Segurança e Robustez de Estratégias para Anonimização e De-Anonimização de Dados Sensíveis de Localização

Marília M. Biz[1], **Henry C. Nunes**[2], **Bruno V. Lima**[1], **Weverton Cordeiro**[1]

[1] Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
[2] Escola Politécnica – Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)

Abstract. *The release of sensitive spatial data raises significant privacy concerns, particularly in urban epidemiological surveillance. This paper investigates the impact of different anonymization techniques applied to georeferenced data of Aedes aegypti breeding sites, analyzing both predictive utility and robustness against de-anonymization attacks. We evaluate techniques based on generalization, aggregation, permutation, and differential privacy in a realistic prospective outbreak prediction scenario. Data utility is assessed through the performance of predictive models trained on historical data, while privacy protection is evaluated using direct linkage, probabilistic linkage, and spatial ambiguity attacks. The results show that properly parameterized anonymization techniques preserve competitive predictive performance compared to the original data, while providing strong resistance to re-identification attempts. These findings demonstrate that privacy and analytical utility can be effectively balanced when spatial anonymization mechanisms are carefully evaluated.*

Resumo. *A divulgação de dados espaciais sensíveis impõe desafios significativos à privacidade, especialmente em contextos de vigilância epidemiológica urbana. Este trabalho investiga o impacto de diferentes técnicas de anonimização aplicadas a dados georreferenciados de focos do mosquito Aedes aegypti, analisando simultaneamente sua utilidade preditiva e sua robustez diante dos ataques de desanonimização. Foram avaliadas técnicas baseadas em generalização, agregação, permutação e privacidade diferencial, considerando um cenário realista de predição prospectiva de surtos. A utilidade dos dados anonimizados foi medida por meio do desempenho de modelos preditivos treinados com dados históricos, enquanto a proteção à privacidade foi avaliada por meio de ataques de ligação direta, probabilística e de ambiguidade espacial. Os resultados indicam que técnicas adequadamente parametrizadas preservam desempenho preditivo competitivo em relação aos dados originais, ao mesmo tempo em que oferecem resistência a tentativas de reidentificação. Esses achados evidenciam que é possível conciliar privacidade e utilidade analítica em dados espaciais sensíveis quando mecanismos de anonimização são cuidadosamente avaliados.*

1. Introdução

O crescimento exponencial de dispositivos IoT e da computação ubíqua gera volumes sem precedentes de dados espaciais, que podem ser extremamente úteis em pesquisas científicas, desenvolvimento de novos produtos e soluções, etc. Há diversos exemplos na literatura de como esses dados podem ser empregados em pesquisas científicas, incluindo

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001

caracterização de mobilidade em redes móveis [Ribeiro et al. 2020], detecção de comunidades [Ribeiro et al. 2021], vigilância epidemiológica [Barnabé et al. 2025], entre outros. Em muitos casos, no entanto, os dados são de natureza extremamente sensível (por ex., dados pessoais sensíveis relativos à saúde ou ao comportamento). Assim, a exposição indevida desses dados pode representar riscos significativos à privacidade individual.

Dado esse contexto, um grande desafio que se impõe é "*Como permitir acesso a grandes volumes de dados sensíveis para investigações científicas, garantindo que as pesquisas possam ser realizadas com a maior qualidade possível, e preservando a privacidade e inviolabilidade dos dados pessoais?*". Considere por exemplo dados de *geolocalização* relacionados à saúde [Fraccaro et al. 2019, Barnabé et al. 2025]. A investigação desses dados pode gerar soluções de saúde pública de amplo benefício social. No entanto, é imperativo um tratamento cuidadoso desses dados, sob risco de prejuízos aos indivíduos que tiveram suas informações coletadas. O aumento de crimes cibernéticos, como os baseados em técnicas de phishing, evidencia essa preocupação, ou, de forma mais simples, o vazamento de dados com informações sigilosas.

Diversas técnicas de anonimização têm sido propostas e empregadas na literatura para permitir a disponibilização de dados com preservação de privacidade. De forma geral, essas técnicas podem ser organizadas em diferentes paradigmas. Abordagens baseadas em generalização e agregação, como o k-anonimato e a microagregação, reduzem a precisão ou agrupam registros a fim de ocultar informações individuais sensíveis [Sweeney 2002, Machanavajjhala et al. 2007, Domingo-Ferrer and Mateo-Sanz 2002]. Outra classe relevante compreende técnicas baseadas em perturbação, nas quais as coordenadas originais são modificadas por meio da introdução de ruído ou da alteração de associações, incluindo mecanismos fundamentados em privacidade diferencial [Dwork et al. 2006, Andrés et al. 2013, Turgay et al. 2023]. Essas abordagens visam preservar a utilidade analítica dos dados e reduzir o risco de reidentificação de indivíduos.

Por outro lado, a literatura também documenta a existência de ataques de desanonimização capazes de explorar informações auxiliares para reidentificar registros, mesmo na ausência de identificadores diretos. Entre esses ataques, destacam-se estratégias de ligação direta e probabilística baseadas em proximidade espacial [Narayanan and Shmatikov 2008, de Montjoye et al. 2013], bem como ataques que exploram ambiguidade espacial e indistinguibilidade de localização [Andrés et al. 2013, Shokri et al. 2012]. Estudos empíricos demonstram que tais ataques podem comprometer a privacidade de dados espaciais anonimizados quando os mecanismos de proteção não são cuidadosamente avaliados [Zang and Bolot 2011, El Emam et al. 2011].

Apesar da significativa atenção que o tópico tem recebido na literatura, as propostas de técnicas de anonimização de dados avaliam de forma limitada o impacto da aplicação dessas técnicas nas investigações que são feitas *à posteriori* sobre os dados anonimizados. Em sua maioria, a literatura compreende estudos que agregam resultados prévios para comparar diferentes técnicas em termos de privacidade e utilidade dos dados. Assim, efeitos colaterais da anonimização, principalmente relacionados à perda da qualidade e representatividade dos dados, podem prejudicar investigações independentes e subsequentes (por exemplo, [Ribeiro et al. 2023]) que aplicam técnicas de aprendizado de máquina para previsão de séries temporais a partir de dados anonimizados. Assim, no presente artigo nos concentramos nas seguintes questões de pesquisa:

- Qual o impacto das técnicas de anonimização de dados de geolocalização nas soluções baseadas em aprendizado de máquina para predição de séries e tendências?

- Qual a resiliência das técnicas de anonimização de dados de geolocalização diante de ataques distintos de desanonimização?

A contribuição deste artigo está relacionada a um estudo comparativo entre diferentes técnicas de anonimização aplicadas a dados espaciais, avaliando seu comportamento diante de distintas formas de desanonimização. O estudo busca elucidar até que ponto a privacidade dos indivíduos é protegida em casos de ataques, em cenários em que os dados foram previamente anonimizados. Os resultados obtidos são relevantes para contextos que envolvem dados sensíveis e que demandam proteção à privacidade. Pelo melhor do nosso conhecimento, este é o único estudo primário nesse sentido.

O restante do artigo está organizado da seguinte forma. A Seção 2 apresenta os principais trabalhos relacionados. A Seção 3 descreve os dados utilizados e as técnicas de anonimização investigadas. A Seção 4 detalha os ataques de desanonimização empregados no estudo. Na sequência, a Seção 5 descreve o modelo de ataque adotado para os experimentos, e a SeçãoSeção 6 discute as metologias e riscos de reidentificação associados à divulgação dos dados anonimizados. A Seção 7 apresenta a avaliação experimental das técnicas de anonimização frente aos ataques mencionados. Por fim, a Seção 8 apresentamos as considerações finais e perspectivas de trabalhos futuros.

2. Trabalhos Relacionados

A anonimização de dados vem recebendo crescente atenção devido ao aumento da coleta massiva de informações pessoais, à maior preocupação da sociedade com a privacidade e à pressão regulatória imposta por leis como a LGPD[1] e o GDPR[2]. Esse cenário tem impulsionado um grande número de estudos sobre técnicas de anonimização e sobre ataques de desanonimização, incluindo dados de localização.

Dentre as principais técnicas de anonimização aplicáveis a dados espaciais, destacam-se dois grupos. O primeiro compreende as técnicas de generalização e agregação, que visam reduzir a precisão ou agrupar registros a fim de ocultar as especificidades de dados individuais. Nesse conjunto incluem-se o k-Anonimato, a Microagregação, o uso de grades espaciais como o H3 Grid e o Arredondamento de coordenadas. O segundo grupo abrange as técnicas baseadas em perturbação, nas quais os dados originais são modificados por meio da introdução de ruído ou da alteração de associações, dificultando a reidentificação. Entre essas, destacam-se a Permutação e a Privacidade Diferencial.

No sentido oposto, estão as técnicas de ataque, como o Ataque de Ligação com Conhecimento e a Análise de Ambiguidade Espacial, que buscam reverter ou explorar fragilidades nos mecanismos de anonimização. Essas abordagens — tanto as defensivas quanto as ofensivas — constituem o núcleo deste trabalho, servindo de base para a avaliação comparativa da robustez e da eficácia das estratégias analisadas.

Apresentamos a seguir uma seleção de trabalhos relacionados, escolhidos por sua proximidade com o foco deste artigo. Embora a revisão não seja exaustiva, priorizamos estudos que avaliam tanto mecanismos de proteção quanto a robustez desses mecanismos frente a ataques de reidentificação em dados espaciais. Nem todos adotaram exatamente as mesmas técnicas aqui implementadas, todos os trabalhos revisados têm como objeto central dados de natureza espacial, tornando-os referências diretas para o nosso estudo.

[1]https://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd

[2]https://gdpr.eu/

No contexto da anonimização e desanonimização de dados provenientes de sinais de telefone, Lin *et al.* [Lin et al. 2021] apresentam uma análise detalhada da legislação chinesa. Embora dados supostamente anonimizados possam ser distribuídos com maior liberdade, o trabalho mostra, com base em estudos primários, que os métodos de anonimização comumente utilizados nesse contexto na China podem ser facilmente revertidos, o que permite identificar informações sensíveis, como residência, local de trabalho e até fotografias dos usuários. O estudo, no entanto, não realiza experimentos próprios, fundamentando-se exclusivamente em pesquisas anteriores para discutir os impactos dessas vulnerabilidades na legislação chinesa. De forma semelhante, no estudo secundário de Sampaio *et al.* [Sampaio et al. 2023], é apresentada uma série de técnicas de anonimização, bem como *cases* de desanonimização. O contexto da pesquisa é o cenário de *smart cities*, um ambiente em que a variedade de dados é muito grande, incluindo, naturalmente, dados espaciais. O trabalho reconhece a utilidade desses dados para terceiros, especialmente para aprimorar serviços urbanos, entretanto, conclui, assim como o estudo anterior [Lin et al. 2021], que, mesmo com o uso de técnicas de anonimização, a reidentificação dos indivíduos ainda pode ocorrer. Outro estudo secundário, proposto por Majeed e Lee [Majeed and Lee 2021], apresenta diferentes técnicas de anonimização para dados tabulares e grafos, incluindo métricas de avaliação, mas não aborda técnicas de desanonimização, além de não conduzir nenhum experimento. De forma diferente quanto aos experimentos, Jin *et al.* [Jin et al. 2023] apresentam um estudo secundário que inclui um experimento com diferentes técnicas de anonimização utilizadas para anonimizar trajetórias, bem como ataques nesses mesmos dados, tendo como foco principal a análise do *trade-off* entre privacidade e utilidade dos dados.

Löbner [Löbner et al. 2021] apresenta um caso específico que evidencia a necessidade de desidentificação no contexto de veículos inteligentes, nos quais dados de clima e de *grid* de energia são compartilhados. O autor discute considerações e cuidados específicos para a implementação de técnicas de anonimização nesse cenário, que, no entanto, podem ser generalizados para outros contextos. Por fim, o trabalho propõe um conjunto de *guidelines* para auxiliar na escolha da técnica de anonimização mais adequada. Ainda assim, o estudo não apresenta um experimento prático envolvendo o uso de técnicas de anonimização ou desanonimização.

No caso de dispositivos inteligentes, Semi *et al.* [Park et al. 2021] apresentam, em seu artigo, um estudo de caso que demonstra que dados de GPS coletados por *wearables* podem facilmente levar à identificação do usuário. Mesmo quando algum tipo de mascaramento é aplicado às informações de GPS, a reidentificação ainda é possível por meio de informações contextuais capturadas pelo próprio dispositivo, como e-mail, padrões de uso, metadados e outros. Além disso, o experimento apresentado no artigo não utiliza técnicas avançadas de anonimização, limitando-se a formas simples de ocultação de coordenadas, as quais se mostram insuficientes.

A comunidade brasileira tem contribuído ativamente para a pesquisa em anonimização de *datasets*, incluindo propostas voltadas ao aprimoramento da seleção de parâmetros e ao desenvolvimento de novas técnicas. Coelho *et al.* [Coelho et al. 2024] propõem um método automatizado para a escolha do parâmetro k no k-anonimato, evidenciando, por meio de resultados experimentais positivos, o *trade-off* entre utilidade e privacidade. Em trabalho posterior, Coelho [Coelho et al. 2025] analisa o nível de anonimato do k-anonimato no contexto de aprendizado de máquina. Pimenta [Pimenta et al. 2025], por sua vez, apresenta o algoritmo *GOK*, inspirado no comportamento de gorilas, para ano-

nimização baseada em agrupamento, assim realizando um comparativo de desempenho com abordagens existentes.

Entre os trabalhos discutidos, os estudos secundários são os que mais se aproximam da presente proposta quanto à variedade de técnicas de anonimização e desanonimização. Entretanto, diferentemente da maioria desses estudos, este trabalho conduz uma avaliação experimental comparativa, investigando empiricamente o comportamento das técnicas de anonimização frente a distintos ataques de desanonimização. O estudo de Jin *et al.* [Jin et al. 2023], embora apresente similaridades metodológicas, concentra-se no cenário de trajetórias, enquanto a presente pesquisa adota uma abordagem mais geral sobre dados espaciais. Dessa forma, o trabalho contribui para preencher a lacuna metodológica entre revisões secundárias e experimentação aplicada, com foco em dados espaciais.

3. Materiais e Métodos

Este estudo investiga o impacto de técnicas de anonimização sobre dados espaciais sensíveis no contexto de vigilância epidemiológica urbana, focando na proteção da localização de focos do mosquito *Aedes aegypti*, evitando a identificação precisa de endereços monitorados e preservando a utilidade para a predição de surtos.

Dados georreferenciados são essenciais para ações de controle e planejamento em saúde pública. Porém, coordenadas de alta precisão permitem inferir localizações sensíveis, impondo o desafio de reduzir o risco de reidentificação sem comprometer análises baseadas em padrões espaciais e temporais, para contextualizar o escopo do estudo e sua condução metodológica, destacam-se os seguintes aspectos principais:

Dataset e Definição do Problema. Utilizam-se dados públicos do projeto "Onde Está o Aedes?" (Prefeitura de Porto Alegre)[3], contendo registros georreferenciados de focos de *Aedes aegypti* de 2018 a 2023. Define-se um problema de classificação binária supervisionada para predição de surtos em regiões e períodos futuros, usando dados de 2018–2022 para treinamento e 2023 para teste prospectivo. A utilidade dos dados anonimizados é medida pelo desempenho preditivo, enquanto a proteção é avaliada via ataques de desanonimização, simulando adversários com conhecimento parcial dos dados originais (nas proporções de 1%, 5% e até 10% dos dados originais).

Abordagem Experimental. A abordagem experimental compreende três etapas: (1) aplicação de técnicas distintas de anonimização às coordenadas geográficas, incluindo métodos determinísticos de agregação/transformação espacial e um mecanismo probabilístico baseado em privacidade diferencial; (2) treinamento de modelos preditivos com dados originais e anonimizados, avaliando a capacidade de prever surtos no conjunto de teste de 2023; (3) submissão das versões anonimizadas a ataques de desanonimização, simulando adversários com diferentes níveis de conhecimento auxiliar.Após a aplicação de todas as técnicas de anonimização avaliadas, o número de registros permaneceu inalterado em relação ao conjunto original. Essa preservação do volume de dados assegura que as diferenças observadas nas análises de utilidade e de privacidade sejam atribuídas exclusivamente aos efeitos das transformações espaciais introduzidas por cada técnica, e não a variações no tamanho do conjunto de dados analisado. Os artefatos, códigos, scripts e resultados do presente estudo estão disponíveis publicamente no GitHub[4].

[3] `https://prefeitura.poa.br/sms/onde-esta-o-aedes`

[4] `https://github.com/mariliamatosbiz/ArtigoSBRC`

Considerações Éticas. Embora os dados sejam públicos e sem identificadores diretos, este estudo adota uma abordagem conservadora quanto à privacidade. Dados espaciais de alta precisão podem, por si só, representar informações sensíveis, justificando a aplicação e a avaliação de técnicas de anonimização conforme princípios de proteção de dados e boas práticas em pesquisa científica.

4. Técnicas de Anonimização

As técnicas avaliadas focam na proteção de coordenadas geográficas das armadilhas, selecionadas para abranger diferentes paradigmas: generalização, agregação, perturbação e privacidade diferencial.

4.1. Generalização e Agregação

Generalização consiste na redução da precisão de coordenadas geográficas via arredondamento decimal, limitando a exatidão da localização. Embora simples, reduz o risco de identificação direta ao custo de perda de granularidade espacial [Murthy et al. 2019].

Agregação espacial e microagregação substituem coordenadas originais por valores médios calculados sobre grupos de registros próximos, garantindo que múltiplas inspeções compartilhem uma localização aproximada. Técnicas baseadas em k-anonimato asseguram que cada localização agregada represente pelo menos k registros distintos. Essas abordagens preservam padrões espaciais globais, mas podem impactar a representatividade local, especialmente em regiões com menor densidade de armadilhas.

4.2. Perturbação e Privacidade Diferencial

Perturbação modifica coordenadas geográficas via ruído aleatório, mantendo a estrutura estatística geral dos dados. Entre essas abordagens, a privacidade diferencial destaca-se por fornecer garantias formais de privacidade [Turgay et al. 2023].

Adotou-se um mecanismo de privacidade diferencial aplicado às coordenadas geográficas, baseado na adição de ruído planar Laplace, conforme o conceito de *geo-indistinguishability*. O orçamento de privacidade foi fixado em $\varepsilon = 1.0$, valor que representa um compromisso entre proteção e utilidade, conforme trabalhos relacionados. A aplicação de privacidade diferencial limita formalmente o impacto da presença ou ausência de uma observação individual sobre os dados publicados, dificultando ataques de reidentificação baseados em informação auxiliar disponível ao adversário.

5. Modelo de Predição e Avaliação de Utilidade

Antes de analisar a robustez das técnicas de anonimização frente a ataques, é fundamental avaliar se os dados anonimizados permanecem úteis para tarefas analíticas reais. Esta seção descreve o modelo de predição e a metodologia para avaliar a utilidade dos dados no contexto de predição de surtos de *Aedes aegypti*.

Pipeline de Predição de Surtos. O pipeline foi estruturado integrando informações temporais, espaciais e climáticas. Inicialmente, as coordenadas geográficas das armadilhas foram agrupadas em regiões espaciais via clustering K-Means, permitindo a extração de variáveis regionais representativas da distribuição espacial do vetor. Em seguida, construíram-se variáveis temporais com defasagens (*lags*) e médias móveis, capturando efeitos acumulados e atrasados de dados entomológicos e variáveis climáticas.

Essas características foram utilizadas como entrada para um modelo de aprendizado supervisionado baseado em XGBoost, escolhido por sua robustez e desempenho em séries temporais com dados tabulares. O modelo foi treinado com dados de 2018 a 2022 e avaliado em 2023, configurando um cenário prospectivo realista.

Métricas de Avaliação. Avaliou-se o desempenho mediante métricas de classificação binária, com foco na detecção de eventos raros e críticos, como surtos epidemiológicos. No contexto de vigilância em saúde pública, empregaram-se métricas avaliando não apenas a acurácia global, mas também a capacidade de discriminação e a sensibilidade do modelo. A capacidade discriminativa foi avaliada via AUC-ROC (*Area Under the Receiver Operating Characteristic Curve*), medindo a habilidade do classificador em distinguir entre semanas com e sem surto. Valores próximos a 1 indicam alta capacidade discriminativa; próximos a 0,5 indicam desempenho equivalente ao acaso.

Para avaliar a efetividade na detecção de surtos, utilizaram-se Recall, Precision e F1-score, considerando a classe positiva como ocorrência de surto. Recall mede a proporção de surtos corretamente identificados, sendo particularmente relevante quando a omissão de um evento crítico resulta em impactos significativos. Precision avalia a proporção de previsões positivas correspondendo efetivamente a surtos reais, enquanto o F1-score representa a média harmônica entre Precision e Recall. Adicionalmente, considerou-se a Balanced Accuracy, adequada para conjuntos com desbalanceamento, como a ocorrência de surtos ao longo do tempo. A avaliação seguiu um cenário prospectivo, utilizando dados de 2023 exclusivamente para teste, enquanto os dados anteriores foram empregados para treinamento, permitindo uma análise realista do comportamento do modelo em condições semelhantes às observadas em cenários de uso operacional.

Impacto da Anonimização na Predição. Avaliou-se o impacto das técnicas de anonimização sobre a utilidade dos dados no contexto de predição de surtos. O objetivo é verificar se a aplicação de mecanismos de proteção à privacidade compromete a capacidade do modelo em aprender padrões relevantes e realizar previsões eficazes.

Modelos preditivos idênticos foram treinados com dados originais e anonimizados por diferentes técnicas, mantendo fixos o pipeline de processamento, as variáveis de entrada e os parâmetros do modelo. Assim, variações de desempenho observadas podem ser atribuídas diretamente aos efeitos da anonimização.

Tabela 1. Métricas de desempenho dos modelos preditivos treinados com dados originais e anonimizados (Dados de teste do ano de 2023).

Técnica	AUC	Recall	Prec.	F1	B.Acc.
Original	0.748	0.706	0.857	0.774	0.710
Priv. Dif. ($\varepsilon = 1.0$)	0.706	0.765	0.867	0.812	0.739
Generalização	0.697	0.824	0.778	0.800	0.626
k-anonimato ($k = 2$)	0.697	0.765	0.812	0.788	0.668
Microagregação ($k = 5$)	0.664	0.882	0.789	0.833	0.655
Permutação	0.571	0.882	0.789	0.833	0.655

A Tabela 1 apresenta métricas completas de desempenho. Embora o modelo com dados originais obtenha maior AUC-ROC (0.748), a privacidade diferencial ($\varepsilon = 1.0$) apresenta desempenho competitivo (AUC = 0.706), com melhorias em Recall (+8,4

Técnicas baseadas em agregação e generalização tendem a aumentar a sensibilidade do modelo, resultando em maiores valores de Recall, ao custo de redução moderada na capacidade discriminativa global. Esse comportamento evidencia o *trade-off* entre discriminação e detecção, no qual a anonimização pode favorecer a identificação de eventos

críticos, mesmo introduzindo ruído ou perda de granularidade espacial.

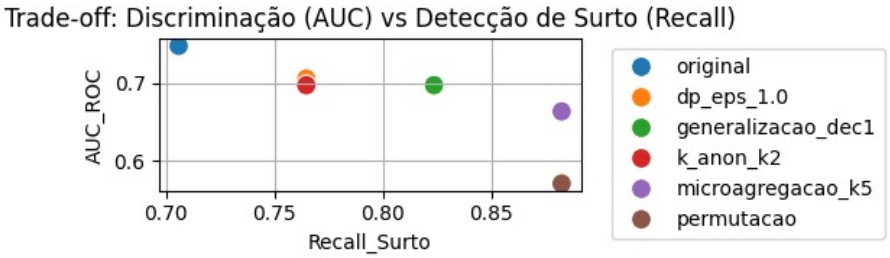

Figura 1. *Trade-off* entre capacidade discriminativa (AUC-ROC) e detecção de surtos (Recall) para modelos com dados originais e anonimizados.

A Figura 1 ilustra o *trade-off* entre AUC-ROC e Recall. Esses resultados mostram que a aplicação de técnicas de anonimização, quando cuidadosamente selecionadas, não inviabiliza o uso dos dados para predição epidemiológica. Em alguns casos, a anonimização pode atuar como regularização implícita, reduzindo a dependência excessiva de padrões espaciais muito específicos e favorecendo a generalização temporal do modelo.

6. Metodologia de Avaliação de Riscos

Descrevem-se metodologias para avaliar riscos de reidentificação associados à divulgação de dados anonimizados, analisando empiricamente o nível de proteção oferecido pelas técnicas quando confrontadas com adversários explorando informações espaciais e temporais. A avaliação é conduzida mediante definição explícita de modelo de ataque e implementação de estratégias alinhadas a esse modelo, considerando diferentes níveis de conhecimento prévio do adversário.

Modelo de Ataque

Assume um adversário com acesso irrestrito aos dados anonimizados e com conhecimento parcial do conjunto original, refletindo situações realistas nas quais dados anonimizados são publicados para pesquisa ou transparência pública, enquanto informações auxiliares podem ser obtidas de outras fontes abertas ou de vazamentos parciais. Especificamente, o adversário possui: (1) acesso completo ao dataset anonimizado; (2) conhecimento de uma fração dos registros originais (1%, 5%, 10%); (3) capacidade de calcular distâncias geográficas e explorar a proximidade espacial; (4) ausência de acesso a identificadores explícitos ou chaves diretas. O adversário não possui conhecimento do mecanismo interno de anonimização, tampouco acesso a dados sensíveis adicionais além de coordenadas geográficas e do tempo de observação. Esse modelo representa um adversário informado, porém não onisciente, alinhado com os pressupostos da literatura de privacidade espacial.

Considera-se que diferentes técnicas alteram a estrutura dos dados de maneiras distintas. Assim, nem todas as estratégias de ataque são aplicáveis a todas as técnicas, adotando-se uma abordagem criteriosa para garantir a validade metodológica. Distribuição das distâncias de deslocamento espacial introduzidas por diferentes técnicas de anonimização, na Figura 6 apresenta a distribuição das distâncias de deslocamento espacial introduzidas por cada técnica de anonimização. Observa-se que as técnicas baseadas em perturbação, em especial a privacidade diferencial e a permutação, produzem distribuições com caudas longas, indicando a ocorrência de deslocamentos espaciais mais expressivos. Em contraste, técnicas baseadas em agregação e generalização concentram os deslocamentos em faixas menores, refletindo uma alteração espacial mais controlada e local.

Estratégias de Ataque para Reidentificação

Para avaliar a robustez das técnicas de anonimização frente a tentativas de reidentificação, foram implementadas estratégias inspiradas em abordagens consolidadas da literatura, explorando diferentes pressupostos de conhecimento e capacidade do atacante. Essas estratégias abrangem desde vínculos diretos entre registros até inferências baseadas em ambiguidade espacial e reconstrução de trajetórias ao longo do tempo:

A1 — Reidentificação direta por vizinhança (NN-Linkage): baseia-se na associação entre registros anonimizados e registros originais a partir da menor distância espacial, sendo uma forma clássica de ataque de ligação direta amplamente discutida na literatura de desanonimização [Narayanan and Shmatikov 2008, de Montjoye et al. 2013]. O atacante busca associar cada registro anonimizado ao registro original mais próximo em termos de similaridade espacial, exclusivamente na proximidade geométrica, é considerado bem-sucedido o ataque quando o registro original correspondente é identificado como o vizinho mais próximo do registro anonimizado.

A2 — Ligação probabilística por conjunto Top-k: generaliza o ataque de vizinhança direta ao considerar um conjunto reduzido de candidatos mais próximos, modelando um adversário capaz de restringir significativamente o espaço de busca mesmo sem reidentificação exata [Narayanan and Shmatikov 2008, de Montjoye et al. 2013].Para cada registro anonimizado, são selecionados os k registros originais mais próximos; um ataque de sucesso ocorre caso o registro verdadeiro pertença a esse conjunto. Essa estratégia modela um atacante capaz de reduzir o espaço de busca, mesmo sem identificação exata.

A3 — Anonimato efetivo por ambiguidade espacial: avalia o anonimato efetivo medindo o número de registros originais plausíveis dentro de um raio de tolerância, conceito alinhado à noção de indistinguibilidade espacial e amplamente utilizado na análise de privacidade de dados de localização [Andrés et al. 2013, Shokri et al. 2012]. Assim sendo, Quanto maior o conjunto de candidatos plausíveis, maior a ambiguidade e menor o risco de reidentificação, medindo a capacidade da anonimização em aumentar a indistinguibilidade espacial. Diversos estudos demonstram que técnicas tradicionais de anonimização espacial podem ser insuficientes frente a adversários com conhecimento auxiliar, permitindo ataques de reidentificação mesmo na ausência de identificadores diretos [Zang and Bolot 2011, El Emam et al. 2011].

A4 — Reconstrução de trajetórias por média temporal: Ataques baseados na reconstrução de trajetórias exploram a consistência temporal de observações anonimizadas para reduzir o efeito de ruído introduzido por mecanismos de perturbação, sendo amplamente discutidos em estudos sobre publicação de trajetórias com preservação de privacidade [Jin et al. 2023]. O atacante explora a continuidade temporal dos dados, estimando a posição real de um indivíduo por meio da agregação estatística de múltiplas observações anonimizadas ao longo do tempo. O ataque é considerado bem-sucedido quando a trajetória reconstruída se aproxima suficientemente da trajetória real, caracterizando um adversário que utiliza séries temporais para reduzir os efeitos do ruído introduzido por mecanismos como permutação e privacidade diferencial. Embora o Ataque A4 seja descrito para fins de completude conceitual, sua avaliação empírica não foi conduzida neste estudo, constituindo uma direção natural para trabalhos futuros.

De modo geral, as estratégias permitem quantificar o risco de reidentificação sob diferentes pressupostos de poder, abrangendo ligações diretas, inferência probabilística, aumento do anonimato por ambiguidade espacial e exploração da consistência temporal.

A Figura 3 apresenta o desvio padrão das coordenadas de latitude e longitude após a aplicação das técnicas de anonimização. Nota-se que técnicas baseadas em agregação reduzem significativamente a variabilidade espacial, indicando maior concentração dos pontos anonimizados. Por outro lado, a privacidade diferencial mantém níveis de variabilidade próximos aos dados originais, preservando propriedades estatísticas globais, ainda que com aumento da incerteza local.

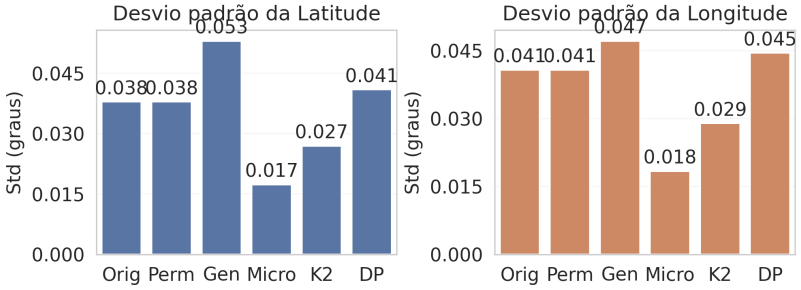

Figura 2. Desvio padrão das coordenadas lat. (a) e long. (b) por técnica.

7. Avaliação Experimental de Robustez

A seguir são apresentados resultados da avaliação de robustez das técnicas frente às estratégias de ataque. A análise verifica se os dados anonimizados permanecem protegidos mesmo sob adversários informados e sob diferentes níveis de vazamento de informação.

Aplicabilidade dos Dados Anonimizados. Verifica-se se os dados anonimizados preservam características estruturais suficientes para uso analítico. As técnicas mantiveram a distribuição espacial global e a coerência temporal, permitindo a utilização em predição de surtos conforme demonstrado na Seção 5. Apesar de introduzirem ruído ou perda de granularidade, não inviabilizaram a construção de modelos preditivos, indicando que a proteção à privacidade não comprometeu completamente a utilidade dos dados.

Robustez frente aos Ataques Apresenta a avaliação de robustez frente às estratégias definidas na Seção 6. O objetivo é analisar se, mesmo sob um adversário informado e sob diferentes níveis de vazamento parcial, os dados anonimizados permanecem protegidos contra tentativas de reidentificação e a redução significativa de anonimato.

Ataques de Ligação Direta e Probabilística

Os ataques A1 (NN-Linkage) e A2 (Top-K) avaliam a capacidade do adversário de reidentificar registros a partir da proximidade espacial entre dados originais e anonimizados. Enquanto o A1 considera apenas o vizinho mais próximo, o A2 generaliza essa estratégia ao permitir que o adversário avalie um conjunto reduzido de candidatos mais próximos.

A Figura 3 apresenta as taxas de sucesso desses ataques em função do vazamento parcial e do raio de correspondência. Observa-se que, no Ataque A1, as probabilidades de reidentificação permanecem extremamente baixas (ordem de 10^{-5}), mesmo sob vazamento de 10% e raios mais permissivos, indicando que a reidentificação exata é improvável no cenário considerado. No Ataque A2, as taxas são ligeiramente superiores (ordem de 10^{-4}), como esperado, porém ainda insuficientes para reduzir o anonimato a um conjunto pequeno de candidatos. Em ambos os casos, técnicas como permutação e privacidade diferencial ($\varepsilon = 1.0$) apresentam comportamento estável frente ao aumento do vazamento, não evidenciando risco significativo de identificação inequívoca.

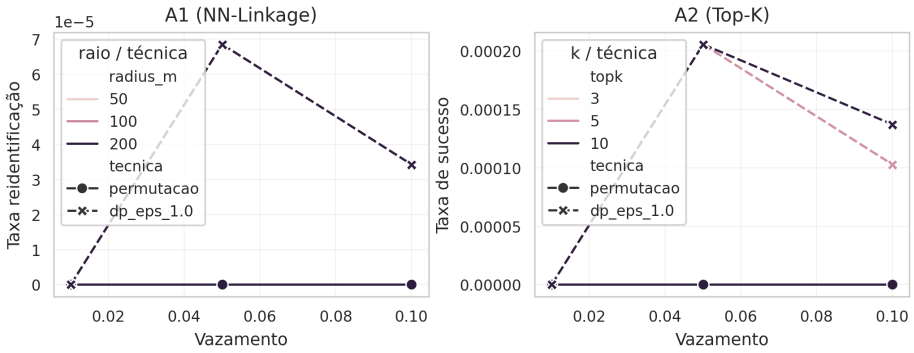

Figura 3. Ataque A1 e Ataque A2

Ambiguidade Espacial

Complementando os ataques de ligação, o Ataque A3 avalia o anonimato efetivo medindo o número de candidatos plausíveis dentro de um raio predefinido. A Figura 4 mostra o número médio de candidatos plausíveis para um raio de 200 m, por técnica. Observa-se que técnicas baseadas em agregação e privacidade diferencial elevam significativamente a ambiguidade espacial, ampliando o conjunto de candidatos potenciais do adversário.

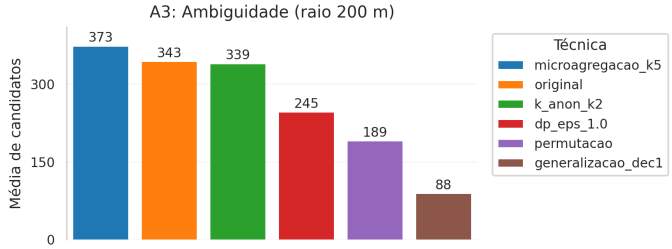

Figura 4. Número médio de candidatos plausíveis por técnica no ataque A3.

Por outro lado, técnicas de generalização apresentam menor ambiguidade, indicando um risco relativo maior em cenários nos quais o adversário explora a proximidade espacial com conhecimento auxiliar. Esses resultados demonstram que as técnicas avaliadas mantêm boa resistência tanto a tentativas de reidentificação direta quanto a estratégias de redução do espaço de busca.

A Figura 5 ilustra mapas de calor da alteração espacial normalizada em relação às coordenadas originais. Técnicas baseadas em agregação preservam a forma espacial global dos dados, enquanto a privacidade diferencial e a permutação promovem maior dispersão espacial. Esses padrões ajudam a explicar os resultados do Ataque A3, no qual técnicas com maior dispersão aumentam o número de candidatos plausíveis, ampliando a ambiguidade espacial enfrentada pelo adversário.

8. Considerações Finais

Este estudo analisou o compromisso entre a proteção da privacidade de dados espaciais sensíveis e a utilidade analítica na predição de séries e tendências, aplicado a dados de geolocalização de vigilância urbana do mosquito Aedes aegypti como estudo de caso. Como contribuição do presente artigo à literatura, complementamos a avaliação quantitativa por uma análise visual do impacto espacial das técnicas de anonimização, permitindo uma interpretação mais clara de sua robustez frente a ataques de reidentificação.

Os resultados indicam que a aplicação adequada de técnicas de anonimização não inviabiliza o desempenho preditivo. Embora o uso de dados originais apresente maior

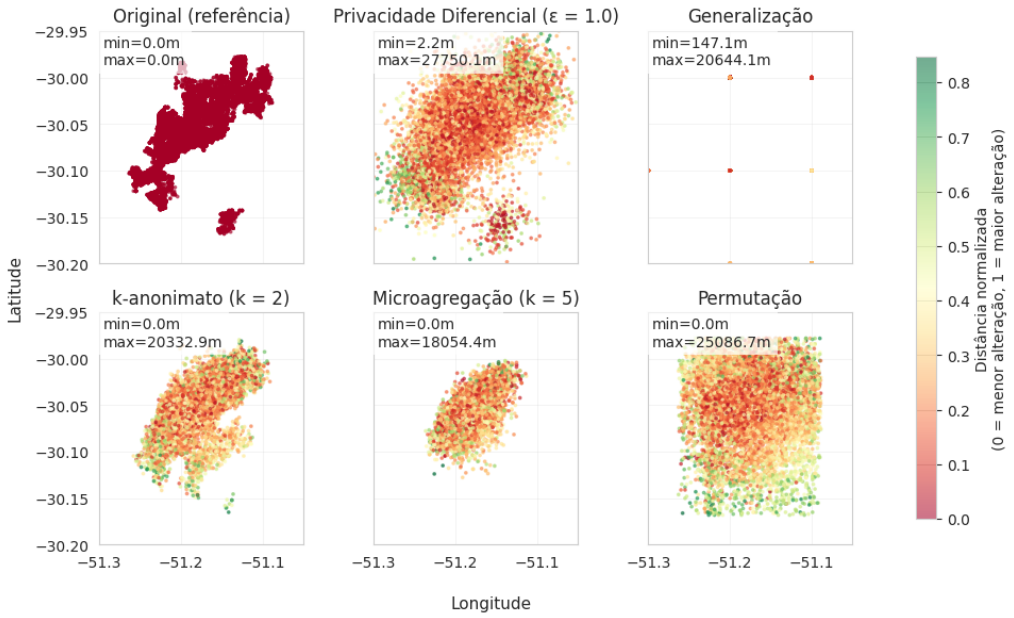

Figura 5. Mapas de calor da alteração espacial em relação às coord. originais.

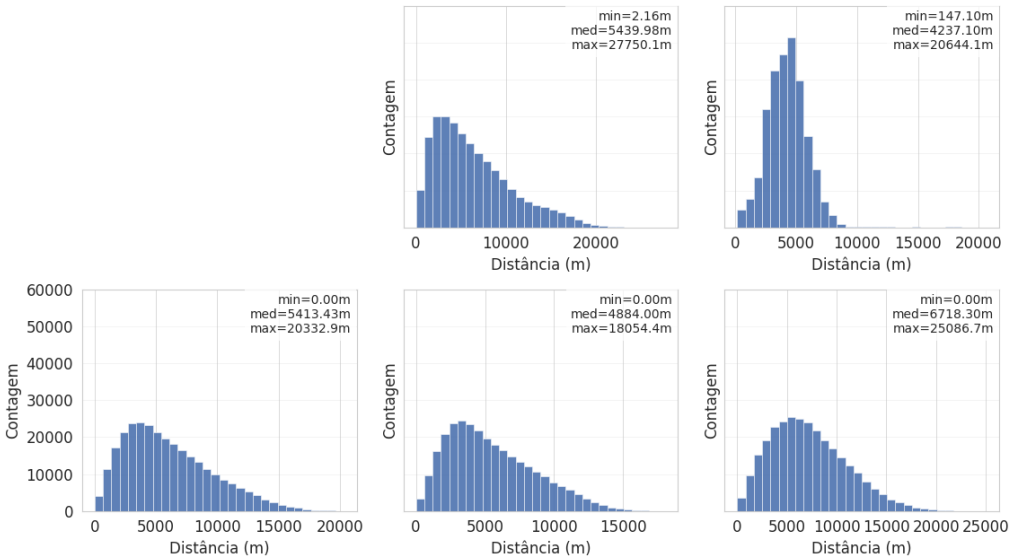

Figura 6. Distribuição das distâncias de deslocamento espacial por técnica.

AUC-ROC, modelos treinados com dados anonimizados mantiveram desempenho competitivo. Em especial, a privacidade diferencial com $\varepsilon = 1.0$ apresentou um equilíbrio favorável entre discriminação e sensibilidade, com ganhos em métricas como Recall e F1-score, sugerindo um efeito de regularização implícita. Do ponto de vista da privacidade, as avaliações empíricas demonstraram resistência significativa às tentativas de reidentificação por meio de ataques de ligação direta, probabilística e de ambiguidade espacial, mesmo sob cenários adversariais informados. Técnicas baseadas em agregação e privacidade diferencial aumentaram substancialmente a incerteza do adversário.

De modo geral, os resultados reforçam que não existe uma técnica de anonimização universal, sendo necessária a consideração conjunta do cenário de aplicação, do modelo de ameaça e dos requisitos de utilidade analítica. No contexto da vigilância epidemiológica urbana, o estudo demonstra que é possível compartilhar e analisar dados

espaciais sensíveis de forma responsável, desde que mecanismos de proteção adequados sejam adotados e avaliados empiricamente no contexto de aplicação.

Referências

Andrés, M. E., Bordenabe, N. E., Chatzikokolakis, K., and Palamidessi, C. (2013). Geo-indistinguishability: Differential privacy for location-based systems. In *ACM SIGSAC Conference on Computer & Communications Security*, pages 901–914. ACM.

Barnabé, S., da Rosa, M. B., et al. (2025). Previsão de surtos de dengue em nível de unidade de desenvolvimento humano (udh) no brasil: Uma abordagem integrada e explicável. In *Escola Regional de Aprendizado de Máquina e Inteligência Artificial da Região Sul (ERAMIA-RS)*, pages 128–131. SBC.

Coelho, K., Okuyama, M., Nogueira, M., Vieira, A., Silva, E., and Nacif, J. (2024). Uma abordagem dinâmica para anonimização de dados de saúde por separatrizes. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 826–839, Porto Alegre, RS, Brasil. SBC.

Coelho, K., Okuyama, M., Nogueira, M., Vieira, A., Silva, E., and Nacif, J. (2025). Metodologia para avaliação da anonimização baseada em k-anonimato nos modelos de aprendizado de máquina. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 742–755, Porto Alegre, RS, Brasil. SBC.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., and Blondel, V. D. (2013). Unique in the crowd: The privacy bounds of human mobility. *Scientific Reports*, 3:1376.

Domingo-Ferrer, J. and Mateo-Sanz, J. M. (2002). Practical data-oriented microaggregation for statistical disclosure control. *IEEE Transactions on Knowledge and Data Engineering*, 14(1):189–201.

Dwork, C., McSherry, F., Nissim, K., and Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography Conference (TCC)*, pages 265–284. Springer.

El Emam, K., Dankar, F. K., Issa, R., Jonker, E., Amyot, D., Cogo, E., Corriveau, J.-P., Walker, M., Chowdhury, S., and Vaillancourt, R. (2011). A systematic review of re-identification attacks on health data. *PLOS ONE*, 6(12):e28071.

Fraccaro, P., Beukenhorst, A., Sperrin, M., Harper, S., Palmier-Claus, J., Lewis, S., Van der Veer, S. N., and Peek, N. (2019). Digital biomarkers from geolocation data in bipolar disorder and schizophrenia: a systematic review. *Journal of the American Medical Informatics Association*, 26(11):1412–1420.

Jin, F., Hua, W., Francia, M., Chao, P., Orlowska, M. E., and Zhou, X. (2023). A survey and experimental study on privacy-preserving trajectory data publishing. *IEEE Transactions on Knowledge and Data Engineering*, 35(6):5577–5596.

Lin, Y., Shen, Z., and Teng, X. (2021). Review on data sharing in smart city planning based on mobile phone signaling big data. *International Review for Spatial Planning and Sustainable Development*, 9(2):76–93.

Löbner, S., Tronnier, F., Pape, S., and Rannenberg, K. (2021). Comparison of de-identification techniques for privacy preserving data analysis in vehicular data sharing. In *ACM Computer Science in Cars Symposium*, New York, NY, USA. ACM.

Machanavajjhala, A., Kifer, D., Gehrke, J., and Venkitasubramaniam, M. (2007). l-diversity: Privacy beyond k-anonymity. In *22nd International Conference on Data Engineering (ICDE)*, pages 24–35. IEEE.

Majeed, A. and Lee, S. (2021). Anonymization techniques for privacy preserving data publishing: A comprehensive survey. *IEEE Access*, 9:8512–8545.

Murthy, S., Abu Bakar, A., Abdul Rahim, F., and Ramli, R. (2019). A comparative study of data anonymization techniques. In *Intl Conference on Big Data Security on Cloud (BigDataSecurity)*, pages 306–309.

Narayanan, A. and Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. In *2008 IEEE Symposium on Security and Privacy*, pages 111–125. IEEE.

Park, S., Kim, R., Yoon, H., and Lee, K. (2021). Data privacy in wearable iot devices: Anonymization and deanonymization. *Security and Communication Networks*, 2021(1):4973404.

Pimenta, I., Araújo, R., Rodrigues, R., Silveira, M., and Gomes, R. (2025). Anonimização de dados para inteligência artificial usando o algoritmo da tropa dos gorilas. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 448–461, Porto Alegre, RS, Brasil. SBC.

Ribeiro, I., Castanheira, L., Schaeffer-Filho, A., Cordeiro, W., and Mota, V. (2020). Caracterização de mobilidade e detecção de comunidades baseadas em tópicos de interesse. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, pages 603–616. SBC.

Ribeiro, I., Castanheira, L., Schaeffer-Filho, A., Cordeiro, W., and Mota, V. (2021). Mobility and community detection based on topics of interest. In *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, pages 1–6. IEEE.

Ribeiro, S. E., Menezes, R. A., Portela, A. L., Araújo, T. P., and Gomes, R. L. (2023). Aplicando redes neurais e análise temporal para predição adaptativa de desempenho de rede. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, pages 490–503. SBC.

Sampaio, S., Sousa, P. R., Martins, C., Ferreira, A., Antunes, L., and Cruz-Correia, R. (2023). Collecting, processing and secondary using personal and (pseudo)anonymized data in smart cities. *Applied Sciences*, 13(6).

Shokri, R., Theodorakopoulos, G., Le Boudec, J.-Y., and Hubaux, J.-P. (2012). Protecting location privacy: optimal strategy against localization attacks. *Proceedings of the ACM CCS*, pages 617–627.

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5):557–570.

Turgay, S., İlter, İ., et al. (2023). Perturbation methods for protecting data privacy: A review of techniques and applications. *Autom. and Machine Learning*, 4(2):31–41.

Zang, H. and Bolot, J. (2011). Anonymization of location data does not work: A large-scale measurement study. In *Proceedings of the 17th Annual International Conference on Mobile Computing and Networking (MobiCom)*, pages 145–156. ACM.