confiança da vítima. Técnicas como alterações na voz com a finalidade de simular um sotaque ou pessoas de interesse, também conhecida como *"audio deepfake"*, têm sido identificadas em chamadas maliciosas. Em 2025, uma em cada quatro chamadas *spam* continham áudio gerado por IA e, destas, 55% foram identificadas como fraude, sendo, portanto, a IA considerada a maior ameaça emergente para as chamadas de voz [1].

Por outro lado, a IA também pode ser usada para proteger as pessoas. A Apple, por exemplo, lançou uma nova funcionalidade no seu sistema operacional iOS 26 que utiliza técnicas de inteligência artificial para atender uma ligação de números desconhecidos [Apple 2026]. Outras empresas, como TrueCaller, Hiya e Whoscall, também surgiram com o objetivo de combater as chamadas *spam*. Elas divulgam relatórios com dados que mostram a dimensão do problema, a tendência dos golpistas e os prejuízos causados, além de oferecer aplicativos que auxiliam na identificação e bloqueio de ligações considerando uma base de dados construída com algoritmos e dados proprietários.

A Agência Nacional de Telecomunicações (Anatel), por sua vez, também vem adotando medidas para mitigar o problema nos últimos anos. Algumas são: a criação do "Qual empresa me ligou?", plataforma que identifica o CNPJ e a Razão Social associados a determinados números de telefone; e a criação do "Outubro CiberSeguro", visando conscientizar a sociedade sobre a importância da proteção e do combate às ameaças online. A agência afirma que, entre junho de 2022 e dezembro de 2024, realizou o bloqueio de 184,9 bilhões de chamadas indesejadas no Brasil [ANATEL 2026]. Apesar dessas iniciativas, em agosto de 2025, a Anatel removeu a obrigatoriedade do prefixo 0303 em chamadas de *telemarketing*, implementado em 2022, sob a justificativa de que houve uma rejeição automática a estas ligações por parte dos usuários [2]. Ao reduzir a transparência da origem da ligação, aumenta-se o risco de que usuários atendam chamadas potencialmente maliciosas, favorecendo tentativas de fraude e engenharia social, especialmente em um contexto de crescente sofisticação dos agentes fraudulentos.

Embora existam diversas soluções comerciais para identificação de chamadas indesejadas, muitas delas dependem de grandes bases de dados proprietárias e algoritmos pouco transparentes. Nesse contexto, este trabalho investiga uma abordagem baseada na análise de padrões comportamentais observados em registros de chamadas, utilizando regras heurísticas simples. A proposta busca avaliar a viabilidade dessa estratégia em um cenário real de uso. Para isso foi desenvolvido e avaliado um aplicativo para Android, denominado "Me Deixe em Paz", capaz de identificar e bloquear chamadas classificadas

[1]Global Call Threat Report: Insights into today's worldwide spam problem, https://pt-br.hiya.com/, 2025.

[2]REDAÇÃO G1. Anatel tira obrigatoriedade do prefixo 0303 em ligações de telemarketing, 2025. Disponível em: https://g1.globo.com/tecnologia/noticia/2025/08/14/anatel-revoga-obrigatoriedade-do -prefixo-0303-em-ligacoes-de-telemarketing.ghtml

como *spam* com base em critérios comportamentais. A proposta destina-se a qualquer cidadão brasileiro usuário de dispositivo Android que deseje mitigar o recebimento de chamadas indesejadas em seu cotidiano.

A fase experimental consistiu na disponibilização do aplicativo a um grupo de usuários voluntários, que o utilizaram em seu contexto cotidiano por um período de até 27 dias. Durante esse período, foram coletados dados referentes às chamadas telefônicas e ao uso geral da aplicação. Esses registros foram posteriormente analisados com o objetivo de avaliar o comportamento das regras implementadas e a capacidade do sistema de identificar e bloquear chamadas potencialmente indesejadas. Os usuários concordaram com os termos e condições apresentados no próprio aplicativo e também concederam as permissões solicitadas pelo sistema operacional. A partir dos dados coletados durante o período de experimento, observou-se que o protótipo foi capaz de bloquear uma parcela significativa das chamadas classificadas como indesejadas, alcançando uma taxa de bloqueio observada de 74,29%, considerando a hipótese de que as chamadas bloqueadas correspondiam a *spam*. Embora não tenha sido possível validar individualmente cada chamada classificada, os resultados sugerem que a adoção de critérios comportamentais simples pode contribuir para a mitigação de chamadas indesejadas em um contexto real de uso, ainda que com limitações.

O restante deste texto está organizado da seguinte forma. Na seção 2 apresenta-se estudos e iniciativas voltados à identificação e bloqueio de chamadas *spam*. Na seção 3, descreve-se o projeto e a implementação da solução proposta. Na seção 4 apresenta-se a avaliação do protótipo desenvolvido e a análise da eficácia na resolução do problema. Finalmente, na seção 5 discute-se as conclusões deste trabalho e possíveis evoluções.

2. Trabalhos relacionados

[Tu et al. 2016] descrevem por que o combate ao *spam* de email é mais fácil e eficaz que o de chamadas telefônicas, uma vez que é possível analisar o conteúdo da mensagem antes da sua entrega ao destinatário, sem restrição forte de tempo. [Li et al. 2018] propõem um sistema de detecção de chamadas maliciosas utilizando aprendizado de máquina aplicado a grandes volumes de registros telefônicos. Os resultados indicam que a observação do comportamento do chamador ao longo do tempo é um fator relevante para a detecção. No estudo de [Azad and Morla 2013] a taxa de detecção de chamadores maliciosos foi de aproximadamente 80% nos primeiros dias de avaliação, podendo alcançar cerca de 99% à medida que os padrões comportamentais se consolidam ao longo do tempo. Trabalhos nesta linha evidenciam o potencial de abordagens supervisionadas, baseadas em grande volume de dados previamente classificados. Existem também soluções comerciais que realizam identificação e bloqueio de chamadas por meio de análise colaborativa e reputação de números. Essas aplicações também utilizam grandes bases de dados e modelos proprietários, o que dificulta o acesso às métricas e aos detalhes metodológicos. Dentre eles, destacam-se o Truecaller, o Whoscall e o Hiya.

De forma geral, trabalhos acadêmicos e soluções comerciais e regulatórias para tratamento de chamadas *spam* evidenciam que o problema das chamadas telefônicas indesejadas é amplamente reconhecido e abordado sob diferentes perspectivas. Observa-se que grande parte das soluções existentes faz uso de bases de dados e algoritmos próprios ou de parcerias com operadoras de telecomunicações, o que pode limitar a transparência

e a reprodutibilidade dessas abordagens.

Diferentemente das soluções que utilizam modelos proprietários, neste trabalho buscamos explorar uma abordagem mais transparente, baseada em critérios explícitos e na análise comportamental de chamadas. Trata-se de uma solução de código aberto, que busca operar com uma base de dados reduzida, priorizando a privacidade do usuário. Por fim, pretende-se avaliar a viabilidade dessa abordagem em um ambiente real de uso.

3. Projeto do aplicativo

O aplicativo proposto foi desenvolvido para o sistema operacional Android e sua finalidade é identificar e bloquear chamadas telefônicas antes da sua entrega ao usuário, caso classificada como *spam*. O aplicativo utiliza informações disponíveis no cabeçalho da chamada e em uma base de dados pré-processada para tomar decisões em tempo real.

Para realizar a identificação e bloqueio de chamadas, o Android disponibiliza um serviço chamado `CallScreeningService`. Este serviço funciona como uma ponte entre o aplicativo e o sistema operacional, transmitindo eventos quando o aparelho recebe uma chamada e aguardando uma resposta do aplicativo quanto à triagem. Nesses eventos, são disponibilizados os números de origem da chamada. É por este número que identificamos um chamador. Chamadas de um mesmo número são entendidas como do mesmo chamador, e, no caso de números diferentes, como de chamadores diferentes.

No restante desta seção, apresentamos o conjunto de regras definidas para identificar chamadas *spam*, o problema da falsificação de números, os requisitos do aplicativo proposto, sua arquitetura lógica e de sistema e questões relevantes da sua implementação.

3.1. Regras para classificar chamadas

Para este projeto, foram definidas e avaliadas as seguintes regras para classificar as chamadas e auxiliar na identificação de um chamador *spam*:

1. **Chamadas curtas**: se o receptor atendeu uma chamada que durou menos de seis segundos.
2. **Chamadas perdidas**: se o receptor perdeu três ou mais chamadas do mesmo chamador.
3. **Chamadas rejeitadas**: se o receptor rejeitou duas ou mais chamadas do mesmo chamador.
4. **Chamadas em massa**: se três ou mais receptores receberam alguma chamada do mesmo chamador.
5. **Chamadas já identificadas**: se há alguma palavra suspeita no nome do chamador. Esta informação é preenchida pelo receptor (caso o número esteja salvo como um contato) ou por terceiros, como a operadora ou outro agente da rede telefônica, que costumam marcar chamadas de chamadores suspeitos como “chamada suspeita”, por exemplo.
6. **Chamadas de prefixo conhecido**: chamadas com o prefixo 0303, criado pela Anatel para chamadas de *telemarketing*, e com o prefixo 0800 de empresas.
7. **Chamadas privadas**: chamadas onde o número não é preenchido por nenhum agente da rede telefônica.
8. **Chamadas longas**: se o receptor atendeu uma chamada que durou mais de seis segundos.

9. **Chamadas de contatos**: se o número do chamador está presente na lista de contatos do receptor.

A regra 1 tem como ponto de partida as diretrizes da Anatel, que caracteriza chamadas com menos de seis segundos como "chamadas curtas". Esse tipo de chamada representa uma parcela significativa do tráfego no sistema telefônico e é frequentemente associado a práticas abusivas, como disparos automatizados para verificação de números ativos ou para induzir o retorno da ligação pelo usuário, condutas que podem configurar uso inadequado do serviço telefônico [ANATEL 2020].

As regras 2, 3 e 4 visam proteger o usuário do excesso de chamadas causadas por certos chamadores. A regra 2 identifica um chamador como *spam* a partir de uma quantidade de chamadas perdidas. Já a regra 3, a partir de uma quantidade menor de chamadas rejeitadas, dando maior peso ao ato de recusar a chamada. A regra 4, por sua vez, visa complementar as anteriores nos casos em que um chamador foca em múltiplos receptores sem a insistência em algum específico. Os números mínimos de chamadas para se enquadrar nestas regras — como três chamadas nas regras 2 e 4, ou duas chamadas na regra 3 — foram escolhidos com base na expectativa da quantidade de usuários no experimento deste trabalho, de cerca de 15 a 20 usuários. Esses valores devem ser ajustados para outras realidades, como uma possível adoção em massa do projeto na sociedade.

A regra 5 utiliza uma informação disponibilizada por outras entidades, seja o próprio receptor ou outro agente da rede telefônica, como a operadora. Dentre os campos armazenados dentro de cada chamada no Android, existe um campo que contém um texto caso este tenha sido exibido na tela do usuário durante o toque. Ao verificar esse texto, podemos validar se ele contém alguma palavra que esteja relacionada com chamadas indesejadas. As palavras verificadas neste projeto são: "spam", "suspeito", "suspeita", "fraude", "golpe", "telemarketing", "venda", "vendas" e "cobrança". Chamadas de números com prefixos previamente associados a atividades comerciais (regra 6) e de números privados ou ocultos (regra 7) são bloqueadas sem a necessidade de análise de comportamento. Essas regras foram incorporadas por apresentarem, em seu próprio identificador, características frequentemente associadas a práticas como *telemarketing* ou ocultação da origem da chamada.

As regras 8 e 9 foram adicionadas para tratar casos onde um número pode se encaixar em uma das regras de identificação de *spam*, mas é um número confiável do receptor. Caso o receptor tenha atendido uma chamada do chamador com duração maior que seis segundos ou o número do chamador esteja salvo na lista de contatos do receptor, o chamador não será classificado como *spam*, mesmo se encaixando nas regras 1 a 7. Ultrapassar seis segundos numa chamada ou estar presente na agenda de contatos é entendido como a demonstração do interesse do receptor em manter a comunicação com este chamador.

Diferentemente de soluções comerciais já mencionadas, o aplicativo proposto não substitui os aplicativos nativos de chamadas ou mensagens do sistema operacional. Ele atua de forma complementar, integrando-se ao sistema apenas para filtrar as chamadas, respeitando as restrições impostas pela plataforma e minimizando o acesso e manipulação de dados sensíveis do usuário. Assim, o aplicativo nativo de chamadas mantém suas funções de realizar e receber chamadas, além de visualizar o histórico. A proposta prioriza uma abordagem acessível, de baixo custo operacional e com código aberto, permitindo auditoria, reprodução acadêmica e evolução da solução por parte da comunidade.

Uma prática frequentemente associada a chamadas indesejadas é o uso de técnicas de *spoofing*, que permitem mascarar o número de origem da chamada. Essa prática reduz a confiabilidade de abordagens baseadas exclusivamente no número de origem da chamada (como é o caso desta proposta) para a identificação de chamadores. Sugere-se o uso de soluções de diferentes tipos de forma conjunta para mitigar o problema [Tu et al. 2016]. [Pietri et al. 2025] mostram como funciona a infraestrutura do sistema telefônico mundial, evidenciando que não há suporte para validação da identidade de chamadores, fazendo com que o *spoofing* seja um grave problema ao combate de chamadas *spam*.

Observa-se ainda que o modelo de negócios do setor de telecomunicações influencia diretamente as estratégias de combate à chamadas *spam* pois a remuneração está associada ao volume de tráfego. Esse cenário contribui para a baixa priorização de medidas preventivas, uma vez que pode impactar negativamente negócios consolidados. Como consequência, observa-se a manutenção de um ambiente favorável à recorrência de chamadas indesejadas, no qual prejuízos financeiros, invasões de privacidade e desgaste do usuário persistem [Pietri et al. 2025].

3.2. Arquitetura lógica e de sistema

A Figura 1 apresenta a arquitetura lógica e de sistema do aplicativo.

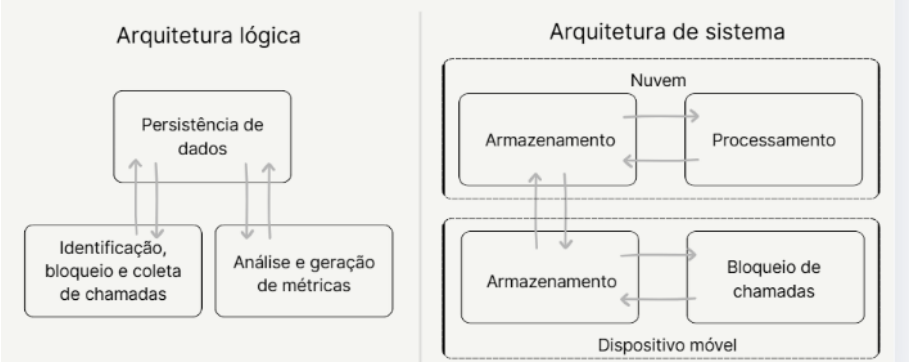

Figura 1. Arquitetura lógica e de sistema do aplicativo

O componente **Identificação, bloqueio e coleta de chamadas** é responsável por interceptar chamadas recebidas, aplicar as regras de detecção de *spam* e executar o bloqueio quando for o caso. Esse componente também realiza a coleta dos metadados das chamadas para posterior análise. O componente **Persistência de dados** é responsável pelo armazenamento estruturado dos dados coletados, bem como pela disponibilização dessas informações para consulta e processamento. Por último, o componente **Análise e geração de métricas** é responsável pelo processamento assíncrono dos registros de chamadas, aplicando regras de classificação e geração de métricas globais do sistema. Esse componente permite identificar padrões comportamentais, como números que realizam chamadas para múltiplos destinatários em curto intervalo de tempo.

No protótipo desenvolvido neste trabalho, optou-se por uma arquitetura de sistema distribuída entre o dispositivo móvel e uma infraestrutura em nuvem (como mostrado na Figura 1). No protótipo, o componente de identificação, bloqueio e coleta de chamadas e parte do componente de persistência (destinada ao armazenamento local dos dados processados) são mantidos no aplicativo móvel. Essa decisão busca garantir desempenho adequado, uma vez que o bloqueio deve ocorrer em tempo compatível com o

fluxo de uma chamada telefônica e deve funcionar mesmo que o dispositivo esteja desconectado da Internet. Na infraestrutura em nuvem foram instanciados a camada principal de persistência de dados (armazenamento consolidado das informações coletadas e das informações mais recentes) e o componente de análise e geração de métricas (processamento assíncrono dos registros e identificação de padrões globais de comportamento). A adoção de uma infraestrutura em nuvem permitiu realizar análises mais complexas e consolidar dados de múltiplos usuários sem comprometer os recursos computacionais do dispositivo móvel. Além disso, essa configuração possibilitou o cruzamento de informações para identificação de comportamentos suspeitos em escala ampliada.

3.3. Questões relevantes da implementação do aplicativo

O aplicativo foi desenvolvido utilizando a linguagem Kotlin, recomendada para o desenvolvimento de aplicações nativas, uma vez que APIs específicas do sistema operacional, como as de identificação e triagem de chamadas telefônicas, precisam ser acessadas. A interceptação e bloqueio das chamadas telefônicas foi realizada por meio do serviço `CallScreeningService`, uma API introduzida no Android 7.0. Quando uma chamada é recebida e o aplicativo é notificado, o sistema inicia uma contagem de cinco segundos. Caso o aplicativo não responda se deseja bloquear ou liberar a chamada dentro deste tempo, o sistema libera a chamada para o usuário e ignora qualquer resposta recebida posteriormente. Caso o aplicativo decida bloquear a ligação, o aparelho não toca e o chamador recebe um aviso genérico e não configurável de indisponibilidade do receptor. **O código do aplicativo está disponível no GitLab** [3]

4. Avaliação

A avaliação realizada teve como objetivo verificar o desempenho da solução proposta em um cenário real de utilização. No total, 17 pessoas participaram do experimento entre 5 e 31 de janeiro de 2026 (7 usuários durante 27 dias e 10 usuários durante 13 dias). Utilizando como base dados da TrueCaller [Truecaller 2022], estima-se que ocorre em média uma (1) chamada de *spam* por usuário por dia. Considerando 7 usuários durante 27 dias e 10 usuários durante 13 dias, estimamos um total de 319 chamadas *spam* para fins de análise dos resultados deste experimento.

Foram analisadas 8.618 chamadas, sendo 7.477 chamadas coletadas no momento da ativação do serviço de bloqueio — referentes ao histórico de chamadas do usuário — e 1.141 durante a fase de experimento com o serviço de bloqueio ativo. Assim, com base na estimativa geral de chamadas *spam* esperadas, presume-se que 28% das chamadas recebidas pelos voluntários seriam *spam*. As 8.618 chamadas foram realizadas por 5.037 números distintos, resultando em uma média de 1,71 chamadas por número chamador e desvio padrão de 5,62. Dos diferentes números, 4.379 realizaram apenas uma chamada, enquanto o maior chamador realizou 224 chamadas. Ao aplicar o algoritmo a estas chamadas, foram identificados 437 números de chamadores *spam*, cerca de 9,97% dos chamadores. Das 1.141 chamadas ocorridas na fase de experimento — e partindo da média de 319 chamadas que poderiam ser consideradas *spam* — 215 foram bloqueadas e 22 foram identificadas e não bloqueadas (regra 8 ou 9), totalizando 237 chamadas iden-

[3]Repositório no GitLab. Disponível em: https://gitlab.com/victorgtdacruz1/medeixaempaz. Acesso em: 10 mar. 2026.

Regras	**Qtde números**	**Porcentagem**
Chamadas em massa	25	05,72%
Chamadas perdidas	44	10,06%
Chamadas rejeitadas	73	16,70%
Chamadas curtas	127	29,06%
Chamadas já identificadas	118	27,00%

Tabela 1. Quantidade de números identificados em cada regra (maiores índices)

tificadas pelo algoritmo após a classificação dos números. A Tabela 1 destaca as regras mais ativadas na identificação de chamadas *spam*.

Ao considerar que todas as chamadas bloqueadas correspondiam efetivamente a uma chamada *spam*, o protótipo apresentou taxa de bloqueio de 74,29%. Entretanto, não é possível validar individualmente cada chamada classificada, uma vez que o estudo se deu em ambiente real de uso e não contou com uma base previamente rotulada.

4.1. Limitações

Algumas limitações deste trabalho devem ser consideradas. A primeira está relacionada ao baixo número de participantes no experimento. Uma amostra reduzida restringe a capacidade de generalização dos resultados, uma vez que os padrões identificados podem não representar adequadamente o comportamento de um público amplo e diverso. Outra questão relevante é o fato da classificação de chamada *spam* ser de caráter subjetivo e variável entre os usuários. A percepção de uma chamada indesejada pode depender de fatores abstratos, como contexto, expectativas individuais e tolerância a chamadas. Por fim, outra limitação é a imprecisão observada nas primeiras chamadas de cada número de origem. Os critérios adotados para classificação de *spam* dependem da existência de um histórico prévio de chamadas associado a cada número. Assim, ao receber as primeiras chamadas de determinado chamador, o sistema não dispõe de dados suficientes para tomar uma decisão de bloqueio com confiança. Essas limitações não invalidam os resultados do estudo, mas evidenciam a necessidade de cautela em sua interpretação e apontam oportunidades para aprimoramentos futuros, como a ampliação da amostra, o aumento do tempo de observação e o refinamento dos critérios de classificação de chamadas.

5. Conclusão

Este estudo teve como objetivo analisar a viabilidade de uma abordagem baseada em histórico de chamadas e critérios comportamentais para o bloqueio de ligações classificadas como *spam* em dispositivos móveis. Para isso, foi desenvolvido um aplicativo capaz de coletar dados de uso real, aplicar critérios de decisão e avaliar o desempenho da solução a partir de um experimento com usuários voluntários. A partir da análise dos dados obtidos, foi possível concluir que o experimento foi bem-sucedido dentro do escopo proposto. A solução alcançou uma taxa de bloqueio estimada de 74,29%, indicando que a abordagem adotada foi capaz de identificar padrões associados a chamadas indesejadas e atuar de forma efetiva na mitigação desse problema. Ressalta-se que ainda são necessários estudos adicionais para o aprofundamento do tema. Explorar amostras maiores, realizar períodos de observação mais longos, novos critérios de classificação e abordagens híbridas podem reduzir incertezas e aprimorar a assertividade das decisões.

Referências

ANATEL (2020). Combate às chamadas abusivas. https://www.gov.br/anatel/pt-br/consumidor/chamadas-abusivas.

ANATEL (2026). Autenticação e identificação de chamadas. https://www.gov.br/anatel/pt-br/regulado/acompanhamento-e-controle/autenticacao-e-identificacao-de-chamadas.

Apple (2026). Manual de uso do iphone. https://support.apple.com/pt-br/guide/iphone/iphe4b3f7823/ios.

Azad, M. A. and Morla, R. (2013). Caller-rep: Detecting unwanted calls with caller social strength. *Computers & Security*, 39:219–236.

Gasa (2024). Golpes digitais no brasil. https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/7bdaac$_c$0e41faf1b774d6da3729412294d2a81.pdf.

IBGE (2025). PNAD Contínua. https://agenciadenoticias.ibge.gov.br. "No Brasil, 88,9% da população de 10 anos ou mais tinha celular em 2024".

Li, H., Xu, X., Liu, C., Ren, T., Wu, K., Cao, X., Zhang, W., Yu, Y., and Song, D. (2018). A machine learning approach to prevent malicious calls over telephony networks. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 53–69. IEEE.

Pietri, M., Mamei, M., and Colajanni, M. (2025). Telecom spam and scams in the 5g and artificial intelligence era: analyzing economic implications, technical challenges and global regulatory efforts. *International Journal of Information Security*, 24(3):139.

Truecaller (2022). Global spam report. https://www.truecaller.com/blog/insights/top-20-countries-affected-by-spam-calls-in-2021.

Tu, H., Doupé, A., Zhao, Z., and Ahn, G.-J. (2016). Sok: Everyone hates robocalls: A survey of techniques against telephone spam. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 320–338. IEEE.