UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

PROGRAMA DE MESTRADO E DOUTORADO EM CIÊNCIA DA COMPUTAÇÃO

MESTRADO ACADÊMICO EM CIÊNCIAS DA COMPUTAÇÃO

RÔNEY REIS DE CASTRO E SILVA

UMA ABORDAGEM DE PRIVACIDADE DIFERENCIAL PARA CONSULTAS SOBRE DADOS RDF NO CONTEXTO DE REDES SOCIAIS

FORTALEZA

2017

RÔNEY REIS DE CASTRO E SILVA

UMA ABORDAGEM DE PRIVACIDADE DIFERENCIAL PARA CONSULTAS SOBRE DADOS RDF NO CONTEXTO DE REDES SOCIAIS

Dissertação apresentada ao Curso de Mestrado Acadêmico em Ciências da Computação do Programa de Mestrado e Doutorado em Ciência da Computação do Centro de Ciências da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Ciências da Computação. Área de Concentração: Banco de Dados

Orientador: Prof. Dr. Javam de Castro Machado

Co-Orientador: Profa. Dra. Vânia Maria Ponte Vidal

FORTALEZA

2017

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

C353c Castro e Silva, Rôney Reis de.
Uma abordagem de Privacidade Diferencial para consultas sobre Dados RDF no contexto de Redes Sociais / Rôney Reis de Castro e Silva. – 2017.
78 f. : il.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Programa de Pós-Graduação em Ciência da Computação, Fortaleza, 2017.
Orientação: Prof. Dr. Javam de Castro Machado.
Coorientação: Prof. Dr. Vânia Maria Ponte Vidal.

1. Preservação de Privacidade. 2. Redes Sociais. 3. Dados Ligados. 4. Resource Description Framework (RDF). I. Título.

CDD 005

RÔNEY REIS DE CASTRO E SILVA

UMA ABORDAGEM DE PRIVACIDADE DIFERENCIAL PARA CONSULTAS SOBRE DADOS RDF NO CONTEXTO DE REDES SOCIAIS

Dissertação apresentada ao Curso de Mestrado Acadêmico em Ciências da Computação do Programa de Mestrado e Doutorado em Ciência da Computação do Centro de Ciências da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Ciências da Computação. Área de Concentração: Banco de Dados

Aprovada em: 27 de Outubro de 2017

BANCA EXAMINADORA

Prof. Dr. Javam de Castro Machado (Orientador)
Universidade Federal do Ceará (UFC)

Profa. Dra. Vânia Maria Ponte Vidal (Co-Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Flávio Rubens de Carvalho Sousa
Universidade Federal do Ceará (UFC)

Prof. Dr. Fábio André Machado Porto
Laboratório Nacional de Computação Científica (LNCC)

À minha família, por sua capacidade de acreditar em mim e investir em mim. Mãe e Pai, vocês foram essenciais para alcançar meus objetivos. Obrigado meu Deus por tudo!

AGRADECIMENTOS

Agradeço primeiramente a Deus que permitiu que tudo isso acontecesse, ao longo da minha vida, em todos os momentos. Agradeço a Universidade Federal do Ceará, seu corpo docente e a administração que oportunizaram a janela que me ajudou a ser quem sou. Ao Departamento de Computação e todos os que contribuíram direta e indiretamente.

Agradeço a todos os professores que à mim forneceram o conhecimento, não apenas racional, mas também de caráter, de formação profissional, por tanto tempo dedicado a mim, não só por terem ensinado, mas por terem me feito aprender. Obrigado a Coordenação Aperfeiçoamento de Pessoal de Núcleo Superior - CAPES, pela ajuda financeira durante os dois últimos anos. Ao Laboratório de Sistemas e Banco de Dados - LSBD, pelo apoio financeiro, material e pessoal. Todos contribuíram de forma muito incisiva na minha formação e no desenvolvimento do meu trabalho.

Ao meu orientador, por toda a paciência que teve comigo. Ao conhecimento passado e orientações. Pela ajuda pessoal, pelo apoio e pela dedicação que me ajudou a chegar aonde eu gostaria de chegar. Obrigado professor, amigo e orientador.

Obrigado a minha namorada e aos meus irmãos, que mesmo em momentos de ausência, momentos de dificuldades, não deixaram de acreditar em mim e de me apoiar. Meus agradecimentos aos meus amigos e a minha família, vocês são tudo na minha vida. A todos que direta ou indiretamente fizeram parte minha formação, o meu muito obrigado.

" Plante um pensamento, colha uma ação; plante uma ação, colha um hábito; plante um hábito, colha um caráter; plante um caráter, colha um destino."

(Stephen Covey)

RESUMO

Em Dados Ligados, informações são representadas por meio da linguagem RDF (*Resource Description Framework*). Uma declaração em RDF consiste de três elementos (uma tripla): sujeito, predicado e objeto. Triplas RDF tomadas em conjunto formam um grafo cujos nós representam recursos e cujas arestas representam propriedades. Em redes sociais, os dados sobre as pessoas e suas relações são potencialmente sensíveis e devem ser tratadas com cuidado, a fim de preservar a privacidade. Simplesmente tornar os dados anônimos, ou seja, mascarar os elementos de identificação, através da anonimização do grafo ou disponibilizar apenas resultados agregados para análises podem não proporcionar proteção suficiente. Neste trabalho, investigamos uma garantia de privacidade forte conhecida como Privacidade Diferencial e como usá-la no contexto de Dados Ligados. Usando a Privacidade Diferencial, propomos uma nova abordagem para garantir a preservação da privacidade em consultas estatísticas para Dados Ligados representados em RDF, cujos os indivíduos e as suas relações influenciam diretamente no resultado da consulta sobre o grafo. Usando técnicas de percorrimento de grafos, demonstramos experimentalmente que a abordagem desenvolvida garante a Privacidade Diferencial. Também desenvolvemos uma estrutura de dados pré-processada, baseada em índices de banco de dados, que permite o cálculo da sensibilidade, uma das entradas para a Privacidade Diferencial, para consultas estatísticas sobre um grafo RDF qualquer. Concluímos analisando a precisão da nossa abordagem através de experimentos com dados reais de redes sociais, avaliando nossas métricas de utilidade dos dados e de tempo de execução. Os resultados comprovam a viabilidade das contribuições para esse tipo de consultas ainda pouco explorado na literatura.

Palavras-chave: Preservação de Privacidade. Redes Sociais. Dados Ligados. Resource Description Framework (RDF). Privacidade Diferencial

ABSTRACT

As the amount of collected information in RDF format grows, the development of solutions for privacy of individuals, their attributes and relationships with others become a more important subject of study. However, privacy solutions are not well suitable for this specific type of data, because they usually do not consider relationships between individuals, which are crucial to semantic data and social networks. Although differential privacy is the most suitable technique for statistical queries, there is still work to be done in this context. This paper presents two main contributions for privacy preserving statistic queries with a relationship as a filter. The first one describes a complete approach to apply ε-differential privacy for linked data and the second one presents an auxiliary data structure and algorithms to efficiently compute parameters for the differential privacy mechanism, i.e. the query's actual value and sensitivity of the data for the given query. We conclude by evaluating our contributions, in real data, presenting utility analysis considering different values of ε as well as performance analysis of our data structure and algorithms.

Keywords: Social Networks. Linked Data. Resource Description Framework (RDF). Differential Privacy

LISTA DE ILUSTRAÇÕES

Figura 1 – Exemplo de tripla RDF. 15
Figura 2 – Exemplo de um grafo com relacionamentos. 17
Figura 3 – Exemplo de situação em que a informação é protegida por um mecanismo. . 18
Figura 4 – Exemplo de rede social representada por um grafo. 22
Figura 5 – Exemplo de RDF representado em um grafo. 25
Figura 6 – Ambiente interativo no modelo de Privacidade Diferencial. 31
Figura 7 – Exemplo de grafos vizinhos em relação às arestas. 33
Figura 8 – Exemplo de grafos vizinhos em relação aos nós. 33
Figura 9 – Exemplo de um grafo contendo relação de *segue*. 37
Figura 10 – Grafos vizinhos gerados a partir do grafo original e suas respectivas respostas da consulta f(contagem). 37
Figura 11 – Grafo com dois triângulos. 42
Figura 12 – Redução de um grafo RDF para uma tabela. 45
Figura 13 – Grafo representando uma rede social com quatro indivíduos. 52
Figura 14 – Conjunto de Dados vizinhos para o grafo da Figura 13. 52
Figura 15 – Visão Geral da Abordagem. 53
Figura 16 – A estrutura de índice. 55
Figura 17 – Visualização da estrutura quando aplicada ao exemplo da Figura 9. 55
Figura 18 – Esquema RDF dos dados de teste (a) e uma instância desse esquema (b). . . 64
Figura 19 – Erro Relativo para dados reais. 66
Figura 20 – Distribuição do erro para conjunto de dados do Facebook. 67
Figura 21 – Distribuição do erro para conjunto de dados do Twitter. 68
Figura 22 – Distribuição do erro para conjunto de dados do Google+. 68
Figura 23 – Relação entre número de nós e arestas, o tempo da computação da sensibilidade (a) e tempo de criação da estrutura auxiliar (b). 69

LISTA DE TABELAS

Tabela 1 – Exemplo de conjuntos de dados vizinhos. 33
Tabela 2 – Cinco possíveis valores de ruído, resposta e probabilidade de ocorrência após a aplicação da Privacidade Diferencial. 38
Tabela 3 – Características dos conjuntos de dados. 63
Tabela 4 – Erro Percentual. 67
Tabela 5 – Desempenho da nossa abordagem para o cálculo da sensibilidade e a construção da estrutura. 69

LISTA DE SÍMBOLOS

ε	Parâmetro de privacidade ε na Privacidade Diferencial é usada para quantificar os riscos de privacidade apresentados após a liberação de resultados estatísticos computados sobre dados sensíveis.

SUMÁRIO

1 INTRODUÇÃO 14
1.1 Motivação 14
1.1.1 Exemplo Prático 17
1.2 Objetivo Geral 19
1.3 Objetivos Específicos 19
1.4 Contribuições 19
1.5 Estrutura da Dissertação 20
2 FUNDAMENTAÇÃO TEÓRICA 21
2.1 Redes Sociais 21
2.2 Dados Ligados 24
2.3 Privacidade de Dados 27
2.4 Privacidade Diferencial 30
2.4.1 Definição Formal 31
2.4.2 Conjunto de Dados Vizinhos 32
2.4.3 Sensibilidade 34
2.4.4 Mecanismo de Laplace 35
2.4.5 Exemplo de utilização da Privacidade Diferencial 36
3 TRABALHOS RELACIONADOS 39
3.1 Anonimização para Grafos 39
3.1.1 Privacy in social networks: A survey 39
3.1.2 Logical Foundations of Privacy-Preserving Publishing of Linked Data . . 40
3.2 Privacidade Diferencial para Grafos 41
3.2.1 Analyzing graphs with node differential privacy 43
3.2.2 Qualitative analysis of Differential Privacy applied over graph structures . 44
3.2.3 Information Privacy for Linked Data 44
3.3 Discussão 46
4 UMA ABORDAGEM DIFERENCIALMENTE PRIVADA PARA RDF DE REDES SOCIAIS 51
4.1 Visão Geral 51
4.2 Etapa de pré-processamento 54

4.2.1 *Estrutura de dados auxiliar* 54
4.2.2 *Criação e povoamento da estrutura* 55
4.3 **Etapa 1: Processamento das consultas** 57
4.4 **Etapa 2: Mecanismo de privacidade** 60
4.5 **Etapa 3: Validação e resposta da consulta** 61
4.6 **Discussão** 61
5 **RESULTADOS** 62
5.1 **Ambiente de experimentação** 62
5.2 **Análise da Utilidade dos Dados** 64
5.3 **Análise de Desempenho** 67
5.4 **Conclusão** 70
6 **CONSIDERAÇÕES FINAIS** 71
6.1 **Conclusão** 71
6.2 **Trabalhos Futuros** 72
REFERÊNCIAS 73

1 INTRODUÇÃO

1.1 Motivação

Em decorrência da facilidade de acesso a dispositivos computacionais por organizações e usuários, a quantidade de dados coletados e publicados cresceu em grandes proporções nos últimos anos. Uma grande parte desses dados são originados da interação entre indivíduos, através de aplicações de redes sociais que geram um grande volume de informações. Além disso, esses dados são semanticamente ricos, proporcionando grandes oportunidades para a realização de análises. Como exemplo, podemos citar a análise do comportamento de indivíduos e suas interações dentro de uma rede social de pesquisadores de áreas distintas a partir de dados disponibilizados publicamente.

Apesar de diversas empresas, governos e instituições de pesquisa realizarem esforços em disponibilizar seus dados, apenas uma quantidade pequena desses dados são publicados em relação ao montante produzido. Por exemplo, dados sobre doenças e tratamentos médicos, por serem bastante sensíveis, não podem ser publicados. Isso significa que estes dados não podem ser acessados por outros especialistas ou pesquisadores, diminuindo consideravelmente as possibilidades de descobertas de novos tratamentos. Assim, a disponibilização de informações é essencial como o primeiro passo para produção de conhecimento.

Para publicar dados é preciso evitar que dados sensíveis dos indivíduos sejam publicados de forma indevida. Por um lado dados precisam ser publicados, mas por outro lado não deve ser possível determinar o indivíduo que cedeu o dado. Por conta da riqueza de informações, a representação dos dados pessoais pode dar margem para associação dos dados a um indivíduo, acarretando inúmeras consequências como a discriminação do seu titular por se referirem, por exemplo, à opção sexual, convicções religiosas, filosóficas e morais, ou até mesmo opiniões políticas. Formalmente, segundo a Lei de Proteção de Dados do Parlamento e do Conselho Europeu (EUROPEU, 2017), dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como os dados relativos à saúde e à vida sexual, incluindo os dados genéticos, são considerados dados sensíveis.

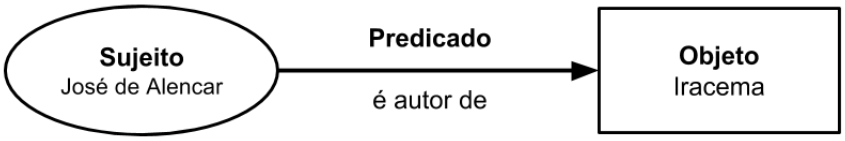
Todo e qualquer dado relativo a indivíduos, pelo potencial discriminatório que apresentam, devem ser melhor protegidos e manipulados de forma adequada. Por exemplo, através de dados publicados pela rede estadual de saúde seja descoberto que um determinado

indivíduo é portador do vírus HIV. Até então esta uma informação não conhecida por nenhum familiar do indivíduo. Quais seriam as consequências caso essa informação fosse exposta publicamente? Isso seria, no mínimo, uma violação à privacidade e constrangedor para esse indivíduo.

Em redes sociais a exposição de informações é vasta. Milhares de publicações todos os dias com bilhões de usuários ativos. As pessoas utilizam todos os dias ferramentas de conversação e outros tipos de iterações sociais. Normalmente, em busca de se comunicar com outras pessoas em seus convívios sociais ou mesmo em busca de conhecer novas pessoas. Muitas vezes postam suas vidas pessoais, relações, planos, informações trabalhistas, fotos e vídeos, não pensando nas consequências que tudo isso pode acarretar. Diante de tanta exposição, abre-se caminho para que usuários maliciosos descubram informações pessoais, potencialmente sensíveis, e possam agir de má fé. Se uma empresa que administra esses dados deseja publicar informações sobre seus usuários, ela precisa tomar muito cuidado para evitar qualquer provável identificação de seus usuários e suas informações sensíveis.

Como forma de disponibilização de dados, a iniciativa de dados ligados define as melhores práticas para publicação e interconexão de dados na Web usando RDF (*Resource Description Framework*) para representar os dados (VIDAL *et al.*, 2016). Ao invés do formato tradicional de armazenamento de dados formado por um conjunto de tuplas, o conjunto de dados é modelado como triplas (sujeito-predicado-objeto) que podem ser representadas como um grafo, visando melhor expressar informações e relacionamentos do mundo real. Veja, na Figura 1, como pode ser representado a informação de que José de Alencar é o autor do livro Iracema.

Figura 1 – Exemplo de tripla RDF.



Fonte: Elaborado pelo autor

A Figura 1 mostra apenas uma declaração. Em situações reais, a quantidade de declarações é muito maior, são centenas ou milhares de declaração expostas publicamente. À medida que a quantidade de informações coletada em RDF cresce, pode-se observar também o crescimento no número de possibilidades de descoberta de informações, seja por pesquisadores ou por usuários maliciosos. Nesse trabalho, focamos em manter a privacidade das pessoas no

cenário em que grande volumes de dados são publicados seguindo o formato descrito pelo RDF.

Nesse cenário, desenvolver soluções que garantam a privacidade de indivíduos, de seus atributos e das suas relações com outros usuários, torna-se uma questão ainda mais importante à medida que coletamos mais dados e também publicamos mais informações. Suponha que uma empresa provedora de uma rede social deseja publicar seus dados sobre as interações de seus clientes para que esses dados possam auxiliar pesquisadores a criar e desenvolver novas ideias. Para isso, a empresa precisa garantir que todas as informações sensíveis sobre seus clientes não sejam associadas ao indivíduo.

Devido a questões de privacidade, não é possível publicar os dados na sua forma original, apenas remover os identificadores explícitos (por exemplo, nome e CPF) não é suficiente para garantir a privacidade dos indivíduos (SWEENEY, 2002; BRITO; MACHADO, 2017). É necessário proteger efetivamente a privacidade dos usuários de redes sociais e evitar que eventuais ligações do indivíduo a uma informação sensível, em um processo de re-identificação ocorram. Porém isso deve ser realizado de forma que ainda se preserve a utilidade dos dados para análise. A proteção dos dados para fins de garantia de privacidade geralmente ocorre de duas maneiras. A primeira consiste na aplicação de técnicas de anonimização tais como generalização e supressão (BRANCO JR *et al.*, 2014). Essas técnicas tem como objetivo a remoção de identificadores explícitos e a substituição por valores mais gerais dos semi-identificadores. Por exemplo, suprime-se o nome e RG e, ao invés de publicar a rua, publica-se apenas o nome do bairro. A segunda forma consiste em liberar apenas informação estatística (informação agregada), sem revelar o conteúdo destes dados, nem mesmo o resultado específico da consulta originalmente realizada.

Entretanto, aplicar técnicas de anonimização ou liberar apenas resultados agregados não fornece garantias suficientes de privacidade, devido a um possível e imprevisível conhecimento prévio relacionado a outras fontes de informações de um atacante (BACKSTROM *et al.*, 2007; TASK; CLIFTON, 2012). Para lidar com esse problema, um dos modelos de privacidade mais aceitos na literatura é a Privacidade Diferencial. A Privacidade Diferencial é um modelo matemático que aplica algum mecanismo gerador de ruídos aleatórios à resposta de uma dada consulta, gerando perturbações nos dados suficientes para esconder a identidade dos indivíduos e preservar utilidade nos dados. Como a maioria das soluções de privacidade, a Privacidade Diferencial foi proposta inicialmente para dados tabulares ou dados no formato de tuplas, portanto ainda há muita investigação científica a ser realizada quando se pretende utilizar

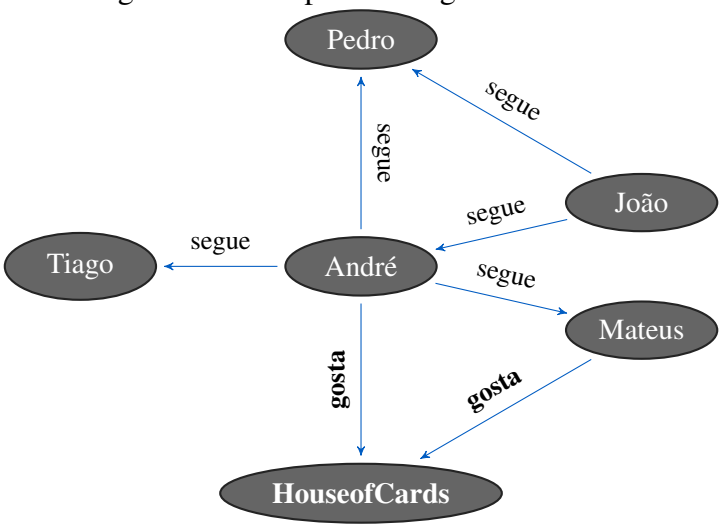
esse mecanismo para dados representados em RDF. Trazer esse modelo de privacidade para ambiente de dados ligados torna-se um grande desafio com ótimas oportunidades de pesquisa e desenvolvimento de novas soluções.

Após revisão criteriosa da literatura relacionada à aplicação da privacidade diferencial para dados RDF (ARON, 2013; FUNG *et al.*, 2010a; GRAU; KOSTYLEV, 2016), não foi encontrado trabalhos que considerassem a interdependência dos relacionamentos entre os indivíduos, aspectos comumente representados em redes sociais. Este trabalho propõe uma abordagem sistemática, prática e eficiente para garantir a Privacidade Diferencial sobre dados RDF em consultas de contagem que consideram as relações entre os indivíduos. Experimentos com dados reais de redes sociais foram conduzidos para validar a contribuição. Os resultados foram analisados a partir da perspectiva de preservação de utilidade com diferentes níveis de privacidade. Também foi analisado o desempenho da abordagem proposta.

1.1.1 Exemplo Prático

Como exemplo, considere a rede social representada na Figura 2. São 6 perfis: Tiago, André, Pedro, João, Mateus e *HouseOfCards*, ligados pela relação *gosta* e *segue*, que não são recíprocos, caracterizados por suas preferências pessoais.

Figura 2 – Exemplo de um grafo com relacionamentos.



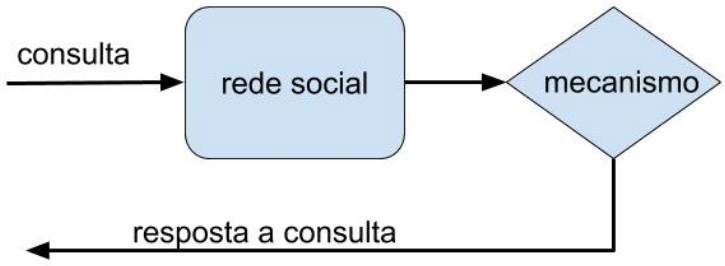
Fonte: Elaborado pelo autor

Imagine a situação em que se deseja disponibilizar informações relevantes sem comprometer a integridade do usuários dessa rede. Para entender a garantia e o que se necessita

proteger, imagine a situação em que uma empresa esteja interessada em descobrir quantos perfis seguem pelo menos uma pessoa que gosta de *HouseofCards*. Se o gosto de filmes é uma informação sensível, o que fazer? Seria seguro enviar essa informação a empresa interessada? Só seria seguro enviar a resposta se houvesse certeza de que a informação enviada não possibilite que um usuário mal intencionado aprenda (com qualquer probabilidade) qualquer nova informação sobre as preferências pessoais dos usuários da rede.

Existem diversas pesquisas relacionadas ao tema da preservação de privacidade dos dados para que esse tipo de situação seja evitado. Uma solução bastante viável seria utilizar um mecanismo onde as respostas são verificadas, modificadas ou até mesmo removidas antes de que a parte interessada receba a resposta a suas consultas. Veja a representação dessa situação na Figura 3.

Figura 3 – Exemplo de situação em que a informação é protegida por um mecanismo.



Fonte: Elaborado pelo autor

Dois perfis satisfazem a consulta: André e João. Se André for removido ou desconsiderado da rede social, nenhum perfil irá satisfazer a consulta. Perceba que a presença ou ausência desse perfil tem bastante impacto na resposta dessa consulta, pois possui forte influência na resposta da consulta. Para garantir a privacidade diferencial dos cinco perfis do grafo é necessário computar o valor da sensibilidade que é a medida do maior impacto causado na remoção ou adição de um determinado indivíduo no conjunto de dados. Ou seja, a sensibilidade mede o quanto um usuário impacta no resultado de um consulta. Porém, para um conjunto de dados reais de redes sociais o número de indivíduos é grande. Computar o valor da sensibilidade considerando cada um dos n indivíduos do conjunto de dados é uma tarefa custosa. São necessárias $n+1$ consultas – uma para cada conjunto de dados que difere de um indivíduo (conjunto de dados vizinhos).

1.2 Objetivo Geral

Esta dissertação propõe uma solução para o problema de garantia de privacidade de dados em redes sociais por meio de consultas diferencialmente privadas sobre dados RDF de redes sociais que considere o relacionamento entre indivíduos. A estratégia da solução busca processar a sensibilidade do indivíduo no grafo de representação dos dados RDF, além de projetar estruturas de dados de apoio para agilizar o cálculo do resultado dessas consultas.

1.3 Objetivos Específicos

Como forma de atender ao objetivo geral deste trabalho, estabelecemos os seguintes objetivos específicos:

- Investigar técnicas de privacidade de dados para dados RDF no contexto de redes sociais;
- Redefinir a noção de sensibilidade de elementos em dados explicitamente interligados numa estrutura de grafo;
- Criar uma estrutura de dados auxiliar para tornar o processo eficiente do cálculo da sensibilidade;
- Avaliar experimentalmente as contribuições propostas utilizando dados reais em termos de utilidade e desempenho.

1.4 Contribuições

Como resultado desta dissertação, foi definida e descrita uma abordagem completa que permite a realização de consultas que possuem relacionamentos entre os indivíduos como referência. Ainda, para prover eficiência para a abordagem, foi proposta uma estrutura de dados auxiliar para computação da resposta real e da sensibilidade, bem como as definições necessárias para extrair os dados RDF que irão povoá-la.

Como resultado direto das contribuições científicas alcançadas com a realização dessa pesquisa, o seguinte artigo foi publicado:

- RÔNEY REIS C. SILVA, BRUNO C. LEAL, FELIPE T. BRITO, VÂNIA M. P. VIDAL, JAVAM C. MACHADO. A Differentially Private Approach for Querying RDF Data of Social Networks. Em: *21st International Database Engineering & Applications Symposium - IDEAS*, p. 74–81, 2017.

No decorrer do trabalho de investigação, os resultados parciais dessa pesquisa

contribuíram indiretamente na publicação dos seguintes artigos:

- ELISEU C. BRANCO JR., RÔNEY REIS C. SILVA, JAVAM C. MACHADO, JOSÉ MARIA MONTEIRO, GABRIEL G. MELO, THIAGO DE SOUSA GARCIA, RICARDO J. LIMA JÚLIO TAVARES, ANGELO BRAYNER. Uma Ferramenta para Assegurar a Confidencialidade de Dados em Serviços de Armazenamento em Nuvem. Em: *Sessão de Demonstrações do XXXII Simpósio Brasileiro de Banco de Dados - SBBD (Prêmio de Melhor Demonstração)*, 2017.
- ELISEU C. BRANCO JR., JOSÉ MARIA MONTEIRO, RÔNEY REIS C. SILVA, JAVAM C. MACHADO. A New Mechanism to Preserving Data Confidentiality in Cloud Database Scenarios. Em: *Livro Enterprise Information Systems: 18th International Conference, ICEIS 2016, Rome, Italy, April 25–28, 2016, Revised Selected Papers (SPRINGER)*, p. 261-283, 2017.
- ELISEU C. BRANCO JR., JOSÉ MARIA MONTEIRO, RÔNEY REIS C. SILVA, JAVAM C. MACHADO. A New Approach to Preserving Data Confidentiality in the Cloud. Em: *Proceedings of the 20th International Database Engineering & Applications Symposium - IDEAS*, p. 256-263, 2016.
- ELISEU C. BRANCO JR., JOSÉ MARIA MONTEIRO, RÔNEY REIS C. SILVA, JAVAM C. MACHADO. A Flexible Mechanism for Data Confidentiality in Cloud Database Scenarios. Em: *18th International Conference on Enterprise Information Systems - ICEIS*, p. 359-368, 2016.

1.5 Estrutura da Dissertação

Este trabalho encontra-se estruturado da seguinte forma: No capítulo 2 são apresentados os principais conceitos necessários para a compreensão desse trabalho. Os trabalhos relacionados são discutidos no capítulo 3, destacando-se suas contribuições e limitações. No capítulo 4 é apresentado a contribuição proposta deste trabalho. No capítulo 5 descrevemos os experimentos e a avaliação de seus resultados. Por fim, no capítulo 6, apresentamos as conclusões e indicações de possíveis trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são abordados os conceitos fundamentais para o desenvolvimento deste trabalho. Dentre eles destacam-se as características das redes sociais, Seção 2.1, os conceitos de Dados Ligados, seu formato, características e suas aplicações, Seção 2.2, as definições em torno da preservação de privacidade de dados, Seção 2.3 e, por fim, aspectos relacionados ao modelo de Privacidade Diferencial, utilizado na abordagem proposta para garantir a privacidade de indivíduos quando consultas são realizadas em uma base de dados, Seção 2.4.

2.1 Redes Sociais

Redes sociais são sistemas online que interconectam usuários. Elas representam um espaço onde as pessoas se relacionam virtualmente e compartilham informações entre si, como fotos, mensagens, vídeos, etc. Exemplos como Twitter, LinkedIn e Facebook tornam-se cada vez mais populares (AGGARWAL, 2011). O Facebook é considerado a maior rede social do mundo, com uma média de 1,32 bilhões de usuários ativos diariamente (outubro de 2017) (FACEBOOK, 2017). Já o Twitter é um serviço de microblogging com mais de onze anos de existência, comanda mais de 328 milhões de usuários (julho de 2017) (TECH, 2017). O LinkedIn é uma rede social de negócios lançada em 2002 e que hoje possui mais de 500 milhões de usuários (outubro de 2017) (LINKEDIN, 2017). Ela é considerada a maior rede profissional do mundo. Semelhante ao Facebook e Twitter, o Google Plus é uma rede social e um serviço de identidade mantido pela empresa Google Inc. Ele possui significativamente menos popularidade que as outras três redes sociais citadas, porém possui cerca de 395 milhões de membros ativos (setembro de 2017) (BRAIN, 2017). Muitas dessas redes sociais são extremamente ricas em conteúdo e dados de relacionamentos entre seus usuários, que podem oferecer inúmeras oportunidades para a análise de dados.

Dados de redes sociais podem ser modelados por grafos, onde os indivíduos são representados por vértices e os relacionamentos entre eles por arestas. Cada indivíduo pode conter um ou mais atributos. Atributos são as propriedades, qualidades ou características dos indivíduos, por exemplo, idade, cor do cabelo ou mesmo seu CPF. Esses atributos também podem caracterizar atitudes, opiniões e comportamentos, como a posição política ou convicções religiosas. Por outro lado, as relações equivalem às conexões entre indivíduos, isto é, as relações

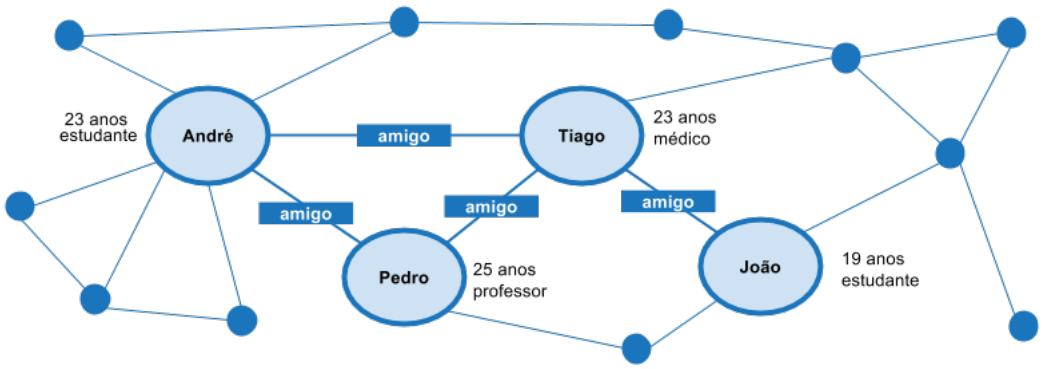
estabelecidas entre dois ou mais indivíduos. Alguns exemplos de relações em redes sociais são: relações de amizade; relações entre grupos de indivíduos; relações entre indivíduos e eventos; entre outras.

Formalmente, uma rede social modelada por um grafo $G = (V, E, A, R)$ possui:

- V conjunto de vértices, que representam os indivíduos nele contidos;
- E conjunto de arestas, ou seja, relacionamentos entre indivíduos, tal que E é um par (v, w), onde v e $w \in V$ representa que uma aresta conecta dois vértices.
- A conjunto de atributos, que consistem em propriedades, qualidades ou características dos indivíduos;
- R conjunto de rótulos, que estão relacionados à descrição dos relacionamentos entre os indivíduos.

Por exemplo, considere a rede social de "amigos pessoais" exemplificada na Figura 4. Cada vértice na rede representa um indivíduo. Cada vértice possui atributos do tipo idade e profissão. Uma aresta representa uma conexão entre duas pessoas que são amigas pessoais, estabelecendo uma relação de amizade entre ambas. Nesse exemplo, André possue 23 anos, é estudante e amigo de Tiago, que por sua vez possue 23 anos, é médico e amigo de João.

Figura 4 – Exemplo de rede social representada por um grafo.



Fonte: Elaborado pelo autor

Embora as redes sociais, como o Twitter, o Facebook e o Google+, tenham um papel relevante em nosso cotidiano, elas podem apresentar sérios riscos de violação à privacidade dos seus usuários. Muitas vezes, informações contidas em redes sociais estão disponíveis publicamente, tais como data de nascimento, endereço de e-mail, número de telefone, endereço residencial, etc. À medida que as redes sociais são extremamente populares, elas favorecem ataques por parte dos usuários mal intencionados. Por esse motivo, a invasão de privacidade e o

roubo de dados das redes sociais, bem como potencial exploração comercial dessas redes por terceiros, tendem a crescer. Medidas que contribuam para amenizar, evitar ou eliminar os riscos de violações de privacidade ganham importância cada vez mais.

Observe que, mesmo que não haja exposição de informações definidas como privadas, nenhum fato impede que ocorram violações de privacidade nesse contexto. Algumas vezes dados que não são rotulados como privados podem ter uma implicação de privacidade em um contexto diferente quando associados a informações colhidas de outras fontes. Por exemplo, o CEP de um indivíduo geralmente não é considerado privado pois não há mapeamento explícito e publicamente disponível contendo as informações pessoais de um indivíduo específico. No entanto, se um hospital publica informações com base no CEP de seus pacientes, o CEP deve ser considerado privado.

À medida que os usuários utilizam as redes sociais, faz-se necessário atentar para os riscos de violação de privacidade envolvidos. Nesse contexto, existem três tipos de ameaça à privacidade dos indivíduos: divulgação de identidade (*identity disclosure*), divulgação de atributos (*attribute disclosure*) e divulgação por meio de ligação social (*social link disclosure*).

A divulgação de identidade ocorre quando um adversário é capaz de determinar o mapeamento de um determinado perfil na rede social para uma entidade específica do mundo real. Por exemplo, um atacante que conheça os atributos únicos de um indivíduo poderia combiná-los com outros atributos observados de um determinado perfil na rede social. Dessa forma, o atacante possui maneiras de calcular a probabilidade de cada atributo que pertença a um indivíduo. Já a divulgação de atributos ocorre quando um atacante é capaz de determinar o valor de um atributo sensível de um indivíduo. Atributos sensíveis são atributos que contêm informações sensíveis sobre os indivíduos (BRANCO JR *et al.*, 2014), por exemplo, o salário, os exames médicos ou os lançamentos do cartão de crédito. Dessa forma, esse tipo de ataque ocorre quando o valor de um atributo pode ser associado a um indivíduo. Esse atributo pode ser um atributo do próprio indivíduo ou dos relacionamentos com os outros indivíduos. Por outro lado, a divulgação por meio de ligação social ocorre quando um adversário é capaz de descobrir a existência de uma relação sensível entre dois usuários, ou seja, uma relação que estes usuários gostariam que permanecesse escondida da sociedade. Por exemplo, a divulgação de que duas pessoas possuem um relacionamento amoroso. Neste trabalho apresentamos uma abordagem para diminuir os riscos de descoberta de informações a partir de dados ligados de redes socias.

2.2 Dados Ligados

Dados Ligados, também conhecidos como *Linked Data*, referem-se a um conjunto de princípios e técnicas para disponibilização de informações estruturadas na Web. Dados Ligados são considerados como um tipo de estrutura de dados interconectada que vem se popularizando ao longo dos últimos anos (FILHO; LÓSCIO, 2015). Esse tipo de dados abrange quase todos os tipos de informações, ou seja, informações estatísticas, redes sociais, informações climáticas, etc. Por exemplo, o projeto DBPedia tem por objetivo extrair conteúdo estruturado das informações da Wikipédia e disponibilizá-lo na Web de forma estruturada, seguindo os conceitos de Dados Ligados.

Através dos princípios de Dados Ligados podemos construir um modelo de dados genérico que integra diversas fontes de dados. Presente em diversos ramos de aplicação, sua utilização continua crescendo principalmente devido ao fato de que os dados estão interligados em uma rede maciça de informações. Grandes representantes como Facebook, Twitter e Google+ estão trabalhando para introduzir semântica em suas informações a fim de facilitar o desenvolvimento de ferramentas por terceiros e permitir novos tipos de aplicações. Por exemplo, hoje é possível utilizar sua *Application Programming Interface* (API) para extrair informações de seus usuários e interligá-las com os dados da DBPedia que sejam relevantes para agregar valor à informação retornada.

Dados ligados também facilitam a recuperação de informações para que essas informações possam ser utilizadas como uma parte do conhecimento acumulado sobre um determinado assunto Por exemplo, pode-se extrair de uma rede social que um grupo de amigos são membros do atual congresso de medicina e, a partir do conjunto de dados do *DBpedia*, descobrir outras informações como o local, data, tema do evento, outras pessoas que frequentaram o mesmo evento, e assim por diante. Os dados publicados na Web possuem significados explicitamente definidos e podem ser processados por máquinas ou podem estar ligados a outras fontes de dados. Quanto mais informações, conceitos, objetos, pessoas, locais estiverem conectados, mais poderosa será a rede de Dados Ligados. Consequentemente, esse enorme conjunto de dados conectados pode trazer problemas maiores de integração, organização, segurança e privacidade.

O criador da Web Semântica e do conceito de Dados Ligados, Tim Berners-Lee (SHADBOLT *et al.*, 2006), estabeleceu quatro grandes princípios para se trabalhar com Dados Ligados:

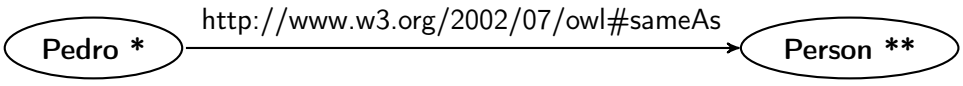
- Usar URIs como nomes para as “coisas” (recursos) disponibilizadas na Web;

- Usar URIs HTTP para que as pessoas ou máquinas possam procurar e acessar esses nomes, usando o protocolo HTTP.
- Quando alguém procurar uma URI, devem ser providas informações úteis, utilizando padrões como RDF, SPARQL, entre outros.
- Incluir links para outras URIs, de modo que possa permitir a descoberta de mais informações.

Esses princípios fornecem uma base para a disponibilização e interligação de dados estruturados na Web. Os principais formatos utilizados para disponibilizar dados estruturados são: JSON, XML, CSV e RDF. O RDF é um formato recomendado pela *World Wide Web Consortium* (W3C) para representar as informações. Esse formato é um modelo de dados descentralizado, baseado em grafo. Ele também é extensível, com um alto nível de expressividade, permitindo a interligação entre dados de diferentes fontes. A estrutura de uma expressão em RDF é dada por uma coleção de triplas, onde cada tripla é formada por um sujeito, um predicado e um objeto. Ela também pode ser definida por dois ou mais nós e arestas direcionadas para representar o predicado como um link entre dois nós. Um nó pode representar um sujeito ou um objeto.

Por exemplo, a Figura 5 apresenta uma declaração em RDF de que Pedro é uma pessoa. Nesse exemplo, existem duas fontes de dados distintas: DBPedia e UFC/OWL. O recurso que identifica o indivíduo Pedro na fonte DBPedia está ligado ao recurso que o identifica na fonte UFC/OWL, onde um recurso é qualquer "coisa" do mundo real identificada por um endereço Web. A propriedade *http://www.w3.org/2002/07/owl#sameAs* define que os recursos interligados representam a mesma entidade do mundo real. Nesse exemplo, vemos que uma especificação de domínio neutra (*sameAs*) é utilizada para descrever um determinado recurso (*Pedro*) a partir de uma fonte distinta (*Person*). A mesma especificação pode ser utilizada em diferentes domínios, mas ainda ser processada pelos mesmos analisadores RDF, isto é, a mesma especificação pode ser reaproveitada em uma outra aplicação e reprocessada por qualquer ferramenta que atue sobre dados RDF.

Figura 5 – Exemplo de RDF representado em um grafo.



∗ http://dbpedia.org/resource/Pedro
∗∗ http://www.ufc.br/owl/resource/person/2017

Fonte: Elaborado pelo autor

Código-fonte 1 – Exemplo de RDF representado em RDF/XML.

```
<rdf:RDF
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
  xmlns:w3="http://www.w3.org/2002/07/owl">
  <rdf:Description rdf:about="http://dbpedia.org/resource/Pedro">
    <w3:name>Pedro</w3:name>
    <w3:sameAs rdf:resource="http://www.ufc.br/owl/resource/person/2017
        "/>
  </rdf:Description>
</rdf:RDF>
```

Fonte: Elaborado pelo autor

A mesma declaração representada na Figura 5 pode ser modelada no formato RDF/XML (Código Fonte 1), e ainda sim possuir o mesmo significado.

A extensão do vocabulário base do RDF, denominado *RDF-Schema* (ou RDF-S) é a especificação que define classes, propriedades e seus relacionamentos e que pode ser utilizada para descrever triplas. Ela é utilizada na definição de *tags* e na estrutura hierárquica de triplas representada em RDF. Tags são marcações de texto simples, atribuídas a um recurso Web, e que geralmente descrevem alguma característica de um recurso associado na Web. Essas características fornecem elementos base para a descrição de ontologias, conhecida como *Web Ontology Language* (OWL). A OWL é uma linguagem desenvolvida e recomendada pelo W3C que descreve um domínio em termos de classes, propriedades e indivíduos. A OWL pode incluir ricas descrições das características de objetos para que programas possam compreender e responder a consultas de agentes (pessoas ou outros programas) por meio do uso de descrições ontológicas (BECHHOFER, 2009) (HORROCKS, 2005). Atualmente, a OWL é a linguagem mais utilizada para definição de ontologias na Web (ISOTANI; BITTENCOURT, 2015). Ela possui variantes da linguagem que lidam com a escalabilidade e expressividade das ontologias. Toda ontologia criada em OWL possui uma estrutura sintática mandatória que é baseada em RDF. Além do documento RDF, é possível criar documentos OWL com diferentes formas de serialização. Serialização é o processo de tradução de documento OWL em um RDF que possa ser armazenado ou processado. Hoje em dia, existem vários formatos de serialização em uso, dentre eles: N3, Turtle e N-Triplas. Todos esses formatos podem ser aplicados para codificar um RDF. Tais formatos também possuem uma organização lógica das triplas semelhantes e a sintaxe é o que define o interpretador apropriado. Neste trabalho realizamos nossa experimentação

utilizando o formato N3, que é o mais compacto e legível dos três apresentados.

Consultas sobre Dados Ligados podem ser realizadas através da linguagem SPARQL (PRUD *et al.*, 2006). SPARQL é uma linguagem de consulta para recuperação de informações contidas em RDF ou mesmo representada em um grafo RDF, semelhantes às consultas realizadas em SQL. Ela é a mais utilizada para este fim e recomendada pela W3C. No entanto, SPARQL não é somente uma linguagem de consulta declarativa, mas também um protocolo utilizado para enviar consultas e recuperar resultados através do protocolo HTTP (CLARK *et al.*, 2007). Além disso, SPARQL permite realizar consultas sobre diversas fontes de dados interligadas e que podem estar armazenadas em um banco de dados de triplas (*triple store*), ou seja, um banco de dados relacional com um esquema de mapeamento para RDF. O mais comum e padrão na comunidade é o uso de banco de dados de triplas.

O SPARQL também admite uma série de filtros e operadores que permitem executar consultas complexas sobre o conjunto de triplas armazenadas. Diversos bancos de dados de triplas oferecem pontos de acesso via Web (URLs), que aceitam o protocolo SPARQL e sua linguagem de consulta. Dessa forma, é possível interagir e integrar com diferentes fontes de dados, utilizando-se de um padrão comum, beneficiando a comunidade que usufrui dessas informações.

O presente trabalho visa proteger a privacidade de dados em redes sociais no contexto de Dados Ligados, a partir de consultas na sintaxe do SPARQL sobre RDF. Para oferecer garantias fortes de privacidade ao resultado das consultas, modelos de privacidade de dados são definidos a seguir.

2.3 Privacidade de Dados

Todas as pessoas têm o direito de manter o seu espaço pessoal, livre de interferências de outras pessoas ou mesmo de organizações. Cabe a cada pessoa zelar pelo seu espaço e decidir sobre o controle de suas informações, decidindo quem deve ter o controle, aonde poderão ser usadas e disponibilizadas e em que momentos isso pode ocorrer. Existem dois conceitos que podem confundir por serem muito semelhantes: segurança e privacidade. Ambos os termos possuem concepções parecidas, mas significados distintos. Quando se trata de dados, a segurança visa regular e restringir o acesso a dados durante todo o ciclo de vida do dado, enquanto a privacidade define restrições ao administrador dos dados sobre o que deve ser exposto e como será realizado esse acesso, na maioria das vezes com base em leis e políticas de privacidade.

Neste ponto, também surge o conceito de controle de acesso como forma de fornecer segurança a um conjunto de dados. O controle de acesso refere-se a regras específicas de quem está autorizado a acessar (ou não) determinados recursos, isto é, quando um conjunto de usuários está apto a acessar um conjunto de dados. Neste trabalho, tratamos de maneiras prática e objetiva a privacidade dos dados.

Quando usuários lidam com Dados Ligados, eles podem indagar se as questões de privacidade levantadas até agora diferem em qualquer aspecto significativo em relação às preocupações introduzidas nas práticas "tradicionais" de disponibilização de informações pessoais. Práticas tradicionais incluem o armazenamento de dados através de registros em bancos de dados e sua disponibilização em diversos formatos, por exemplo via XML. Preocupações de privacidade associadas a Dados Ligados têm muitas características comuns às preocupações tradicionais utilizadas na captura, armazenamento e troca de informações pessoais. Afinal, ambas as técnicas dependem do uso de tecnologias para gravar, armazenar e trocar informações, como o uso de grandes espaços de armazenamento para gravar dados.

Quando se trata de divulgação dos dados, os atributos podem ser classificados como identificadores e semi-identificadores. Identificadores são atributos que identificam unicamente os indivíduos, por exemplo, CPF, nome, número da identidade. Por outro lado, semi-identificadores são dados que podem ser combinados com informações externas e assim utilizados para reidentificar indivíduos. Dessa forma, um adversário poderá descobrir que o registro no conjunto de dados publicado pertence a um indivíduo com uma probabilidade alta de descoberta. Isso pode levar a sérios riscos de violação de privacidade por causa do uso não autorizado de informações sensíveis pertencentes aos indivíduos. Para solucionar esse tipo de problema, uma estratégia simples seria a não publicação dos dados para qualquer finalidade (WONG; FU, 2010). Entretanto, isso poderia comprometer as análises das informações por terceiros. Este tipo de análise fornece embasamento para a tomada de decisões estratégicas em governos, organizações, instituições, etc. Além disso, torna-se possível a detecção e análise de padrões e tendências para a sociedade. A não publicação desses dados dificultaria o possível crescimento dessas entidades.

Anonimizar os dados antes de qualquer disponibilização (FUNG *et al.*, 2010b) tem sido uma boa estratégia para solucionar o problema da preservação de privacidade de dados em redes sociais. Nesse contexto, uma abordagem convencional para anonimizar dados é a remoção dos identificadores explícitos de indivíduos, como nome, CPF, e-mail, etc. do conjunto de dados antes de uma publicação. Contudo, simplesmente remover esses identificadores não é

suficiente para proteger a privacidade dos indivíduos devido à existência dos semi-identificadores (SWEENEY, 2002).

Em um processo de anonimização, um conjunto de dados original D é transformado em um novo conjunto D', por meio de modificações. Como forma de preservar a utilidade de D deve-se assegurar que o mínimo de modificações deva ser gerado na anonimização, uma vez que, essas modificações podem gerar distorções em relação ao conjunto de dados original. A distorção causada por um processo de anonimização é denominada perda de informação. O objetivo desse processo é evitar a descoberta de informações sensíveis por usuários maliciosos com o mínimo de perda de informação. Técnicas de anonimização como a generalização, supressão e perturbação produzem um conjunto de dados D' menos preciso que o conjunto original D, no entanto ambos os conjuntos diferem no quesito perda de informação e também na proteção da privacidade ocasionada por cada técnica.

Na técnica de generalização, os valores dos atributos que são considerados semi-identificadores são substituídos por valores semanticamente semelhantes, porém menos específicos. Já a técnica de supressão de dados é uma estratégia a qual valores em um conjunto de dados são removidos ou substituídos por algum valor especial, possibilitando a não descoberta de semi-identificadores por adversários. Por exemplo, substituir o nome por um caractere especial. Por outro lado, a perturbação tem sido comumente utilizada em controle de descoberta estatística (IYENGAR, 2002) devido à sua simplicidade, eficiência e capacidade de preservar informações estatísticas. A ideia geral dessa técnica é substituir os valores dos atributos semi-identificadores originais por valores fictícios, de modo que informações estatísticas calculadas a partir dos dados originais não se diferenciem significativamente de informações estatísticas calculadas anteriormente sobre os dados perturbados.

A partir das técnicas de anonimização, diferentes modelos de privacidade sintáticos surgiram com o passar dos anos, por exemplo: ***k*-anonimato** (SWEENEY, 2002), ***l*-diversidade** (MACHANAVAJJHALA *et al.*, 2006), ***t*-proximidade** (LI *et al.*, 2007), etc. Esses modelos têm como objetivo estabelecer uma determinada condição a qual os dados devem satisfazer, após um processo de anonimização. Desse modo, operações de generalização e/ou supressão sobre os dados devem ser realizadas até que uma condição sintática seja atendida, de modo que o conhecimento do adversário torne-se restrito à descoberta de atributos sensíveis a partir de semi-identificadores.

Esses modelos de privacidade sintáticos foram surgindo ao longo do tempo para

resolver limitações encontradas nos modelos vigentes da época. Por exemplo, l-diversidade surgiu como forma de sanar uma limitação do k-anonimato, provendo proteção contra ataques de ligação ao atributo. Entretanto, apesar dos avanços e melhorias, os modelos sintáticos podem não ser adequados para determinados contextos, dependendo do risco concreto a ser mitigado. Todos eles demonstraram ser vulneráveis a ataques de uma forma ou de outra. Por exemplo, para situações em que considera-se que um adversário possua algum conhecimento prévio (*background knowledge*) sobre os dados originais (BACKSTROM *et al.*, 2007; TASK; CLIFTON, 2012). No entanto, nos últimos anos surgiu um novo modelo, chamado Privacidade Diferencial (CYNTHIA, 2006), que diminuiu os diversos tipos de riscos de privacidade.

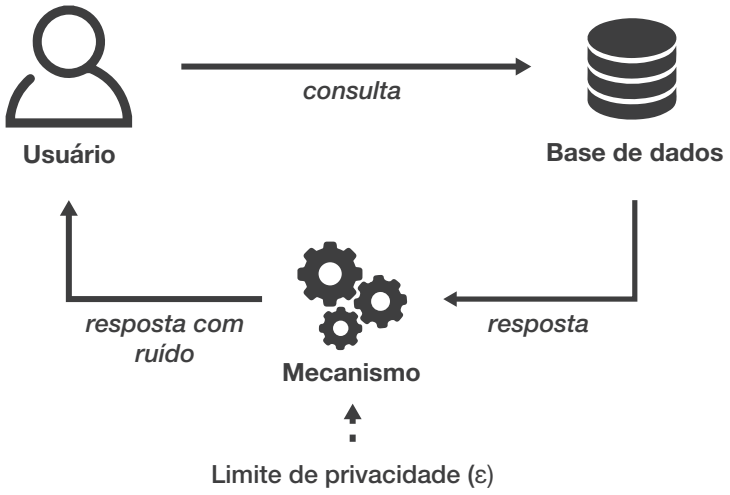
2.4 Privacidade Diferencial

A Privacidade Diferencial é um modelo matemático que oferece garantias sólidas de privacidade. Ela investiga a ideia de fornecer resultados de consultas estatísticas de modo que ruídos sejam adicionados a esses resultados. Em outras palavras, os dados provenientes de consultas são perturbados para garantir a privacidade dos indivíduos. Assim, um usuário malicioso não poderá identificar um indivíduo com 100% de certeza. A Privacidade Diferencial exige que as chances de ocorrência de resultados sejam essencialmente iguais, independentemente da presença de qualquer indivíduo no conjunto de dados.

A Privacidade Diferencial é satisfeita por um algoritmo aleatório, também chamado de mecanismo. O objetivo deste modelo é fornecer informações estatísticas sobre um conjunto de dados sem comprometer a privacidade de seus usuários. Este modelo foi projetado em um ambiente interativo, onde os usuários submetem consultas a um conjunto de dados, que por sua vez responde por meio de um mecanismo de anonimização. Este ambiente interativo é mostrado na Figura 6.

O ambiente interativo mostrado na Figura 6 funciona da seguinte forma: uma consulta é realizada por um usuário sobre uma base de dados e a resposta da consulta é absorvida por um mecanismo de privacidade. O mecanismo então gera um certo ruído que é adicionado a resposta da consulta. Após a adição do ruído, a resposta com ruído é retornada ao usuário.

Figura 6 – Ambiente interativo no modelo de Privacidade Diferencial.



Fonte: Elaborado pelo autor

2.4.1 Definição Formal

O propósito da Privacidade Diferencial é garantir a privacidade de seus indivíduos, utilizando-se de um mecanismo κ. Um mecanismo κ é um algoritmo aleatório que produz uma certa quantidade de ruído que é adicionado a resposta de uma consulta. Formalmente:

Definição 1 *Um mecanismo κ provê ε-Privacidade Diferencial se para todos os conjunto de dados D_1 e D_2 que diferem no máximo em um elemento, e para todo S contido na variação de resultados de κ, isto é, para todo $S \subseteq Range(\kappa)$,*

$$Pr[\kappa(D_1) \in S] \leq exp(\varepsilon) \times Pr[\kappa(D_2) \in S],$$

onde a probabilidade é tomada sobre a aleatoriedade de κ e $exp(\varepsilon)$ é a exponencial do parâmetro de privacidade ε.

A Privacidade Diferencial requer que a probabilidade Pr de uma consulta em D_1 deve diferir por um fator multiplicativo $exp(\varepsilon)$. Isso ocorre quando a consulta é aplicada sobre um conjunto de dados original D_1 e comparada à probabilidade de responder o mesmo valor aplicado ao conjunto de dados vizinho D_2. Em outras palavras, isso implica que a adição ou remoção de um indivíduo no conjunto de dados não afetará significativamente o resultado da consulta de qualquer análise estatística realizada no mesmo conjunto de dados (DOMINGO-FERRER *et al.*, 2016).

A definição formal de Privacidade Diferencial não determina a escolha do valor do parâmetro ε. Esse parâmetro não possui correlação explícita com a privacidade dos indivíduos,

como nas técnicas de anonimização sintáticas. O valor de ε depende da consulta que está sendo realizada e dos próprios dados que estão no conjunto de dados. Alguns trabalhos (DWORK, 2008; DWORK; SMITH, 2010; LEE; CLIFTON, 2011) consideram que o valor de ε deve ser pequeno, como por exemplo, 0.01, 0.1 ou até $ln2$ ou $ln3$. Quanto menor o valor de ε, maior a privacidade. Ajustá-lo de forma muito alta faz com que a confidencialidade dos dados diminua, isto é, existe maiores possibilidades de descoberta de informações confidenciais. Por outro lado, ajustá-lo de forma muito baixa faz com que as respostas obtidas não sejam mais úteis, isto é, a quantidade de ruído gerada será muito maior e, consequentemente, a resposta obtida será muito diferente da resposta real. Dessa forma a escolha do valor de ε deve ser experimental e algumas vezes encontrada empiricamente. Portanto, para cada mecanismo, deve ser feita uma análise para escolher o parâmetro adequado utilizando métricas (NGUYEN *et al.*, 2013) para avaliar a precisão da resposta do mecanismo com diversos valores de ε (LEE; CLIFTON, 2011).

A Privacidade Diferencial foi definida em um modelo interativo, onde o usuário submete consultas a um mecanismo e esse fornece uma resposta ε-Diferencialmente Privada. No entanto, existem diversas formas de se atingir a Privacidade Diferencial através de um mecanismo. Nosso objetivo então é aplicar um mecanismo κ que irá adicionar um ruído adequado para produzir uma resposta a uma consulta f feita pelo indivíduo. A quantidade de ruído necessária depende do tipo que consulta f e de como ela varia com o conjunto de dados. Para entender essa variação, precisamos definir o que é a sensibilidade de um conjunto de dados D. Pela definição surge o conceito de conjuntos de dados vizinhos.

2.4.2 Conjunto de Dados Vizinhos

Por definição, dois conjuntos de dados D_1 e D_2 são vizinhos se eles diferem em uma unidade. Formalmente, D_1 e D_2 são vizinhos se $D_1 = D_2 \cup \{x\}$ ou $D_2 = D_1 \cup \{x\}$, isto é, um conjunto de dados é um subconjunto do outro com tamanho menor, em uma unidade.

Definição 2 *Dado um conjunto de dados D, todos os conjuntos de dados D_i decorrentes da remoção de um indivíduo i do conjunto de dados original D são definidos como vizinhos.*

Por exemplo, considere o conjunto de dados D na Tabela 1a. Um de seus vizinhos pode ser obtido pela remoção do registro de ID $= 2$, resultando na Tabela 1b, uma vez que não houve alterações nos valores dos registros.

Tabela 1 – Exemplo de conjuntos de dados vizinhos.

ID	Nome	Idade	Profissão
1	Andre	23	estudante
2	Mateus	25	advogado
3	João	19	estudante
4	Pedro	25	professor

(a)

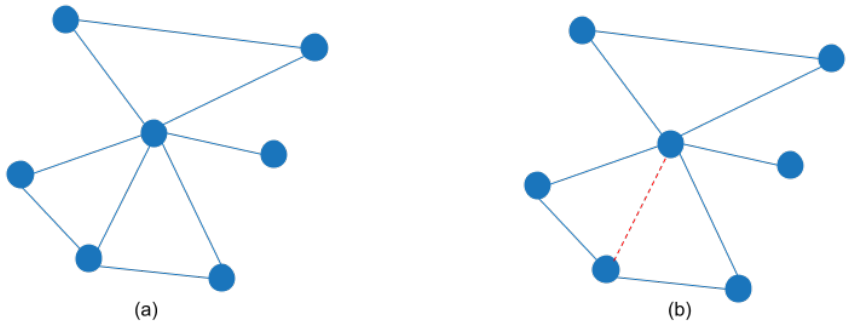
ID	Nome	Idade	Profissão
1	Andre	23	estudante
3	João	19	estudante
4	Pedro	25	professor

(b)

Fonte: Elaborado pelo autor

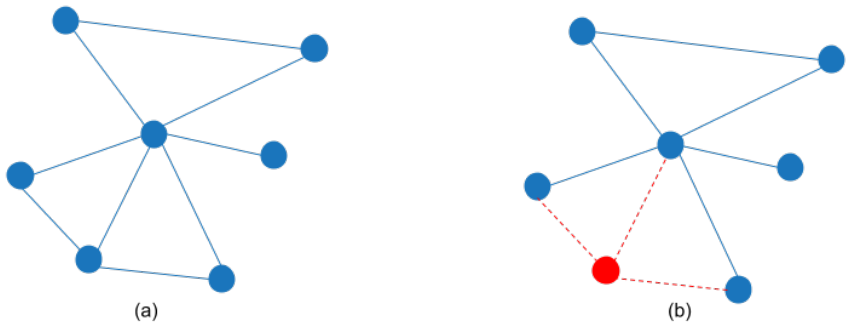
Para dados tabulares, D_1 e D_2 são vizinhos quando diferem em um registro. A unidade diferenciadora é um registro no banco de dados. Já para dados em RDF, são propostas duas interpretações (KASIVISWANATHAN *et al.*, 2013) para diferir um grafo vizinho do outro: vizinhos em relação aos nós (*node privacy*) e vizinhos em relação às arestas *edge privacy*. Ou seja, um grafo G_1 é vizinho de G_2 se diferem em um nó ou em uma aresta.

Figura 7 – Exemplo de grafos vizinhos em relação às arestas.



Fonte: Elaborado pelo autor

Figura 8 – Exemplo de grafos vizinhos em relação aos nós.



Fonte: Elaborado pelo autor

Intuitivamente, a Privacidade Diferencial relativa às arestas, representada na Figura

7, deve garantir que o resultado não revele a inclusão ou remoção de uma aresta particular do grafo. Isso significa que estamos ocultando a presença ou a ausência de uma certa propriedade de um indivíduo ou mesmo uma relação entre dois indivíduos. A Privacidade Diferencial em relação aos nós, representada na Figura 8, oculta a inclusão ou remoção de um nó junto com todas as arestas adjacentes. Ou seja, adicionar ou remover um nó do grafo significa ocultar a presença ou ausência de um indivíduo no grafo.

2.4.3 Sensibilidade

Um conceito importante também no contexto de Privacidade Diferencial é o conceito de sensibilidade do resultado (CYNTHIA, 2006). A sensibilidade, uma das entradas para o modelo, é o maior impacto causado ao remover ou adicionar um indivíduo no conjunto de dados para o resultado de uma determinada consulta. Para calcular a sensibilidade para uma determinada consulta, é necessário considerar todos os possíveis conjuntos de dados vizinhos. A sensibilidade então irá medir quanta diferença um usuário faz ao ser removido (ou adicionado) no conjunto de dados na resposta da função de consulta. Isso é fundamental para o cálculo adequado do ruído a ser adicionado pelo mecanismo, uma vez que, quanto maior o valor da sensibilidade, maior quantidade de ruído deve ser adicionado à resposta do mecanismo para mascarar a remoção de um indivíduo, de forma a assegurar sua privacidade (DOMINGO-FERRER *et al.*, 2016).

Existem definições distintas em relação a sensibilidade. Uma medida de sensibilidade é a sensibilidade global, que é a diferença máxima entre o resultado de uma consulta em dois possíveis conjunto de dados vizinhos, conforme a definição adiante:

Definição 3 *Seja D o domínio de todos os conjuntos de dados. Seja f uma função de consulta que mapeia conjuntos de dados a vetores de números reais e para todos $x, y \in D$. A sensibilidade global SG da função f é:*

$$SG_f = \max_{x,y \in D; d(x,y)=1} \| f(x) - f(y) \|$$

A sensibilidade global SG_f de uma função f é a máxima diferença $\| f(x) - f(y) \|$ para todo x pertencente a D, y diferindo de no máximo um elemento. Outra definição de sensibilidade é a sensibilidade local (NISSIM *et al.*, 2007; DWORK; LEI, 2009), que é a diferença máxima entre os resultados da consulta sobre o verdadeiro banco de dados e qualquer vizinho dele. Formalmente:

Definição 4 *Seja D o domínio de todos os conjuntos de dados. Seja f uma função de consulta que mapeia conjuntos de dados a vetores de números reais e para um x ∈ D. A sensibilidade local SL da função f em x é:*

$$SL_f(x) = \max_{y \in D; d(x,y)=1} \| f(x) - f(y) \|$$

A sensibilidade local SL_f de uma função f em um conjunto de dados x é a máxima diferença de $\| f(x) - f(y) \|$ para todo y, tal que y difere de x em pelo menos um elemento. Observe que SL_f depende de uma instância y de x. A sensibilidade local é muitas vezes menor do que a sensibilidade global, uma vez que é uma propriedade do banco de dados única e verdadeira, ao invés de considerar o conjunto de todos os possíveis bancos de dados. Por isso, neste trabalho, consideramos a sensibilidade local e a denotamos simplesmente por sensibilidade.

Essa noção se estende naturalmente ao caso dos dados de grafo, desde que a sensibilidade seja definida da mesma forma que ela é conceituada na Privacidade Diferencial para dados tabulares. O trabalho (NISSIM *et al.*, 2007) define a sensibilidade em termos da privacidade em relação aos nós e às arestas para um grafo G, definida a seguir:

Definição 5 *Para uma função f que mapeia conjuntos de dados D a vetores de números reais e um grafo G ∈ D, a sensibilidade de f em G é definida por*

$$S_f(G) = \max_{G'} \| f(G) - f(G') \|$$

onde o máximo é ocupado por todos os vizinhos G' de G em relação ao nós.

2.4.4 Mecanismo de Laplace

Um mecanismo de privacidade é um algoritmo que introduz uma certa quantidade de ruído à resposta original de uma consulta sobre uma base de dados. Dessa forma, ele garante a privacidade de dados ao introduzir aleatoriedade às respostas de diferentes consultas. Um dos mecanismos mais adotados para aplicação da Privacidade Diferencial é o *Mecanismo de Laplace*. O mecanismo de Laplace envolve a adição de ruído aleatório que está em conformidade com a distribuição estatística de Laplace. Dada uma função f em um domínio D que leva o subconjunto de todos os elementos de D até um elemento do conjunto dos números reais $\Re$, o mecanismo de Laplace. $\kappa_f(D) = f(D) + Laplace(\Delta f/\varepsilon)$ provê ε-Privacidade Diferencial, onde Δf é:

Definição 6 *(DWORK, 2008) Seja D o domínio dos possíveis conjunto de dados e f uma consulta, o valor real da consulta é dado por $f(D)$. Temos, então, que a sensibilidade da função é:*

$$\Delta f = \max_{D_1,D_2} = \| f(D_1) - f(D_2) \|_1$$

para todo D_1, D_2 que diferem em no máximo um indivíduo.

O Mecanismo de Laplace é o método mais comum e simples para alcançar a Privacidade Diferencial. A adição de ruído é baseada na geração de uma variável aleatória da distribuição de Laplace com média μ e escala b da seguinte forma:

$$Laplace_{\mu,b}(x) = \frac{1}{2b}\exp(-\frac{|x|}{b})$$

A distribuição de Laplace é uma versão espelhada e assim simétrica da distribuição exponencial. Para fazer a variável contínua e, consequentemente, diferencialmente privada, a distribuição é gerada com média centrada em 0. Podemos então definir formalmente o mecanismo de Laplace:

Definição 7 *Dada uma função de consulta $f : D \to \Re$, o mecanismo de Laplace M:*

$$M_f(D) = f(D) + Laplace(0, \Delta f/\varepsilon)$$

fornece ε-Privacidade Diferencial. Onde $Laplace(0, \Delta f/\varepsilon)$ retorna uma variável aleatória da distribuição de Laplace com média zero e escala $\Delta f/\varepsilon$.

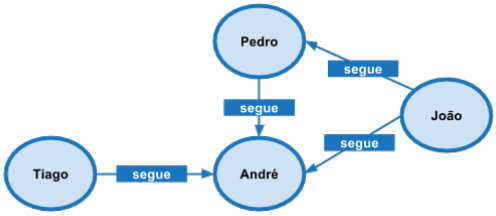
2.4.5 Exemplo de utilização da Privacidade Diferencial

Considere o seguinte exemplo de utilização da Privacidade Diferencial em pequena escala. Ele contém a relação *segue*, conforme a figura 9.

Seja f uma consulta que conta a quantidade de indivíduos que seguem alguém. Suponha que f seja aplicada sobre o grafo representado na Figura 9. Para aplicar a Privacidade Diferencial sobre esses dados é necessário calcular f para cada vizinho do conjunto original. A resposta real da consulta é 3, ou seja, 3 indivíduos seguem alguém, são eles: Tiago, Pedro e João. A Figura 10 mostra os conjuntos de dados vizinhos gerados a partir do grafo original pela eliminação de cada um dos nós e suas respectivas respostas da consulta f.

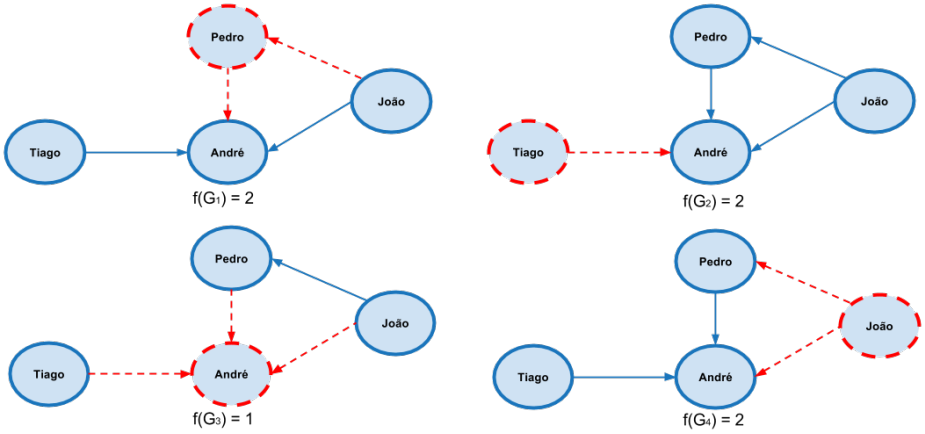
Para garantir a privacidade acerca de um indivíduo, ele participando ou não do conjunto de dados, é preciso calcular a variação máxima que a ausência do indivíduo provoca

Figura 9 – Exemplo de um grafo contendo relação de *segue*.



Fonte: Elaborado pelo autor

Figura 10 – Grafos vizinhos gerados a partir do grafo original e suas respectivas respostas da consulta f(contagem).



Fonte: Elaborado pelo autor

no resultado da consulta. Essa variação é proveniente da remoção do André, pois, conforme vemos na Figura 10, tem a menor resposta da consulta f. Isso quer dizer que remover o André causa a maior variação na resposta da consulta. Em seguida, é necessário calcular a sensibilidade da consulta aplicada ao conjunto de dados. Conforme definida nesta seção, a sensibilidade é calculada pela maior diferença $|f(G) - f(G')|$ e ocorre quando removemos o indivíduo André, pois gera como resultado $|3-1| = 2$. Por fim, o ruído a ser adicionado pelo mecanismo para atender ao modelo de Privacidade Diferencial, utilizando um mecanismo de Laplace, deve ser igual a $Laplace(0, \frac{2}{\varepsilon})$, aplicando a Definição 7.

O parâmetro ε é definido pelo detentor dos dados. A Tabela 2 apresenta cinco exemplos de ruído, respostas e probabilidade de ocorrência após a aplicação da Privacidade Diferencial sobre o conjunto de dados original da Figura 9, considerando $\varepsilon = 1$. Observe que na primeira linha o valor do ruído gerado foi $-2,62$. Esse valor é adicionado ao valor real da consulta, conforme a segunda coluna. O valor $0,37$ constitui a saída do modelo de privacidade, isto é, o valor que será retornado ao usuário. A terceira coluna da tabela corresponde

Tabela 2 – Cinco possíveis valores de ruído, resposta e probabilidade de ocorrência após a aplicação da Privacidade Diferencial.

Ruído	*f(G) + ruído*	*Pr(f(G) + ruído)%*
-2,62	0,37	6,74
0,20	3,20	22,59
0,49	3,49	19,52
-0,09	2,90	23,89
-1,31	1,68	12,95

Fonte: Elaborado pelo autor

a probabilidade de que o resultado da consulta adicionado ao ruído tenha a partir da uma entrada a cada execução do mecanismo.

Conclusão

Este capítulo apresentou um conjunto de conceitos e definições vinculados as garantias de privacidade para dados em redes sociais em que os dados são produzidos no formado de grafo RDF. Foram definidos os aspectos mais importantes que circundam o contexto de redes sociais, bem como suas representações e possíveis violações de privacidade. Também, foram apresentados os principais conceitos relacionados ao conjunto de práticas de publicação de dados estruturados na Web chamado de Dados Ligados. Um maior enfoque foi dado aos conceitos relacionados a especificação RDF por ser o foco desse trabalho. Além disso, foram apresentadas as principais formas de garantir a privacidade de dados e as características do modelo Privacidade Diferencial. Neste modelo foi explorado a definição formal, como calcular os dados vizinhos e como calcular a sensibilidade. Por fim, descrevemos como atua o mecanismo de Laplace na Privacidade Diferencial.

3 TRABALHOS RELACIONADOS

Neste capítulo apresentamos alguns dos principais trabalhos relacionados à aplicação de técnicas de garantia de privacidade para dados de redes sociais no formato de grafos. Existem duas principais abordagens quando se trata de preservação de privacidade: através de técnicas de anonimização ou apenas por meio da disponibilização de resultados estatísticos para análise. Dessa forma, os trabalhos relacionados são classificados por abordagem, considerando os mais expressivos e analisando seus pontos fortes e suas limitações. Mais especificamente, na Seção 3.1, abordamos formas de anonimização para a publicação de dados no formato de grafos no contexto de redes sociais. Na Seção 3.2, abordamos a aplicação do modelo Privacidade Diferencial em dados em formato de grafos. O nosso objetivo está mais relacionado ao tema da disponibilização de resultados estatísticos e, por esse motivo, apresentamos mais detalhes sobre essa abordagem. Ao final do capítulo, realizamos uma breve discussão destacando as limitações dos trabalhos apresentados em comparação com a nossa contribuição.

3.1 Anonimização para Grafos

Muitos conjuntos de dados são naturalmente representados como um grafo com vários tipos de conexões. Redes sociais são normalmente representadas em formato de grafos. Existem diferentes formas de garantir a privacidade em redes sociais, uma das técnicas mais comuns é a anonimização dos dados para a publicação, tanto em dados tabulares (FEDER *et al.*, 2008; LIU; TERZI, 2008; NARAYANAN; SHMATIKOV, 2009; LI; SHEN, 2010; ZHELEVA; GETOOR, 2011) quanto em dados no formato de grafos (HAY *et al.*, 2006; GENG; VISWANATH, 2012; WANG; WU, 2013).

3.1.1 Privacy in social networks: A survey

Vimos no Capítulo 2 três tipos de riscos de violação de privacidade: divulgação de identidade, divulgação de atributos e divulgação de ligação social. O trabalho de (ZHELEVA; GETOOR, 2011) detalha essas violações e os possíveis ataques de privacidade estudados na literatura, considerando técnicas de anonimização. O trabalho apresenta dois cenários distintos que ilustram bem o assunto. No primeiro cenário, o adversário está interessado em descobrir as informações sensíveis de um indivíduo. No segundo cenário, o provedor dos dados está interessado em publicar sua rede social para possíveis pesquisadores, mas mantendo a privacidade

dos usuários pertencentes a rede.

Para esse segundo cenário, a técnica mais comum é a anonimização dos dados. O objetivo da anonimização é remover ou perturbar os atributos dos dados que podem ajudar um adversário a inferir informações confidenciais, pressupondo que os dados estão todos em uma única tabela para que seja aplicada alguma técnica de anonimização. Apesar da anonimização ser apropriada para esse cenário, segundo a autora, os dados de redes sociais podem ter uma grande variedade de dependências entre indivíduos, trazendo possíveis oportunidades para que adversários consigam explorar e aprender mais sobre os indivíduos. Em vez de assumir dados que são descritos por uma única tabela de registros independentes com informações de atributos para cada um, a autora leva em consideração conjuntos de dados complexos do mundo real.

Uma maneira ingênua de anonimizar uma rede social é remover todos os atributos dos perfis, deixando apenas a estrutura de vínculo social. Isso cria um grafo anonimizado que é similar ao grafo original. A intuição por trás dessa abordagem é que, se não houver atributos que identifiquem os perfis, os riscos relacionados as divulgações de atributos e identidade não ocorrerão, portanto, a privacidade dos usuários é preservada. Entretanto, essa técnica não apenas remove muita informação importante, diminuindo a utilidade, mas também não garante a privacidade dos usuários. Por exemplo, o atacante poderia inserir contas falsas em uma rede social antes da divulgação e fazer diversas ligações com outros usuários, a fim de monitorar e descobrir padrões na rede. Ou, através de uma rede social auxiliar em que a identidade dos usuários são conhecidas, poderia ter ajuda para identificar os nós da rede social alvo.

Segundo a autora, as estratégias de anonimização para estruturas como as de uma rede social se enquadram em quatro categorias principais: modificação das arestas, randomização, generalização de rede e mecanismos diferencialmente privados. Baseados na intuição de que o risco para a privacidade de alguém não deve aumentar substancialmente como resultado da participação em um banco de dados, os mecanismos de Privacidade Diferencial aplicados a redes sociais diminuem substancialmente os riscos de possíveis descobertas de informações. Segundo a autora, a Privacidade Diferencial oferece boas garantias de preservação da privacidade dos usuários de uma rede social.

3.1.2 Logical Foundations of Privacy-Preserving Publishing of Linked Data

O trabalho (GRAU; KOSTYLEV, 2016) considera a anonimização de grafos RDF. Segundo o autor, a Preservação da Privacidade na Publicação de Dados (PPPD) refere-se ao

problema de proteger a privacidade individual, garantindo, ao mesmo tempo, que os dados publicados permaneçam úteis para a análise. O objetivo do trabalho é estabelecer bases teóricas para o PPPD no contexto de Dados Ligados, com um foco nos requisitos semânticos que um grafo RDF anonimizado deve satisfazer antes de ser lançado na Web, bem como sobre a complexidade computacional de verificar se esses requisitos são atendidos.

Um *Internationalized Resource Identifiers* (IRI) é um padrão que estende a definição de *Uniform Resource Identifier* (URI) para conter caracteres na codificação ISO. Na abordagem proposta, um grafo RDF anonimizado G é obtido a partir do grafo original G_0 substituindo algumas ocorrências de IRIs em triplas por nós em branco, isto é, valores nulos rotulados. Por exemplo, um tripla representada por $t_1 = (alice, seenby, mary)$ poderia ser substituída por nós vazios n_1 e n_2, representando respectivamente *alice* e *mary*. De maneira geral o autor apresenta um framework para PPPD que garanta que grafos anonimizados possam ser publicados na Web Semântica.

Segundo o autor, o problema da anonimização de RDF permanece bastante inexplorado. Uma das limitações desse trabalho é que não considera as ontologias, que são usadas para enriquecer a semântica dos grafos RDF. Tecnologias como o k-anonimato e a l-diversidade até agora foram usadas, mas essas técnicas resultaram em perda significativa de informação. Nesse trabalho, o autor concluiu argumentando que ainda faltam técnicas que proporcionem a privacidade com perda mínima e que melhore a utilização dos dados publicados.

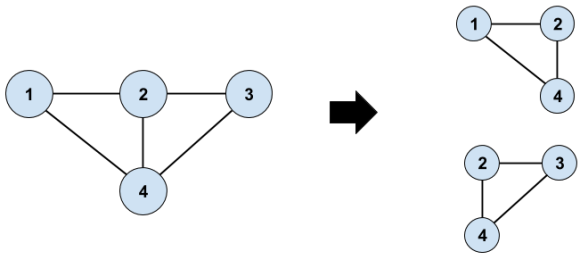
3.2 Privacidade Diferencial para Grafos

Conforme definimos no Capítulo 2, existem duas abordagens principais quando tratamos da Privacidade Diferencial para grafos: relacionado a remoção ou adição de uma aresta ou relacionado a remoção ou adição de um nó. Remover ou adicionar uma aresta significa que um atacante não seria capaz de determinar se há uma associação entre dois indivíduos A e B. Remover ou adicionar um nó significa que não seria possível determinar a presença de um indivíduo A ou B no conjunto de dados. Dessa forma, os trabalhos relacionados são classificados por Privacidade Diferencial para grafos relacionados a remoção ou adição de arestas ou de nós.

O primeiro trabalho que tratou de computar o modelo de privacidade sobre grafos foi proposto no trabalho (NISSIM *et al.*, 2007), onde foi mostrado como estimar, com a Privacidade Diferencial relacionada às arestas, o custo da árvore de expansão mínima e o número de triângulos em um grafo. Uma árvore de expansão mínima é um subconjunto de arestas de um grafo

conectado, ponderado e não direcionado que conecta todos os vértices do conjunto, sem ciclos e com mínimo possível do total de pesos das arestas. Em vista disso, o autor define que dado um grafo conectado, onde todos os pesos das arestas são inferiores a algum número w, a sensibilidade local será no máximo w. A principal ideia é expressar a sensibilidade local em termos da árvore de expansão mínima. Da mesma forma, a sensibilidade local também é expressa em termos da contagem de triângulos do grafo. Veja um exemplo de contagem de triângulos, mostrado na Figura 11. Nesse exemplo, o grafo possui dois triângulos.

Figura 11 – Grafo com dois triângulos.



Fonte: Elaborado pelo autor

Para estimar a Privacidade Diferencial relacionada às arestas do grafo, aplicou-se técnicas de adição de ruído em que o ruído é calibrado para uma variante mais local de sensibilidade, denominada sensibilidade suave (*smooth sensitivity*). Isto é, a sensibilidade suave é uma medida de variação de uma função f em um grafo vizinho de um conjunto de dados de entrada. A ideia é gerar uma sensibilidade local proporcional a global, adicionando ruído de forma proporcional ao dado de entrada.

A partir desse trabalho, surgiram novos estudos como (HAY *et al.*, 2009) e (KARWA *et al.*, 2011). O trabalho (HAY *et al.*, 2009) descreve e analisa um algoritmo que produz estimativas precisas da distribuição de grau de uma rede social. Essas estimativas são publicadas garantindo a privacidade. O trabalho (KARWA *et al.*, 2011) propõe algoritmos para liberar estatísticas úteis sobre dados de grafo que satisfazem a Privacidade Diferencial. Seus algoritmos fornecem respostas aproximadas a consultas de contagem de subgrafos. Esses estudos contribuíram para o surgimento da Privacidade Diferencial para a adição e remoção de nós.

3.2.1 Analyzing graphs with node differential privacy

Segundo o trabalho (KASIVISWANATHAN *et al.*, 2013), muitas técnicas relacionadas a Privacidade Diferencial para grafos atacam o problema de remoção ou adição de nós. De acordo com os autores, a ideia principal desse trabalho é "projetar" um grafo de entrada G em um conjunto de grafos com grau máximo limitado um determinado limite. Isto é, transformar G em um grafo de grau limitado G_D e avaliar uma consulta q em G_D, de tal forma que o grau máximo não possa exceder D.

O benefício dessa abordagem é que a sensibilidade de uma determinada função de consulta pode ser muito menor quando a função é restrita a grafos de um determinado grau, uma vez que a inserção de um nó afeta apenas uma parte relativamente pequena do grafo. Para redes mais realistas, como grafos mais esparsos, a projeção do grafo de entrada perde relativamente pouca informação quando o limite do grau é escolhido com cuidado. A dificuldade dessa abordagem é que a própria projeção pode ser muito sensível a uma mudança de um único nó do grafo original. Para resolver esse obstáculo, os autores propõem operadores de projeção adaptados. Esses operadores atuam retornando uma fração do grafo (de baixo grau) que é uma solução para um problema de otimização convexa, dado por uma instância do *fluxo máximo* ou da progressão linear, baseados nas extensões de *Lipschitz*. Com esses operadores é possível criar projeções do grafo original para liberar com precisão o número de arestas em um grafo e contagens de pequenos subgrafos, como triângulos, k-ciclos e k-estrelas.

Uma função de fluxo é uma importante técnica definida nesse trabalho para contagem de subgrafos. Os autores mostram que é possível determinar uma função de fluxo que possui baixa sensibilidade global em relação aos nós de grafos de graus limitados e calcula corretamente o número de arestas de um grafo. Outra importante técnica apresentada nesse trabalho mostra como liberar de forma privada o número de cópias de um modelo pequeno de grafo específico H em um grafo de entrada G. Por exemplo, H pode ser um triângulo, um k-ciclo ou um k-estrela. Usando essas projeções, algoritmos podem liberar com precisão consultas de vários tipos. De forma mais geral, para grafos mais realistas, é realizado uma projeção "ingênua" que simplesmente descarta nós de alto grau no grafo e calcula a sensibilidade local dessa projeção. A partir disso, é feito uma redução genérica que permite que qualquer algoritmo diferencialmente privado para grafos de graus limitados seja projetado em um grafo arbitrário. Essa redução genérica baseia-se na análise da sensibilidade suave em uma solução ingênua que simplesmente descarta os nós de alto grau.

3.2.2 Qualitative analysis of Differential Privacy applied over graph structures

No contexto da privacidade relacionado à remoção ou adição de arestas, o trabalho (COSTEA *et al.*, 2013) analisa como aplicar algoritmos de Privacidade Diferencial em grafos ponderados. O objetivo desse trabalho é liberar estatísticas, como por exemplo o número de usuários que combinam com determinados critérios. A maioria das redes sociais pode ser representada como um grafo ponderado em que vértices correspondem aos indivíduos e uma aresta que liga dois vértices i e j é ponderada pelo número de interações entre i e j. Isto é, se a mesma aresta aparece 3 vezes, então o peso 3 será atribuído à respectiva aresta.

A abordagem proposta pelos autores (COSTEA *et al.*, 2013) funciona da seguinte forma: seja $G = (V,E)$ um grafo de entrada, a Privacidade Diferencial é utilizada para perturbar os pesos das arestas, obtendo assim um novo grafo $G' = (V,E')$. Para cada par de nó origem e destino, algoritmos calculam o caminho mais curto tanto para o grafo original quanto para o novo grafo G', utilizando o algoritmo de Dijkstra (DIJKSTRA, 1959). P e P' são respectivamente as arestas com pesos do menor caminho entre o par de nós de G e G'. Por exemplo, considere que o caminho real entre dois nós aleatórios A e B terá um custo total de 12. Isto é, antes de qualquer mecanismo de Privacidade Diferencial estar envolvido. Depois que o ruído de Laplace é adicionado ao grafo, o mesmo caminho entre A e B tem um custo de 15. Isso pode acontecer se o ruído gerado tiver um valor de 3 e A e B estiverem diretamente conectados através de uma única aresta. No entanto, um novo caminho pode ser descoberto no grafo com ruídos. Esse mesmo caminho, se seguido no grafo inicial, naturalmente poderia retornar um valor inferior ao ótimo (neste caso, 15).

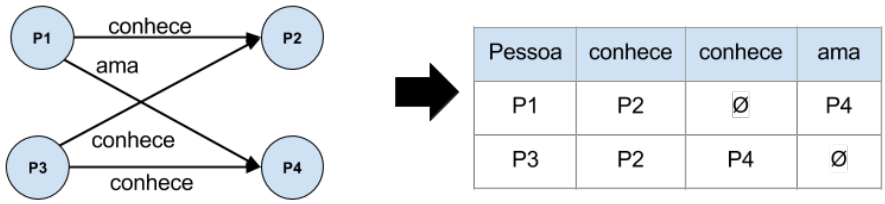
3.2.3 Information Privacy for Linked Data

De todos os trabalhos apresentados até agora, o que mais se aproxima ao nosso é o proposto em (ARON, 2013). Nesse trabalho, o autor investiga como construir mecanismos diferencialmente privados para Dados Ligados usando combinações de técnicas como autenticação, controle de acesso e mecanismos desenvolvidos para manter a Privacidade Diferencial em relação ao contexto de Dados Ligados. O objetivo é fornecer um módulo flexível que forneça garantias de privacidade para diversos conjuntos de dados, funcionando como um serviço web que permite clientes executarem consultas no padrão SPARQL. O módulo, chamado de *SPARQL Privacy Insurance Module* (SPIM), utiliza várias técnicas para alcançar seu objetivo. A primeira

técnica aplicada é a autenticação, onde o sistema verifica se o usuário tem permissão para acessar o módulo. A segunda técnica é a utilização do *Accountability in RDF* (AIR) (KHANDELWAL *et al.*, 2010), um idioma de definição de políticas para a web semântica, utilizado para definir as políticas de privacidade que controlam as informações. Por fim, é utilizado a Privacidade Diferencial para diminuir os riscos ligados a privacidade dos dados no contexto de Dados Ligados.

Boa parte desse trabalho é dedicado a Privacidade Diferencial para Dados Ligados. Inicialmente, o autor propôs generalizar o modelo Privacidade Diferencial para Dados Ligados. Foi necessário generalizar os conceitos do modelo, começando pelo conceito de conjunto de dados vizinhos. Dois conjuntos de dados são vizinhos se diferem em um unidade. Poderia ser considerado uma tripla como unidade de diferença, mas, segundo o autor, usar qualquer unidade de diferença menor do que o "registro pessoal" não ofereceria garantia suficientemente forte para proteger o indivíduo. Por isso, a unidade de diferença utilizada foi um indivíduo, isto é, a diferença entre existir ou não uma pessoa no conjunto de dados. Posteriormente, o autor mostrou a redução de Dados Ligados para registros a fim de fazer uma correspondência de como seria a Privacidade Diferencial aplicada em uma tabela que foi gerada a partir de um grafo RDF. O autor mostrou que converter um grafo para o formato tabular geraria muitos valores vazios. Veja na Figura 12 como seria a redução de um grafo RDF para uma tabela. Veja que os atributos foram repetidos e alguns valores vazios foram gerados.

Figura 12 – Redução de um grafo RDF para uma tabela.



Pessoa	conhece	conhece	ama
P1	P2	Ø	P4
P3	P2	P4	Ø

Fonte: Elaborado pelo autor

Por último, o autor mostrou como calcular a sensibilidade para o contexto de Dados Ligados. O autor propõe a sensibilidade para 5 funções: COUNT, SUM, AVG, MIN e MAX.

Segundo o autor, a sensibilidade de alguma consulta de contagem C, que conta a incidência de um tripla correspondente em um grafo de Dados Ligados, é $Max_p|C(S) - C(S - S_p)| = Max_pC(S_p)|$, ou seja, o número máximo de triplas correspondentes pertencentes a uma pessoa. Para calcular a sensibilidade utilizando o SPARQL, baseando-se em umas das funções definidas, o autor utiliza alguns artifícios. Primeiro, para encontrar os conjuntos vizinhos, a cláusula MINUS é utilizada para "remover" um usuário do grafo. Segundo, a cláusula WHERE e o atributo "foaf: nome" são utilizados para identificar os indivíduos.

3.3 Discussão

Garantir a privacidade dos dados para redes sociais é um desafio que vem sendo enfrentado há alguns anos. Segundo (ZHELEVA; GETOOR, 2011), redes sociais estão susceptíveis a diversos tipos de ataques. De modo consequente, diferentes modelos de preservação de privacidade foram sendo desenvolvidos, a citar a anonimização e a Privacidade Diferencial. Primeiramente, surgiu a anonimização com suas diferentes técnicas, cada nova técnica propondo resolver falhas encontradas nas anteriores. O autor (GRAU; KOSTYLEV, 2016) apresenta a aplicação da anonimização em dados RDF, contexto até então pouco explorado. O framework proposto busca a publicação de um grafo anonimizado no contexto da Web Semântica. Posteriormente, o trabalho (MAYIL; VANITHA, 2017) faz uma revisão das técnicas de anonimização que surgiram ao decorrer dos anos. Avaliando alguns artigos, inclusive o trabalho (GRAU; KOSTYLEV, 2016), o resultado é bastante revelador. Todos os trabalhos apresentaram perda de informação útil. Analisando o trabalho (MAYIL; VANITHA, 2017) e o trabalho (ZHELEVA; GETOOR, 2011), percebemos que as garantias de privacidade não são tão consistentes como deveriam.

Dado esse cenário, alternativas foram surgindo ao longo do tempo. A Privacidade Diferencial (CYNTHIA, 2006) é um marco para a comunidade científica, agregando conceitos da Estatística, esse modelo propõe diminuir as chances de descobertas de informações através da aplicação de ruído. Proposto inicialmente para dados tabulares, foram surgindo novas aplicações em contextos diferentes, como é o caso do formato de grafos. No contexto da aplicação da Privacidade Diferencial em grafos, a maior parte dos trabalhos trata da descoberta e da contagem de padrões de subgrafos como, por exemplo, contagem de triângulos, k-estrelas, etc. O trabalho (KASIVISWANATHAN *et al.*, 2013) é um exemplo disso. Ele faz uma análise da aplicação da Privacidade Diferencial, reduzindo um grafo de entrada em subgrafos de grau limitado. A

partir dos subgrafos, os algoritmos atuam de forma mais precisa para publicar estimativas mais efetivas, como o número de arestas e contar o número de k-estrelas.

Apesar de todos os benefícios do trabalho (KASIVISWANATHAN *et al.*, 2013), a perda de precisão durante a redução depende de um baixo grau do grafo de entrada. Segundo o autor, as garantias de precisão do pior caso são problemáticas para algoritmos diferencialmente privados em relação aos nós. É feito uma suposição leve sobre a distribuição de graus do grafo de entrada. Isto é, o valor do grau máximo do grafo é conhecido. No entanto, as redes do mundo real não são bem modeladas por grafos de grau fixo, uma vez que podem exibir, por exemplo, nós influentes de alto grau. Além disso, as soluções apresentadas estão mais relacionadas a contagem de certas propriedades, como o número de triângulos do grafo. Nossa solução é geral, para várias formas de consultas de contagem, para grafos que exibem nós influentes, típicos de redes sociais e bem próximos da realidade. Além disso, nossa abordagem é eficiente quando grafos possuem grande número de nós e arestas.

Seguindo o mesmo contexto da aplicação da Privacidade Diferencial para grafos, o trabalho (COSTEA *et al.*, 2013) propõe uma abordagem um pouco diferente. O propósito é garantir as propriedades da Privacidade Diferencial em relação as arestas, buscando prevenir a descoberta das propriedades dos indivíduos. Cada aresta é ponderada e, a partir de uma matriz, flexibiliza os pesos e o nível de ruído adicionado as consultas. Embora a pesquisa trate com o conceito de pesos nas arestas, representando estatísticas, o trabalho não considera os nós de origem e de destino no cálculo da sensibilidade. Em consequência, são aplicados algoritmos de Privacidade Diferencial nas informações representadas pelas arestas, não nos sujeitos do grafo como acontece em nossa abordagem. Outra diferença desse trabalho com a nossa abordagem é o valor da sensibilidade. Nesse trabalho a sensibilidade da função é sempre 1 para as consultas de contagens. Em nosso trabalho, a sensibilidade pode ser diferente de 1.

Estamos interessados no contexto de Dados Ligados. Poderíamos optar pela anonimização como fez o trabalho (GRAU; KOSTYLEV, 2016), mas pretendíamos oferecer garantias mais fortes de privacidade como aquelas decorrentes do modelo de Privacidade Diferencial (CYNTHIA, 2006). A carência de trabalhos nesse contexto e a motivação gerada a partir da leitura do trabalho (ARON, 2013) nos levou a investigar estratégias de aplicação da Privacidade Diferencial, originalmente proposta para dados tabulares, em dados representados em RDF. Propomos adaptações da Privacidade Diferencial para os dados em formato de grafos. Um RDF, formato padrão de disponibilização de dados em Dados Ligados, pode ser modelado como um

grafo comum. Na definição padrão da Privacidade Diferencial, dois conjuntos de dados são vizinhos se diferem por um indivíduo. No caso de dados tabulares, diferir em um indivíduo é o mesmo que diferir em um registro. Para Dados Ligados, as informações de um indivíduo estão associadas a um conjunto de triplas. Um registro em um banco de dados convencional representa as informações de um indivíduo. Um indivíduo em Dados Ligados é representado por um conjunto de triplas.

Um conceito definido e provado matematicamente é que a sensibilidade para consultas de contagem em dados tabulares sempre será no máximo 1. Diferentemente dos dados tabulares, uma consulta em grafo pode ser maior que 1. Em especial quando tratamos de redes socias, a maioria das vezes a sensibilidade é diferente de 1, pois em uma rede social os nós estão bem conectados, com milhares de relacionamentos entre indivíduos, isto é, milhares de arestas conectando milhares de nós. Para exemplificar, o Facebook por si só coleta milhares de novas interações de dados de usuários, cerca de $1,32$ bilhões de atividades diárias (FACEBOOK, 2017).

Sabe-se que a sensibilidade e o ε são fatores importantes que determinam a quantidade de ruído que deve ser adicionado na resposta de uma consulta para garantir a Privacidade Diferencial. Entretanto, os riscos associados a privacidade dos dados podem ser bastantes afetados se um ou poucos indivíduos têm muito mais impacto que os demais. Neste caso é preciso identificar quais indivíduos impactam mais do que outros. Porém, dependendo do tamanho do conjunto de dados, custo associado a descobrir os indivíduos que mais impactam na consulta pode inviabilizar uma solução, sendo capaz de resultar em um alto custo computacional e muito provavelmente em um tempo de resposta inadequado, principalmente no contexto de redes sociais onde os grafos podem ser muito grande.

Segundo o trabalho (ARON, 2013), o autor propôs uma generalização da Privacidade Diferencial para Dados Ligados. Para isso, o autor definiu formalmente como calcular a sensibilidade para consultas do tipo COUNT, SUM, AVG, MIN e MAX. Entretanto, para calcular a sensibilidade, o autor considera apenas a remoção das arestas que pertencem ao usuário. Em outras palavras, seja D e D' dois conjuntos de dados em RDF, tal que D' é vizinho de D, D' é obtido a partir de D removendo apenas as arestas de saída de um determinado nó pertencente a D. Porém, neste trabalho, consideramos a remoção de arestas de saída e de entrada. Isto é, arestas não só que pertencem ao indivíduo, mas também as arestas que fazem menção a esse indivíduo. O motivo de considerarmos todas as arestas é que se um indivíduo é removido do

conjunto, não faria sentido manter informações desse indivíduo ou que possam fazer referência a ele de alguma forma, já que o próprio tipo de dado tem como característica principal a ligação entre as informações.

Além disso, podemos citar outras limitações desse trabalho. Primeiro, o autor não faz referências sobre o tipo de sensibilidade que se está interessado. Se a sensibilidade é global, local, ou alguma outra específica. Segundo, a forma de identificar a representação de um registro de um indivíduo no conjunto de dados é um problema, segundo o autor, sendo considerado apenas o atributo "foaf:name", mas podem existir indivíduos sem esse atributo. Terceiro, o autor não define quais propriedades são de natureza sensível e precisam ser protegidas. Em nosso trabalho, consideramos a sensibilidade local e definimos que um indivíduo é identificado pela classe "foaf:Person", mas que pode ser alterado para uma outra classe ou atributo. Além disso, estamos interessados em proteger a identidade dos indivíduos, assumindo que as relações tem caráter público.

A Tabela 1 apresenta um breve comparativo das principais características consideradas pelas estratégias discutidas neste capítulo, incluindo a nossa estratégia (SILVA *et al.*, 2017), proposta neste trabalho.

Quadro 1 – Análise Comparativa entre os Trabalhos Relacionados.

Trabalho	Modelo Privacidade	Técnica	Previne Descoberta	Tipo de Dado
ZHELEVA et al., 2011	Anonimização	Supressão/Generalização	Indivíduo, Atributo	Tabular
GRAU et al., 2016	Anonimização	Supressão	Identidade, Atributo	RDF
KASIVISWANATHAN et al., 2013	P.Diferencial	Remoção/Adição de Nós com todas as suas arestas adjacentes	Indivíduo	Grafos
COSTEA et al., 2013	P.Diferencial	Remoção/Adição de Arestas	Pesos das Arestas	Grafos
ARON et al., 2013	P.Diferencial	Remoção/Adição de Nós pertencentes a um indivíduo	Indivíduo	RDF
R. SILVA et al., 2017	P.Diferencial	Remoção/Adição de Nós com todas as suas arestas adjacentes	Indivíduo	RDF

Fonte: Elaborado pelo autor

A Tabela 1 divide os trabalhos em dois tipos de modelo de privacidade apresentados até agora. Os trabalhos (ZHELEVA; GETOOR, 2011) e (GRAU; KOSTYLEV, 2016) empregam como modelo de privacidade a anonimização. Cada um tratando tipos de dados diferentes, utilizando técnicas semelhantes e com o mesmo objetivo: prevenir a descoberta do indivíduo e de seus atributos. Entretanto, apesar de oferecer garantias de privacidade, conforme vimos anteriormente, a anonimização apresenta vulnerabilidade, passível de possíveis violações de privacidade. Os trabalhos (KASIVISWANATHAN *et al.*, 2013), (COSTEA *et al.*, 2013), (ARON, 2013) e a nossa abordagem (SILVA *et al.*, 2017) utilizam o modelo Privacidade Diferencial. A Privacidade Diferencial oferece garantias fortes de privacidade e pode ser aplicada tanto

para prevenir a descoberta dos indivíduos, quanto para prevenir a descoberta dos atributos dos indivíduos. Os trabalhos (KASIVISWANATHAN *et al.*, 2013) e (COSTEA *et al.*, 2013) apresentam duas técnicas diferentes para aplicação da Privacidade Diferencial em grafos. O primeiro trabalho utiliza técnicas cujo objetivo é a remoção e adição de nós e todas as arestas que estão relacionadas a estes nós. Isso significa que o principal propósito é garantir que a identidade dos indivíduos não seja descoberta. O segundo trabalho está interessado em garantir a anonimização das características dos indivíduos, ao invés da identidade. Especificamente, os atributos estão representados como pesos.

O trabalho (ARON, 2013) e a nossa abordagem (SILVA *et al.*, 2017) tratam de garantir a privacidade dos dados em RDF. Apesar de (ARON, 2013) não descrever explicitamente que o objetivo é prevenir a descoberta dos indivíduos, pelas características apresentadas no trabalho, admite-se que é esse o objetivo. Nossa abordagem também está interessada em esconder a presença ou ausência de um determinado indivíduo, porém empregamos uma técnica diferente da proposta por (ARON, 2013). Baseado em trabalhos já conhecidos que tratavam a remoção e adição de nós (HAY *et al.*, 2009; KASIVISWANATHAN *et al.*, 2013; CHEN; ZHOU, 2013), propusemos uma técnica de adição e remoção de nós em grafos RDF, removendo (ou adicionando) o indivíduo e todas as arestas do grafo que estão relacionadas a ele. No entanto, o trabalho (ARON, 2013) propõe a adição/remoção de triplas pertencentes a um indivíduo.

4 UMA ABORDAGEM DIFERENCIALMENTE PRIVADA PARA RDF DE REDES SOCIAIS

Este trabalho propõe uma abordagem que garante privacidade diferencial sobre dados RDF de redes sociais para consultas analíticas (SILVA *et al.*, 2017). A estratégia opera desde a execução de uma consulta até o retorno da resposta que garante a privacidade e ao mesmo tempo preserva a utilidade dos dados. O método é independente do conhecimento prévio de um atacante, isto é, não importa a que dados anteriores o atacante tenha acesso, não será possível inferir a presença ou ausência de um indivíduo no conjunto de dados com probabilidade maior que a anterior à execução da abordagem. Em particular, busca-se resolver o problema do cálculo da sensibilidade para consultas agregadas sobre seleções que possuem relacionamentos de redes sociais entre indivíduos como predicado, isto é, obter a contagem de indivíduos que possuem mais do que cem amigos.

4.1 Visão Geral

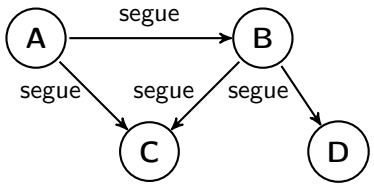
Privacidade Diferencial é uma das técnicas mais adequadas para prover privacidade para consultas agregadas. Entretanto, a maioria das soluções existentes foi projetada inicialmente para dados tabulares, e não dados em grafo. Um dos problemas ocorre quando se trata do cálculo da sensibilidade para consultas que possuem como critério de seleção as propriedades das relações entre indivíduos. Por exemplo, computar a sensibilidade para uma consulta q_1 que requer "contar o número de indivíduos que seguem dois ou mais indivíduos" sobre o grafo da Figura 13 – essa consulta sobre uma base de dados RDF seria representada como no Código Fonte 2. Para isso é preciso considerar o impacto de cada indivíduo para a resposta, isto é, a diferença entre a resposta sobre o conjunto de dados original e todas as suas combinações que diferem em um indivíduo (conjunto de dados vizinhos). A maior dessas diferenças (em módulo) é a sensibilidade para a consulta. Os conjuntos de dados vizinhos para o grafo da Figura 13 são ilustrados na Figura 14. Para o grafo da Figura 13, o valor retornado para a consulta q é 2 (A e B satisfazem). Para conjunto de dados vizinho onde D é desconsiderado (Figura 14a) a resposta é 1 (A satisfaz). Tanto para o conjunto de dados vizinho da Figura 14b quanto para o da Figura 14c a resposta é 0 – nenhum indivíduo satisfaz. Por último, obtém-se a resposta 1 para o conjunto de dados da Figura 14d (B satisfaz). Portanto, o valor da sensibilidade para esse exemplo seria 2 ($|2-0|$).

Código-fonte 2 – Consulta de contagem em SPARQL.

```
1 PREFIX : <http://ufc.br>
2 SELECT (count(*) as ?count)
3 WHERE {
4     filter(?total>=2){
5         SELECT (count(?o) as ?total) ?s
6         WHERE {
7             ?s a :Pessoa .
8             ?s :segue ?o }
9         GROUP BY ?s}}
```

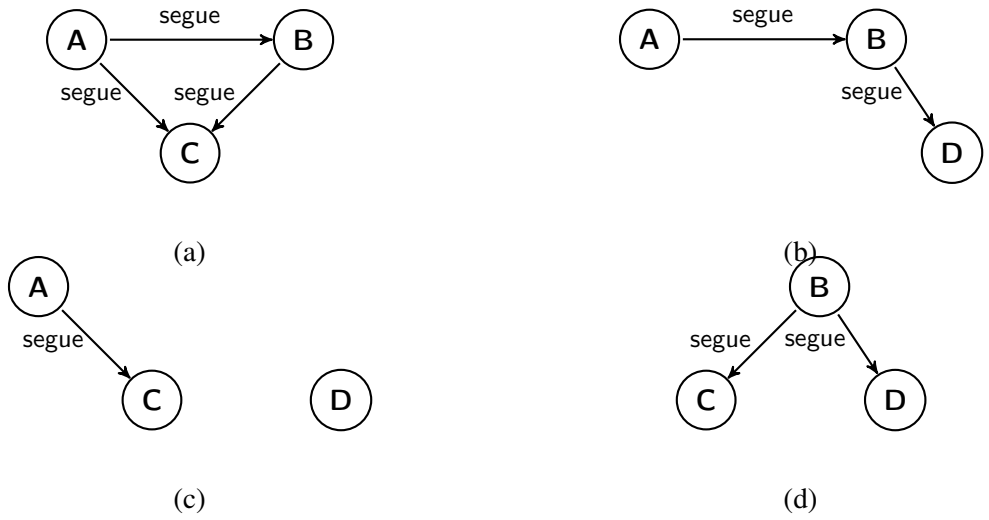
Fonte: Elaborado pelo autor

Figura 13 – Grafo representando uma rede social com quatro indivíduos.



Fonte: Elaborado pelo autor

Figura 14 – Conjunto de Dados vizinhos para o grafo da Figura 13.



Fonte: Elaborado pelo autor

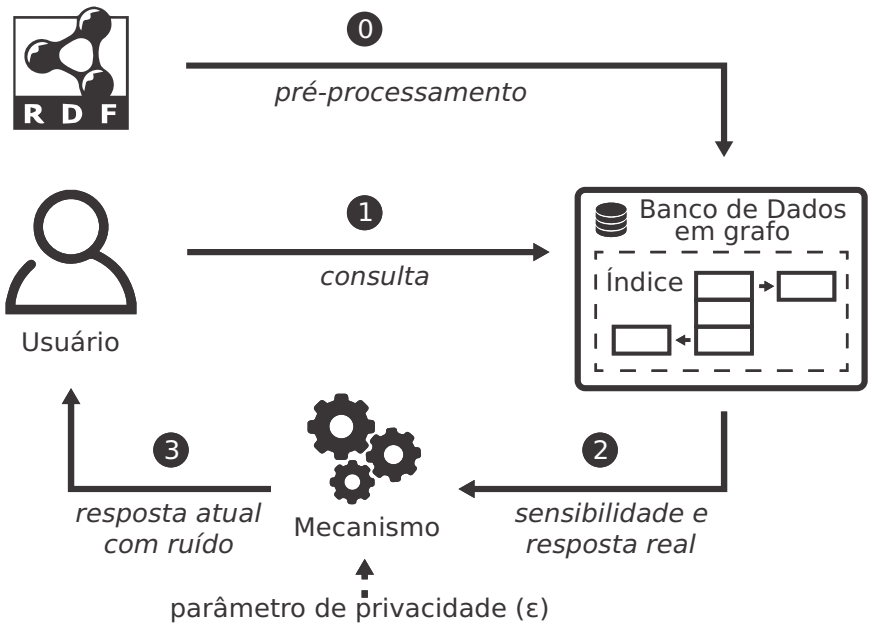
Nenhuma solução proposta na literatura apresenta uma abordagem completa diferencialmente privada que considera a remoção de um indivíduo como um todo (o nó e suas arestas de entrada e saída) para computação da sensibilidade em dados RDF de redes sociais. Além disso, o número de conjunto de dados vizinhos a considerar para computação da sensibilidade é

igual ao número de indivíduos. Isso acarreta um problema quando se trata conjunto de dados reais de redes sociais, onde o número de indivíduos é elevado.

Para tratar os problemas de privacidade sobre dados RDF de redes sociais foi desenvolvida uma abordagem completa de privacidade diferencial, na qual consultas são realizadas sobre uma base de dados e as respostas são perturbadas pela adição de ruído aleatório. A abordagem proposta consiste em quatro etapas orquestradas conforme Figura 15. Essas etapas são definidas da seguinte maneira:

- **Etapa 0 - Pré-processamento**: etapa (*off-line*) abrange: (i) a definição para extração de um dado relacionamento (propriedade) de rede social a partir de dados RDF; (ii) a definição da estrutura de dados auxiliar e (iii) algoritmo para povoamento da estrutura auxiliar.
- **Etapa 1 - Computação da sensibilidade e resposta da consulta**: processamento da consulta sobre a estrutura criada no passo anterior para obtenção do valor real da consulta e o valor da sensibilidade para a mesma.
- **Etapa 2 - Mecanismo de privacidade**: aplicação do mecanismo de privacidade para os valores de saída do passo anterior e o valor de entrada, dado o parâmetro de privacidade ε.
- **Etapa 3 - Validação e resposta da consulta**: adição de ruído obtido no passo anterior ao valor da consulta e validação da resposta.

Figura 15 – Visão Geral da Abordagem.



Fonte: Elaborado pelo autor

4.2 Etapa de pré-processamento

Nessa etapa define-se como os dados que representam um relacionamento em redes sociais são extraídos para a aplicação e utilizados para criar e povoar uma estrutura de dados auxiliar, formada por uma sequência encadeada de elementos, utilizada no cálculo da sensibilidade. Uma rede social é comumente representada por um grafo. A representação de uma rede social expressa em RDF é carregada em nossa solução e pré-processada para que seja armazenada e manipulada de forma eficiente. A partir dessa etapa, são criadas instâncias para representar cada indivíduo. Para cada tripla do RDF que representa um indivíduo, cria-se um nó no grafo identificado por s_i com $i = [1,n]$, onde n é o número de indivíduos. Por exemplo, o usuário representado pela URI *http://dbpedia.org/resource/Pedro* é substituído por uma instância s_1. Para cada tripla do RDF que representa um relacionamento entre dois indivíduos, cria-se uma aresta entre os dois nós. Esse grafo é, então, armazenado em um banco de dados em grafos a ser representado pela estrutura de dados auxiliar proposta.

Essa etapa também define a estrutura de dados auxiliar que tem como principal objetivo prover eficiência no cálculo tanto do valor da consulta de entrada da abordagem, quanto do valor da sensibilidade. Esta etapa acarreta na realização de operações custosas para extração dos dados RDF e povoamento da estrutura auxiliar, portanto deve ser uma operação *off-line*.

4.2.1 Estrutura de dados auxiliar

O objetivo da estrutura de dados auxiliar é representar qualquer forma de associação entre indivíduos representados no grafo. Essas associações podem ser uma relação de amizade, de namoro, etc. Por meio dessa estrutura é possível fornecer eficientemente o valor da sensibilidade e o valor de resposta para consultas que possuem a associação entre os indivíduos como filtro de seleção.

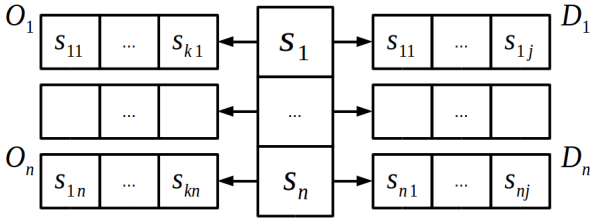
A estrutura de dados auxiliar incorpora conceitos referentes às relações entre os indivíduos. De maneira formal, a estrutura proposta para um determinado relacionamento entre indivíduos no conjunto de dados é definida da seguinte forma:

- $S = ((O_1, s_1, D_1), \ldots, (O_n, s_n, D_n))$ onde s_i é um indivíduo do conjunto de dados, tal que $i \in [1,n]$ e n é o número de nós do grafo que representa os indivíduos;
- $O_i = (s_{1i}, \ldots, s_{ki})$ são os k elementos de s que são nós de origem de um relacionamento r com o nó s_i;

- $D_i = (s_{i1}, \ldots, s_{ij})$ são os j elementos de s que são nós de destinos de um relacionamento r com o nó s_i.

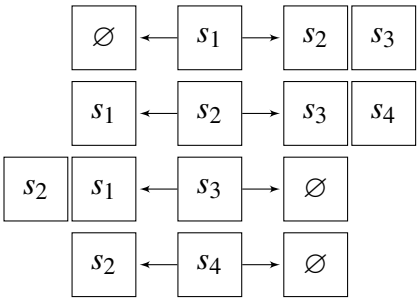
A Figura 16 apresenta uma ilustração da estrutura auxiliar com base nas definições acima. Para exemplificar, a Figura **??** apresenta uma visualização da estrutura auxiliar quando povoada a partir dos dados da Figura 13. Nela temos quatro indivíduos A, B, C e D representados respectivamente pelas instâncias s_1, s_2, s_3 e s_4 e as arestas que representam a relação "segue".

Figura 16 – A estrutura de índice.



Fonte: Elaborado pelo autor

Figura 17 – Visualização da estrutura quando aplicada ao exemplo da Figura 9.



Fonte: Elaborado pelo autor

Se um nó s_i tem relação direcionada com um nó s_j através de uma aresta rotulada que representa um relacionamento, então s_j é adicionado como elemento de destino de s_i (lado direito). Nesse caso, s_i é um nó de origem de s_j e s_j é um nó de destino de s_i. Perceba, por exemplo, que ao adicionar o indivíduo A da Figura 13 na estrutura da Figura **??**, representado pela instância s_1, o nó s_3 é adicionado como nó de destino, portanto na instância s_3, s_1 deve aparecer como nó de origem.

4.2.2 Criação e povoamento da estrutura

A estrutura de dados auxiliar será utilizada para varrer todos os indivíduos de maneira eficiente, dado que todos devem ter seu impacto medido para computação da sensibilidade.

Primeiramente, para criar e povoar a estrutura, é preciso definir uma forma de extrair e processar os dados de um RDF de rede social que a irão compor. Para isso, é necessário extrair o grafo que representa apenas os indivíduos de interesse de um dado relacionamento, bem como os relacionamentos entre estes. Então, a partir desse grafo, e com base nos algoritmos propostos, pode-se realizar a construção da estrutura auxiliar.

Para definição dos dados necessários para povoar a estrutura, considere um grafo direcionado $G = (V,E)$, que representa um RDF R, onde V é o conjunto de vértices e E o conjunto de arestas. Seja, também, P o conjunto de propriedades de objetos de R, que trataremos neste trabalho como *labels*, enumeramos o seguinte:

1. $V_I = \{v \in V \mid v \text{ representa um indivíduo }\}$
2. $E_I = \{(v_a, v_b) \in E \mid v_a, v_b \in V_I \wedge v_a \neq v_b\}$;
3. Dado $g : E \rightarrow P$ uma função que mapeia arestas para labels.
4. $L = \{l \mid l = g(v_a, v_b), (v_a, v_b) \in E_I\}$

Definição 8 *(Subgrafo induzido por arestas) Dado um grafo $G = (V,E)$ e $E' \subseteq E$, um subgrafo induzido pela aresta $G[E']$ é um subgrafo definido por um subconjunto das arestas E' juntamente com quaisquer nós em suas extremidades.*

Definição 9 *(Subgrafo induzido por label) Dado $l_i \in P$ um label de um grafo $G = (V,E)$ e $g : E \rightarrow P$ uma função que mapeia arestas para labels, um subgrafo induzido por label $G[[l_i]]$ é um subgrafo induzido por aresta $G[E_i]$ (Definição 8), onde $E_i = \{(v_a, v_b) \in E, g(v_a, v_b) = l_i\}$.*

A partir do RDF R pode-se obter o subgrafo G_i para cada label l_i em L, isto é para cada relacionamento em uma rede social, tem-se o subgrafo induzido por label $G_i = G[[l_i]]$ (Definição 9) e uma estrutura de dados auxiliar S para $G_i = (V_i, E_i)$ como a seguir:

- $S = \{(O_1, s_1, D_1), ..., (O_n, s_n, D_n) \mid j = [1,n], s_j \in V_i\}$;
- $O_j = \{(s_j, x) \in E_i\}$;
- $D_j = \{(x, s_j) \in E_i\}$;

A estrutura S é construída como especificado no Algoritmo 1. Na linha 1 a variável *individualsList* representa todos os n indivíduos na base de dados RDF. As linhas de 2 a 5 realizam a inicialização dos elementos da estrutura. Ao final da execução deste trecho tem-se uma lista com n elementos (O_i, s_i, D_i), i variando de 1 a n, com O_i e D_i vazios. Para cada elemento s desta lista (linha 7), percorre-se todos os seus relacionamentos que têm o label l dado como parâmetro de entrada, e para cada um desses relacionamentos (arestas) pegamos o nó

da outra extremidade (linha 9). Se esse nó for um nó de origem do relacionamento (linha 10), adiciona-se a referência para esse nó na lista *O* de *s* (linha 11), caso contrário o nó é considerado como nó de destino e é adicionado na lista *D* de *s*.

Algoritmo 1: buildStructure constrói a estrutura auxiliar.

```
   Input: label de relacionamento l
   Output: estrutura de dados auxiliar S
 1 individualsList ← todos os nós que representam indivíduos
 2 for each nó n in individualsList do
 3 |   crie o elemento s
 4 |   s.N ← n
 5 |   adicione s in S
 6 end
 7 for each s in S do
 8 |   for each relacionamento rel of type l in s.N do
 9 |   |   parNo ← outro nó de rel
10 |   |   if parNo é o nó de origem in rel then
11 |   |   |   append parNo in s.O
12 |   |   end
13 |   |   else
14 |   |   |   append parNo in s.D
15 |   |   end
16 |   end
17 end
18 return S
```

Análise do Algoritmo 1. Dado um grafo $G = (V,E)$, $v \in V$, $n = |V|$ e $m = |E|$, o laço na linha 2 tem complexidade $\Theta(n)$ pois é executado uma vez para cada nó. Visto que há um *s* para cada nó, o laço na linha 7 também tem complexidade $\Theta(n)$. Já o laço interno na linha 8 é executado $(2 * Adj[v])$ vezes devido ao fato que cada aresta é visitada duas vezes – uma vez para o nó de origem e outra para o de destino. Sabendo que $\sum_{v \in V} |Adj[v]| = (2 * m)$, o custo para as linhas 8 a 16 é $\Theta(m)$. Então a complexidade para as linhas 7 a 17 é $\Theta(n+m)$.

4.3 Etapa 1: Processamento das consultas

Essa etapa apresenta como computar de forma eficiente tanto o valor real da consulta de entrada da abordagem como o valor da sensibilidade. A ideia principal é evitar refazer a computação da consulta para cada possível conjunto de dados vizinhos a fim de detectar o maior impacto de um indivíduo (sensibilidade).

Código-fonte 3 – Formato de consulta tratada pela abordagem.

```
1 SELECT COUNT(x)
2 WHERE COUNT( (x)−[rotulo]−>(y) ) [OPERADOR_DE_COMPARACAO] [valor_de_filtro]
3 {[OPERADOR_LOGICO] (x:atributo) [OPERADOR_DE_COMPARACAO] [valor_de_atributo]};
```

Fonte: Elaborado pelo autor

O formato de consultas suportadas pela abordagem está detalhado no Código Fonte 3, uma variável entre parênteses, por exemplo (x), representa um nó de indivíduo; uma variável entre os símbolos "$-$" e "$->$" indica o rótulo de uma propriedade de associação; partes entre chaves são opcionais; finalmente, valores entre colchetes são os valores a serem definidos para a consulta. Apenas uma cláusula com propriedade de associação entre os indivíduos é suportada, como no exemplo da consulta no Código Fonte 3 com a propriedade *segue*.

Cláusulas opcionais com base em atributos dos nós poderiam ser adicionadas (linha 3). Consultas de contagem são as mais básicas e essenciais para várias tarefas importantes de mineração de dados, tais como mineração de itens frequentes e regras de associação (HAN *et al.*, 2011), portanto uma questão importante a ser tratada.

Para processar a consulta de entrada, isto é, a consulta realizada por um usuário, o Algoritmo 2 atua sobre a estrutura auxiliar definida na etapa anterior. Primeiramente o Algoritmo 3 é invocado para computar o valor de resposta da consulta. Em seguida, computa-se a sensibilidade para a consulta varrendo cada elemento e medindo o seu impacto para a resposta da consulta. Após verificar todos os elementos, consegue-se saber o maior e o menor valor da consulta considerando todos os possíveis conjuntos de dados vizinhos e, com isso, é possível computar a maior diferença em relação ao valor de resposta da consulta, isto é, a sensibilidade.

O Algoritmo 2 funciona como descrito a seguir. Para cada elemento s (linha 4), primeiro verifica se ele é um dos elementos que satisfaz a consulta (linhas 7 e 8). Em seguida é computado o impacto de s verificando os elementos que são origem de um relacionamento com s, isto é, elementos em $s.O$, caso s seja removido do conjunto de dados. Para cada um destes elementos de origem (linha 10), é verificado se eles satisfazem a consulta antes de considerar a remoção de s (linha 11) e após a remoção (linha 14). Com esses valores de antes e depois é possível computar o real impacto considerando o conjunto de dados vizinho onde s é removido (linhas 18 e 19). São mantidos o maior e o menor valor de impacto ao testar todos os elementos (linhas 20 a 25). Após varrer todos os elementos s em S e obter os valores de maior e menor

Algoritmo 2: getSensitivity computa o valor da sensibilidade

Input: estrutura de dados auxiliar S
Output: O valor da sensibilidade

```
1  valorReal ← getRealValue()
2  maiorValor ← −∞
3  menorValor ← +∞
4  for each s in S do
5  |  contadorAnterior ← 0
6  |  contadorPosterior ← 0
7  |  if (tamanho de s.D) que satisfaz a consulta then
8  |  |  contadorAnterior++
9  |  end
10 |  for each o in s.O do
11 |  |  if tamanho de o.D satisfaz a condição da consulta then
12 |  |  |  contadorAnterior++
13 |  |  end
14 |  |  if (tamanho de o.D) − 1 satisfaz a condição da consulta then
15 |  |  |  contadorPosterior++
16 |  |  end
17 |  end
18 |  dif ← |contadorAnterior − contadorPosterior|
19 |  valor ← |valorReal − dif|
20 |  if valor ≥ maiorValor then
21 |  |  maiorValor ← valor
22 |  end
23 |  if valor ≤ menorValor then
24 |  |  menorValor ← valor
25 |  end
26 end
27 sA ← |valorReal − maiorValor|
28 sB ← |valorReal − menorValor|
29 return max(sA, sB)
```

Algoritmo 3: getRealValue calcula o resultado da consulta

Input: estrutura de dados auxiliar S
Output: o valor real do resultado da consulta

```
1  valorReal ← 0
2  for each s in S do
3  |  if tamanho de s.D satisfaz a condição da consulta then
4  |  |  valorReal++
5  |  end
6  end
7  return valorReal
```

impacto, a sensibilidade é calculada considerando a maior diferença em módulo entre o valor real da consulta e o maior e menor valor (linha 27 a 29).

Análise do Algoritmo 2. Dado um grafo $G = (V,E)$, $v \in V$, $n = |V|$ e $m = |E|$, a linha 1 executa o Algoritmo 3, que possui complexidade $\Theta(n)$, pois é executada uma vez para cada nó. O laço na linha 4 é executado uma vez para cada elementos s, i.e., $\Theta(n)$. Já o laço interno na linha 10, executa uma vez para cada aresta de s no qual s é o elemento de destino desta aresta, então $|IncomingAdj[v]|$ vezes, visto que cada s representa um $v \in V$. Como $\sum_{v \in V} |IncomingAdj[v]| = \Theta(m)$, pode-se afirmar que o custo total do algoritmo é $\Theta(n+m)$.

4.4 Etapa 2: Mecanismo de privacidade

Essa etapa consiste na aplicação de um mecanismo que garanta as propriedades da privacidade diferencial para a saída de uma consulta. Em outras palavras é preciso garantir que o resultado das consultas atendam aos requisitos do modelo. Para alcançar o modelo de privacidade diferencial na abordagem foi definido o mecanismo de Laplace, amplamente aceito e utilizado nos trabalhos da área de Privacidade Diferencial (LI *et al.*, 2010; SARATHY; MURALIDHAR, 2011; KASIVISWANATHAN *et al.*, 2013), principalmente para consultas de contagem.

São necessários três parâmetros de entrada para o mecanismo de privacidade nesta etapa: o valor do resultado da consulta, o valor da sensibilidade e o valor de ε. Os dois primeiros parâmetros são computados pela etapa anterior e o terceiro deve ser informado por um especialista de domínio ou definido empiricamente. Quanto maior o valor de ε menor ruído é adicionado e a utilidade dos dados para análise é maior, porém o nível de privacidade é menor. Esse *trade-off* entre privacidade e utilidade dos dados determina a escolha do parâmetro ε. Em geral, deve-se realizar avaliações com diferentes valores de ε para análise desse *trade-off*.

Conforme vimos na Seção 2.4.4, o mecanismo de Laplace envolve a adição de ruído aleatório a partir da distribuição de Laplace. Nesta etapa, o valor aleatório do ruído é obtido a partir da distribuição de Laplace centrada no 0 e com escala definida por $\frac{\Delta f}{\varepsilon}$, onde Δf é o valor da sensibilidade para a consulta de entrada da abordagem. A saída r para uma consulta q desta etapa é dada conforme a Definição 7, sendo $f_q(D)$ uma função que retorna o valor de uma consulta q sobre um conjunto de dados D e $Laplace(0, \frac{\Delta f}{\varepsilon})$ uma função que retorna um valor aleatório a partir da distribuição de Laplace. Os valores de $f_q(D)$ e Δf são provenientes da etapa anterior.

4.5 Etapa 3: Validação e resposta da consulta

Na etapa final da abordagem, é adicionado o ruído obtido como saída da etapa anterior à resposta da consulta. Por exemplo, se uma consulta que conta a quantidade de pessoas dentro de um estádio retornar o valor c, então uma quantidade específica de ruído y é adicionada a resposta c, tal que a saída da etapa é dada por $c + y$.

Além da adição de ruído, é verificado se a consulta excede o limite de publicações, sem violar a privacidade ou aumentar o poder de inferência de um atacante. Por exemplo, pela média das respostas anonimizadas de uma mesma consulta executada diversas vezes sobre abordagens diferencialmente privadas, pode-se inferir um valor próximo do valor de resposta da consulta. Caso o limite de submissões de uma mesma consulta já tenha sido atingido, deve ser impedido que se retorne o valor desta etapa.

Para evitar possíveis violações de privacidade relacionadas ao problema de repetição de consultas pode-se manter um registro (*log*) para auditoria das consultas (NABAR *et al.*, 2006), ou seja, um registro das consultas é mantido e todas as novas consultas são verificadas para constatar possíveis exposições de informações, permitindo e autorizando consultas de um determinado usuário. A negação de uma consulta ocorre sempre que a resposta a essa consulta e as consultas anteriores podem ser combinadas para coletar informações sobre qualquer indivíduo.

4.6 Discussão

Neste capítulo foi apresentado e discutido cada etapa da abordagem proposta, incluindo algoritmos próprios como solução ou referenciando soluções em trabalhos já existentes para compor cada uma das partes. Em relação aos Algoritmo 1 e Algoritmo 2 propostos, a complexidade para ambos é de $\Theta(n+m)$, onde m é o número de nós e n é o número de arestas. Entretanto, operações do Algoritmo 1 na Etapa 0 para construção da estrutura de índice, principalmente se executadas para banco de dados com persistência em disco, tornam-se custosas. Portanto, esta deve ser uma etapa pré-processada.

Além disso, é importante reafirmar que a contribuição apresentada, é para cenários de consultas agregadas que possuem um relacionamento entre indivíduos como predicado (*filtro*) em dados dispostos em forma de grafo, isto é, se a consulta não envolver relacionamento (aresta) como predicado, ou os dados não possuírem interdependência para a consulta, a contribuição seria menos relevante.

5 RESULTADOS

Neste capítulo apresentamos uma série de resultados para avaliar nossa abordagem. Primeiramente, avaliou-se a privacidade resultante da aplicação da nossa estratégia em termos de erro relativo. Essa métrica nos mostra uma medida de precisão do mecanismo utilizado pela abordagem. Avaliou-se também aspectos relativos a utilidade dos dados após aplicação do modelo Privacidade Diferencial sobre consultas executadas em dados RDF. Desse modo, executou-se experimentos variando o parâmetro ε com o objetivo de avaliar quão distante, isto é, quão distorcidas as respostas das consultas diferencialmente privadas estão das respostas reais. Observou-se também aspectos e métricas de avaliação em termos de eficiência e tempo de execução, que inclui tanto o tempo de construção da estrutura auxiliar quanto o tempo de aplicação da Privacidade Diferencial em diferentes conjuntos de dados de redes sociais. Em particular, foi avaliado o tempo de execução no cálculo da sensibilidade, visto que esse cálculo é primordial para aplicação da Privacidade Diferencial, podendo ser o gargalo da aplicação.

5.1 Ambiente de experimentação

A abordagem proposta, suas estruturas de dados e algoritmos foram desenvolvidos na linguagem Java. Foi adotado o banco de dados em grafos Neo4j (NEO4J, 2017), utilizado por ser um banco de dados em grafo nativo e, também, devido à sua capacidade de gerenciar os dados através de sua API Java. Todos os experimentos foram realizados em uma máquina com Sistema Operacional Windows 10, processador Intel Core i5 de $3,10$ GHz, 12 GB de RAM e disco de 380 GB.

Em relação aos dados utilizados para avaliar nosso método, foram adotados três conjuntos de dados reais, extraídos do projeto *Large Network Dataset Collection* da Universidade de Stanford (LESKOVEC; KREVL, 2014). Tais conjuntos são compostos de dados sobre círculos de relacionamentos entre usuários nas seguintes redes sociais: Facebook, Twitter e Google+. O conjunto de dados do Facebook utilizado para avaliar nossa estratégia possui 4.039 nós, representando seus usuários, e 88.234 arestas, representando as relações entre tais usuários. Já o conjunto de dados do Twitter possui 81.306 nós e 1.768.149 arestas, considerado vinte vezes maior em relação aos dados do Facebook. Já o conjunto do Google+ possui 107.614 nós e 13.673.453 arestas, o que representa um volume de cerca de vinte e seis vezes maior em relação aos dados do Facebook e pouco maior que os dados do Twitter. Esse foi o maior

conjunto de dados utilizado na nossa experimentação, o qual permite uma análise mais precisa da abordagem à medida que o volume de dados cresce. O resumo das características de cada um desses conjuntos, em termos de indivíduos e relacionamentos, pode ser visto na Tabela 3.

Tabela 3 – Características dos conjuntos de dados.

Conjuntos de Dados	**Nós**	**Arestas**
Facebook	4.039	88.234
Twitter	81.306	1.768.149
Google+	107.614	13.673.453

Fonte: Elaborado pelo autor

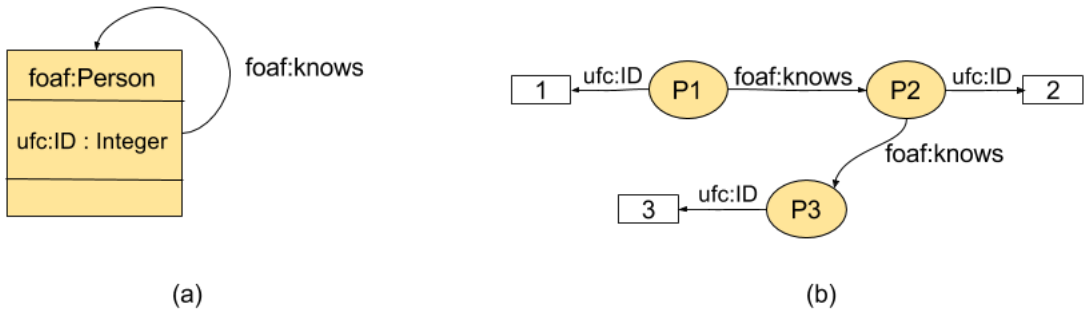
Os dados combinados contêm mais de 192 mil nós de usuários e mais de 15 milhões de relacionamentos, que foram anonimizados substituindo-se os IDs internos de cada usuário por um novo valor, mas preservando as características originais. Por exemplo, o ID 14519713 de um usuário do Facebook foi substituído por um outro número qualquer, sem perda na representação de seus relacionamentos com outros usuários. Assim, mesmo com o dado anonimizado, é possível determinar se dois usuários possuem alguma relação entre si. Entretanto, não é possível determinar quem são os indivíduos. Portanto, a mesma correlação é utilizada em nossos experimentos.

Os dados são compostos de tuplas com dois atributos numéricos dos indivíduos (ID-ID). Dessa forma, cada tupla representa um relacionamento entre os dois IDs. Além disso, para cada tupla, existe um relacionamento direcionado no sentido do ID da primeira coluna para o ID da segunda. Por exemplo, seja $t = (19, 25)$ uma tupla com os IDs 19 e 25. Ao ser exibido em um grafo, o ID 19 representa um indivíduo e o ID 25 representa um outro indivíduo. Além disso, existe uma aresta que liga o ID 19 ao ID 25 e que esta aresta representa um relacionamento entre os dois indivíduos do tipo *conhece*.

Por fim, vale ressaltar que devido à falta de conjuntos de dados semânticos de redes sociais disponíveis, os conjuntos de dados originais foram convertidos para o formato RDF com base em um esquema RDF simples, apresentado na Figura 18, criado para representação de uma rede social. A Figura 18a exibe o esquema RDF que representa os dados, definido através do vocabulário FOAF *(Friend of a Friend)*. A especificação FOAF é um projeto dedicado a ligar pessoas e informações através da Web utilizando a tecnologia RDF (FOAF, 2017). A classe *Person* representa as pessoas, isto é, um recurso é um *Person* se ele é uma pessoa na vida real. A propriedade *knows* relaciona duas classes *Person*, isto é, representa que uma pessoa conhece outra pessoa. Comumente, a relação entre duas pessoas que se conhecem é recíproca.

No entanto, tal fato não implica a obrigação de qualquer uma das partes publicar uma declaração FOAF, descrevendo esse relacionamento. Assim, um relacionamento conhecido não implica em uma relação de amizade. Em nosso contexto consideramos que não há reciprocidade. A Figura 18b apresenta um exemplo dessa definição. Nesse exemplo temos que a pessoa P1 conhece uma pessoa P2 e que P2 conhece P3. No entanto, não significa que P2 conhece P1 e nem que P3 conhece P2. Além disso, como o vocabulário FOAF não possui a especificação para a propriedade ID, criamos um vocabulário simples, apenas descrevendo a propriedade ID.

Figura 18 – Esquema RDF dos dados de teste (a) e uma instância desse esquema (b).



Fonte: Elaborado pelo autor

Os dados RDF foram consultados e manipulados utilizando o framework atual de ontologia Apache Jena (JENA, 2017) para operações de contagem de indivíduos, número de relacionamentos e consultas do tipo “contagem de pessoas com número de amigos maior que x”, as quais foram verificadas com o arquivo de dados originais. Com isso, validou-se o conjunto de dados RDF dos experimentos através dessas consultas e da comparação com as respostas obtidas nos experimentos.

5.2 Análise da Utilidade dos Dados

Avaliamos para a utilidade da abordagem proposta em termos de erro relativo para verificar em que medida os resultados obtidos correspondem aos resultados reais. O erro relativo é diferença em módulo entre o valor obtido experimentalmente e o valor verdadeiro dividido pelo valor verdadeiro. Em outras palavras, o erro relativo é a razão entre o erro absoluto e o valor verdadeiro. Utilizamos o erro relativo para comparar os resultados da estratégia com os valores

exatos, para se obter uma média de precisão do mecanismo. Adotamos a Equação 5.1 para o erro relativo.

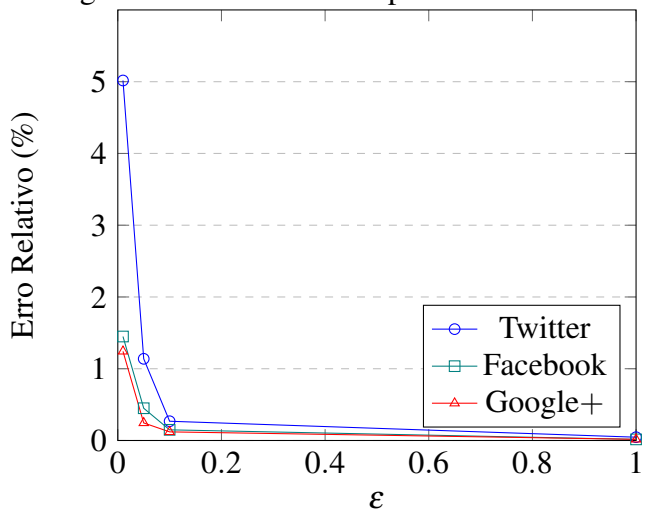
$$RE = \frac{|p - q(D)|}{q(D)} \tag{5.1}$$

Essa é a mesma métrica utilizada por vários autores ao se aplicar a Privacidade Diferencial em seus diversos contextos (XIAO *et al.*, 2011; KARWA *et al.*, 2011; NGUYEN *et al.*, 2013). O valor $q(D)$ representa a resposta real de uma determinada consulta q e p é a resposta retornada pelo modelo. A Figura 19 mostra a variação do erro relativo à medida que o limite de privacidade ε varia. Utilizamos os valores de ε na lista $[0.01, 0.05, 0.1, 1.0]$, com base do trabalho descrito em (SHOARAN *et al.*, 2012). Os resultados mostram que o erro relativo, para todos os conjuntos de dados, diminui à medida que o limite de privacidade ε aumenta. Desse modo, valores de erro relativo, isto é, valores de distorção média produzidos pelo mecanismo quando são executadas as consultas, são bastante elevados quando o limite de privacidade ε é mais próximo de zero. Ou seja, para valores muito baixo de ε, o erro relativo apresenta valores elevados e, consequentemente, a resposta obtida pelo mecanismo será muito diferente da resposta real da consulta. Por exemplo, utilizando o mecanismo de Laplace, o conjunto de dados do Facebook apresenta erro relativo igual a $18,47\%$ quando o valor de ε fornecido é muito baixo: $\varepsilon = 0.01$. Resultado disso, vemos na Figura 19 que quanto mais o valor de ε se aproxima do valor 1, mais diminui o erro relativo. Consequentemente, os três conjuntos de dados tendem a se aproximar do mesmo valor.

Dado que quanto menor o ε, menor a utilidade dos dados, pode-se concluir que a utilidade dos dados é bastante prejudicada com altos valores de erro relativo. Por exemplo, um usuário que executar uma consulta do tipo "Quantos alunos em uma sala de aula de 50 alunos possuem média acima de 7?". A resposta da consulta é 35 alunos, mas se o mecanismo de privacidade retornar o valor 49, essa resposta não terá utilidade alguma. Por outro lado, valores de erro relativo são baixos quando valores de ε são altos. Para obter soluções ótimas, alcançando o nível desejado de privacidade e garantindo um nível mínimo de utilidade e vice-versa, é necessário explorar o *trade-off* variando o valor de ε até encontrar valores ideias. Além disso, existem estudos (ALVIM *et al.*, 2011; SANKAR *et al.*, 2013) que ajudam a lidar com o *trade-off* entre a utilidade e privacidade, apresentando diferentes abordagens.

Foi analisado também o *trade-off* entre utilidade e privacidade sob outro ponto de vista. De acordo com (CHEN *et al.*, 2016), para uma determinada consulta q, a utilidade da

Figura 19 – Erro Relativo para dados reais.



Fonte: Elaborado pelo autor

resposta pode ser mensurada a partir do valor verdadeiro da resposta de uma consulta pelo seu valor obtido após aplicação dos mecanismos de privacidade. Dessa forma, utilizamos a métrica de erro percentual para analisar a utilidade da nossa abordagem. O erro percentual é definido como a porcentagem da diferença entre o valor medido e o valor exato (real) definido na Equação 5.2, onde q_a^i é a resposta real da consulta i, q_o^i é a resposta obtida da consulta i com ruído e n é o número de consultas. A Tabela 4 mostra que as porcentagens são muito próximas de zero, o que significa um resultado próximo ao valor real da consulta, ou seja, um bom resultado de utilidade.

$$\sum_{i=1}^{n} \left| \frac{q_a^i - q_o^i}{q_a^i} \right| 100 \tag{5.2}$$

A Tabela 4 apresenta os resultados da nossa estratégia em relação a utilidade dos dados. Para o conjunto de dados do Google+, o erro percentual é abaixo de 0.1. Isso significa que a média dos valores obtidos após aplicação do ruído está próxima do valor ideal. Já no conjunto de dados do Facebook, para $\varepsilon = 0.01$, temos o maior erro percentual: $18,47\%$. Assim, o valor médio das respostas está mais distante das respostas ideias. Isso pode ser útil para determinadas aplicações que visam maiores níveis de garantias de privacidade. Essa variação de resultados é esperada dado que, quanto maior o valor de ε, maior a privacidade, além de, quanto maior o conjunto de dados, mais a média se aproxima das taxas de erros menores.

Para análise com melhor percepção visual do *trade-off* entre utilidade dos dados anonimizados e privacidade, pode-se observar a Figura 20, que representa a diferença entre a resposta esperada (valor real) e o valor para consultas anonimizadas, tanto para o maior quanto

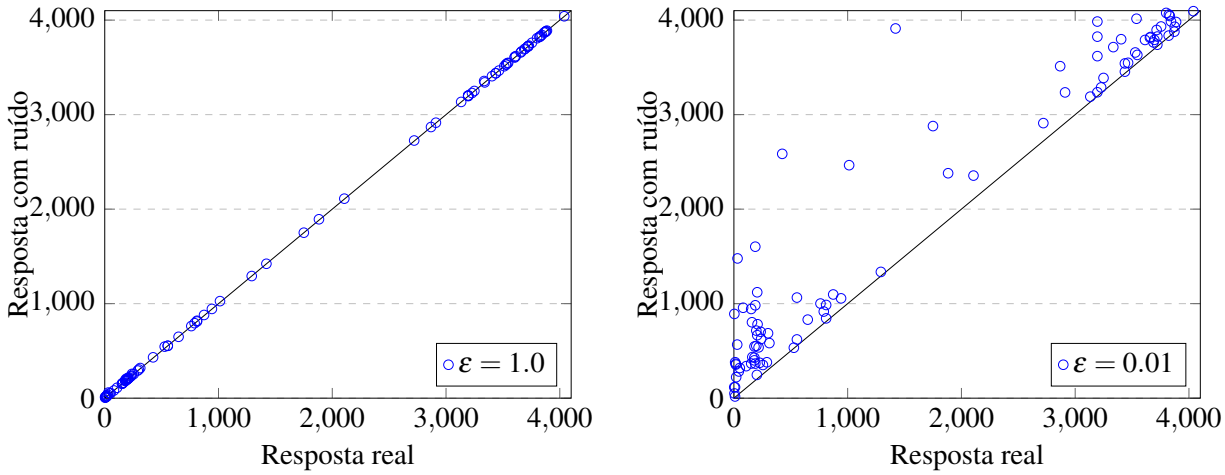
Tabela 4 – Erro Percentual.

Conjuntos de dados	$\varepsilon = 0.01$	$\varepsilon = 0.05$	$\varepsilon = 0.1$	$\varepsilon = 1.0$
Facebook	18,47%	4,18%	2,15%	0,21%
Twitter	6,99%	1,40%	0,86%	0,07%
Google+	10,17%	2,04%	0,95%	0,08%

Fonte: Elaborado pelo autor

para o menor valor de ε definidos para os experimentos no conjunto de dados do Facebook. A diagonal representa o valor esperado, enquanto os pontos representam os valores obtidos com ruído. Portanto, quanto mais aproximados da diagonal os pontos estão, melhor a utilidade dos dados e menor a privacidade. Isto significa que para ε igual a 1, os resultados mostram que as respostas com ruído estão mais próximas das respostas reais, consequentemente as respostas com ruído possuem maior utilidade. Por outro lado, para o gráfico da Figura 20 com ε igual a 0.01, os resultados exibem uma quantidade maior de pontos que estão distantes da reta diagonal do gráfico. Isso significa que as respostas estão mais distantes da resposta real e, consequentemente, oferecem maiores garantias de privacidade. O mesmo pode ser observado na Figura 21 para o conjunto de dados do Twitter e na Figura 22 para o conjunto de dados do Google.

Figura 20 – Distribuição do erro para conjunto de dados do Facebook.

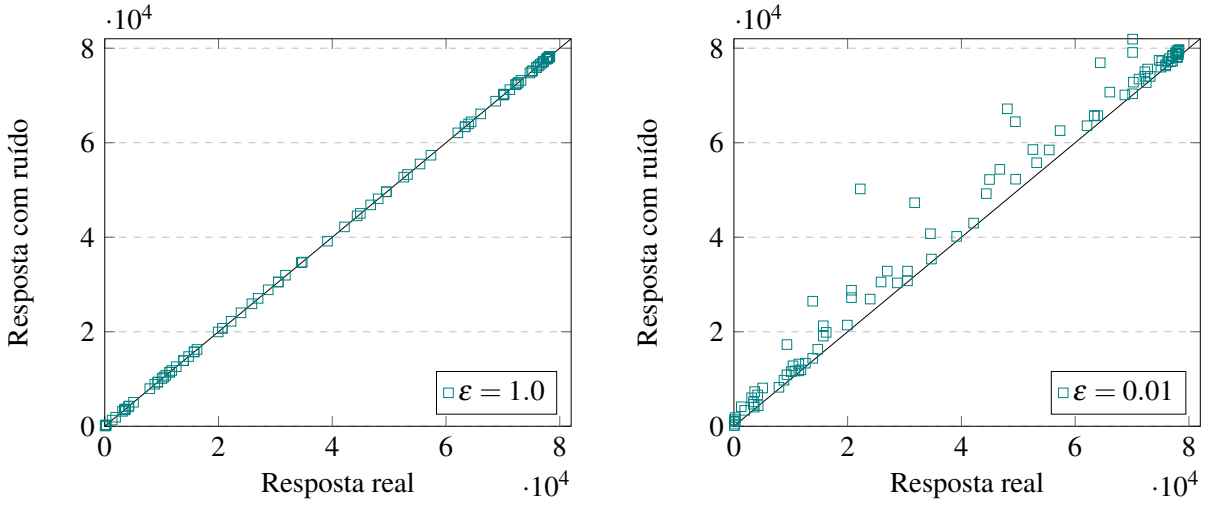


Fonte: Elaborado pelo autor

5.3 Análise de Desempenho

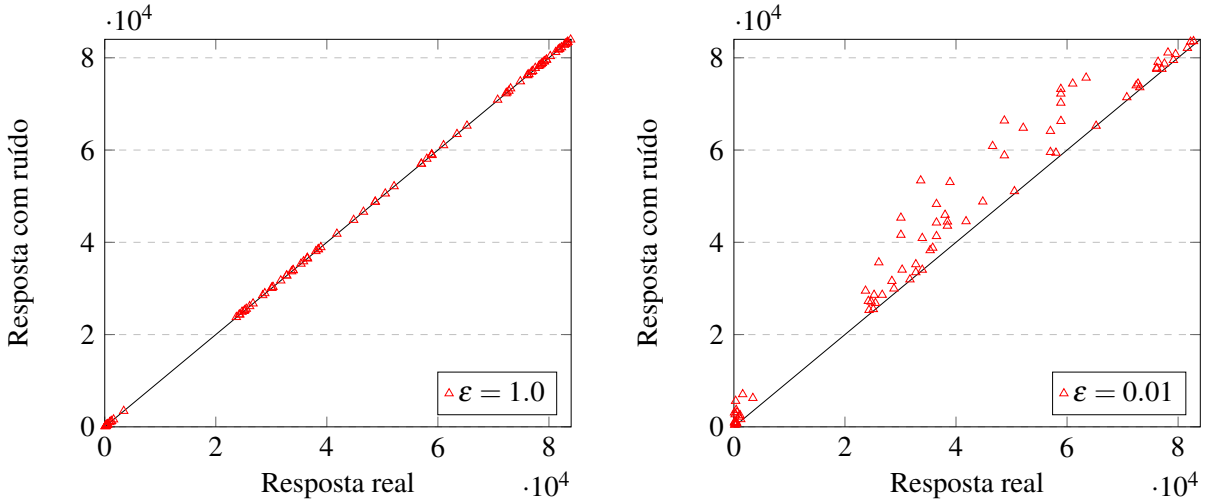
O desempenho da abordagem proposta neste trabalho foi avaliado por duas medidas: tempo de criação da estrutura auxiliar e tempo de cálculo de sensibilidade para cem consultas de contagem aleatórias. Quando calculamos a sensibilidade, o tempo de execução do mecanismo de Privacidade Diferencial com a distribuição de Laplace é insignificante, uma vez que consiste

Figura 21 – Distribuição do erro para conjunto de dados do Twitter.



Fonte: Elaborado pelo autor

Figura 22 – Distribuição do erro para conjunto de dados do Google+.



Fonte: Elaborado pelo autor

apenas em algumas operações matemáticas e, portanto, não foi incluso. Nosso principal objetivo é o desempenho das estruturas e algoritmos propostos.

Para a avaliação de desempenho, repetimos a execução da abordagem completa cem vezes para cada conjunto de dados. Cada consulta foi elaborada randomicamente, variando os operadores $(=, >, <, >=, <=, <>)$ e operandos (0 a 100) da consulta.

Os resultados da criação das estruturas auxiliares e o cálculo da sensibilidade para todos os conjuntos de dados são mostrados na Tabela 5. O tempo para computação da sensibilidade se mostrou bastante eficiente, mesmo no caso do maior conjunto de dados. Mesmo para os dados do Google+ que possui mais de 100 mil nós e mais de 13 milhões de arestas, a abordagem levou menos de um segundo para calcular a sensibilidade. Em contrapartida, o tempo necessário para criar a estrutura auxiliar levou $50,565$ minutos para finalizar. Por isso, a conclusão a que se

chega, é que a criação da estrutura auxiliar leva um tempo considerável, portanto deve ser um trabalho realizado *off-line*, conforme definido na abordagem proposta.

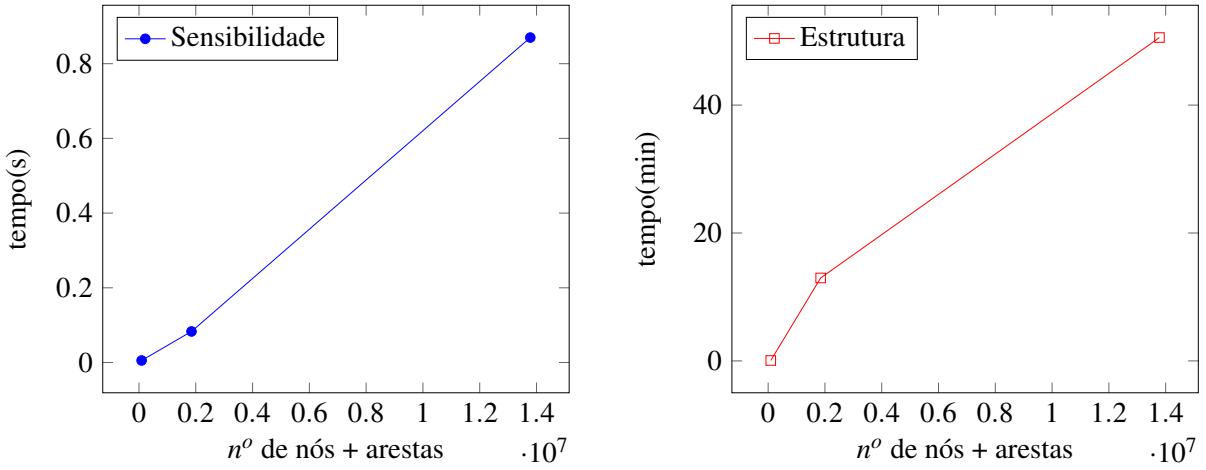
Tabela 5 – Desempenho da nossa abordagem para o cálculo da sensibilidade e a construção da estrutura.

Conjuntos de dados	**Nós**	**Arestas**	**Tempo(s)**	**Estrutura(min)**
Facebook	4.039	88.234	0,0054	0,0664
Twitter	81.306	1.768.149	0,0831	12,969
Google+	107.614	13.673.453	0,87	50,565

Fonte: Elaborado pelo autor

Na Figura 23 também é possível visualizar a relação entre o número de nós e arestas de cada conjunto de dados utilizado nos experimentos com o tempo necessário para computação da sensibilidade e construção da estrutura auxiliar para os três conjuntos de dados. O comportamento linear descreve que o desempenho do sistema é controlado pela variação do tamanho do conjunto de dados.

Figura 23 – Relação entre número de nós e arestas, o tempo da computação da sensibilidade (a) e tempo de criação da estrutura auxiliar (b).



Fonte: Elaborado pelo autor

Então, apenas para base de comparação, foi executada uma abordagem ingênua que consiste em executar n consultas, uma para cada conjunto de dados vizinho, onde n é o número de nós de indivíduos. Utilizou-se o Apache Jena para extrair e manipular dados em RDF. Para o conjunto de dados do Facebook com 4039 nós, levou $0,002$ segundos em média (100 consultas executadas) para calcular um vizinho, ou seja, $0,002 * 4039 = 8,078$ segundos para obter a sensibilidade. Mesmo sem considerar as demais etapas – determinar os vizinhos e o cálculo sobre os resultados para computar a sensibilidade – o tempo resultante é muito maior do que

$0,0054$ segundos no total da nossa abordagem.

5.4 Conclusão

Neste capítulo foi verificada a efetividade da abordagem proposta utilizando dados reais de redes sociais, explorando a utilidade das respostas e o desempenho geral da abordagem com diferentes tamanhos dos dados, diversos tipos de consultas de contagem e variando o parâmetro de privacidade ε.

Por meio dos resultados experimentais, a abordagem apresenta bons resultados de utilidade sobre consultas as quais o valor de ε tende ao valor 1 e melhores resultados em termos de privacidade quando ε vale 0.01. Isso já era esperado em uma solução diferencialmente privada conforme sua definição, visto que na definição da Privacidade Diferencial, valores pequenos de ε implicam menos utilidade. Dessa forma, a escolha de ε depende do objetivo da aplicação. Para aplicações que utilizam a abordagem proposta e necessitam de uma maior privacidade, recomenda-se utilizar valores baixos para o limite de privacidade ε. Em contrapartida, para aplicações que necessitam que as respostas tenham mais utilidade, recomenda-se utilizar valores altos para ε.

Outro fator a considerar sobre a abordagem proposta é que ela conseguiu obter um bom tempo médio de resposta para o cálculo da sensibilidade em todos os conjuntos de dados. No pior caso, para os dados do facebook (com mais de 4 mil nós e mais de 88 mil arestas), o cálculo realizado para a sensibilidade foi de $0,0054$ segundos. Por outro lado, a etapa de construção da estrutura auxiliar varia linearmente de acordo com a quantidade de dados, obedecendo a complexidade vista na Seção 4.2.2 que equivale a $\Theta(n+m)$, onde n é o número de vértices e m é o número de arestas. Apesar de levar um tempo considerável para construir a estrutura, essa etapa pode ser realizada antes da realização das consultas. Dessa forma, é necessário preparar os dados, criando a estrutura auxiliar, antes que as consultas sejam realizas para diminuir o tempo de resposta total da abordagem.

6 CONSIDERAÇÕES FINAIS

6.1 Conclusão

Conforme cresce a popularidade das redes sociais, cresce o número de usuários e, consequentemente, a quantidade de dados de caráter pessoal, levando a problemas com a privacidade dos indivíduos. Os dados sobre as pessoas e suas relações são potencialmente sensíveis e devem ser tratadas com cuidado, a fim de evitar possíveis riscos de violação de privacidade. Como forma de evitar esses riscos, neste trabalho foi investigado o problema de garantia de privacidade de dados em RDF no contexto de redes sociais que considere o relacionamento entre indivíduos. Desse modo, essa dissertação apresentou uma abordagem que garante a privacidade de indivíduos para consultas estatísticas sobre os grafos RDF no contexto de redes sociais, mesmo considerando impactante a remoção (ou adição) de um indivíduo na garantia de privacidade para consultas desse tipo. Esse impacto é devido à interdependência que existe entre os indivíduos quando a consulta tem um relacionamento como predicado. Para oferecer garantias fortes de privacidade, foi aplicado o modelo Privacidade Diferencial em dados RDF, formato pouco explorado na literatura em trabalhos que investigam esse modelo. Um dos desafios da aplicação desse modelo de privacidade é o cálculo da sensibilidade. A abordagem proposta demonstrou como calcular a sensibilidade das consultas no grafo de representação dos dados RDF.

Os objetivos propostos neste trabalho foram cumpridos. Primeiramente, investigou-se as técnicas de privacidade para dados RDF, analisando trabalhos relacionados com a abordagem proposta, apontando as semelhanças e diferenças. A noção de sensibilidade de elementos em dados explicitamente interligados numa estrutura de grafo foi redefinida e uma estrutura de dados auxiliar que facilita o processo do cálculo dessa sensibilidade foi proposta e desenvolvida.

Foram apresentados experimentos em dados reais a fim de avaliar a abordagem proposta com base na utilidade dos dados para análise e no desempenho. Uma análise do *trade-off* entre utilidade e privacidade foi realizada, mostrando que a quantidade de ruído adicionado ao conjunto de dados ainda produz resultados úteis para análise, enquanto ao mesmo tempo atende à garantia de Privacidade Diferencial que é independente de qualquer conhecimento prévio de um atacante.

Segundo os resultados, a abordagem apresentou ótimo desempenho no cálculo da sensibilidade, retornando resultados em um curto intervalo de tempo, menos de 1 segundo, para

dados com mais de 100 mil nós de mais de 13 milhões de arestas. Apesar do baixo tempo médio de resposta para o cálculo da sensibilidade, o tempo para a construção da estrutura auxiliar ainda é relativamente alto, 50.5 minutos para o teste com o maior conjunto de dados. Por isso, é recomendado que essa operação seja realizada *off-line*.

De um modo geral, este trabalho contribuiu para a compreensão da preservação da privacidade de indivíduos em dados de redes sociais em formato RDF. Além disso, conclui-se que nenhum trabalho anterior apresenta uma solução que trata desde a submissão de uma consulta a uma base de dados RDF até o retorno da resposta com garantia de privacidade diferencial, sendo capaz de lidar com o custo de computação da sensibilidade para consultas com propriedades de associação entre indivíduos como critério de seleção para o contexto de redes sociais, o que foi comprovado com experimentos nesta dissertação.

6.2 Trabalhos Futuros

Existem algumas oportunidades de trabalhos futuros que derivam da pesquisa realizada neste trabalho, incluindo:

- Investigar extensões às contribuições apresentadas para outros contextos e para outros tipos de consultas estatísticas. Por exemplo, dados médicos e consultas de máximo e mínimo valor.
- Investigar o cálculo da sensibilidade de forma dinâmica.
- Investigar a possibilidade de definir o ε a partir do resultado de consultas anteriores partindo de uma heurística específica.
- Adicionar suporte a atualização do conjunto de dados.
- Realizar uma melhor investigação sobre o limiar do número de consultas permitidas em relação a cada tipo de consulta a fim de aprimorar a Etapa 3 da abordagem.
- Investigar a viabilidade para atualização da estrutura de dados auxiliar para cenários *on-line*.
- Paralelizar a construção da estrutura auxiliar e calcular o custo de armazenamento gerado para manter a estrutura.

REFERÊNCIAS

AGGARWAL, C. C. An introduction to social network data analytics. **Social network data analytics**, Springer, p. 1–15, 2011.

ALVIM, M. S.; ANDRÉS, M. E.; CHATZIKOKOLAKIS, K.; DEGANO, P.; PALAMIDESSI, C. Differential privacy: On the trade-off between utility and information leakage. **Formal Aspects in Security and Trust**, Springer, v. 7140, p. 39–54, 2011.

ARON, Y. **Information Privacy for Linked Data**. Tese (PhD dissertation) — Massachusetts Institute of Technology, 2013.

BACKSTROM, L.; DWORK, C.; KLEINBERG, J. Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography. In: ACM. **Proceedings of the 16th international conference on World Wide Web**. [S.l.], 2007. p. 181–190.

BECHHOFER, S. Owl: Web ontology language. In: ____. **Encyclopedia of Database Systems**. [S.l.]: Springer, 2009. p. 2008–2009.

BRAIN, S. **Google Plus Demographics Statistics**. 2017. Disponível em: <http://www.statisticbrain.com/google-plus-demographics-statistics/>.

BRANCO JR, E. C.; MACHADO, J. C.; MONTEIRO, J. M. Estratégias para proteção da privacidade de dados armazenados na nuvem. **Simpósio Brasileiro de Banco de Dados. Citado na pág**, v. 6, 2014.

BRITO, F. T.; MACHADO, J. C. Preservação de privacidade de dados: Fundamentos, técnicas e aplicações. **Simpósio Brasileiro de Banco de Dados**, p. 40, 07 2017.

CHEN, C.-L.; PAL, R.; GOLUBCHIK, L. Oblivious mechanisms in differential privacy: Experiments, conjectures, and open questions. In: IEEE. **Security and Privacy Workshops (SPW), 2016 IEEE**. [S.l.], 2016. p. 41–48.

CHEN, S.; ZHOU, S. Recursive mechanism: towards node differential privacy and unrestricted joins. In: ACM. **Proceedings of the 2013 ACM SIGMOD International Conference on Management of Data**. [S.l.], 2013. p. 653–664.

CLARK, K. G.; FEIGENBAUM, L.; TORRES, E. Serializing sparql query results in json. **World Wide Web Consortium**, 2007.

COSTEA, S.; BARBU, M.; RUGHINIS, R. Qualitative analysis of differential privacy applied over graph structures. In: IEEE. **Roedunet International Conference (RoEduNet), 2013 11th**. [S.l.], 2013. p. 1–4.

CYNTHIA, D. Differential privacy. **Automata, languages and programming**, p. 1–12, 2006.

DIJKSTRA, E. W. A note on two problems in connexion with graphs. **Numerische mathematik**, Springer, v. 1, n. 1, p. 269–271, 1959.

DOMINGO-FERRER, J.; SÁNCHEZ, D.; SORIA-COMAS, J. Database anonymization: privacy models, data utility, and microaggregation-based inter-model connections. **Synthesis Lectures on Information Security, Privacy, & Trust**, Morgan & Claypool Publishers, v. 8, n. 1, p. 1–136, 2016.

DWORK, C. Differential privacy: A survey of results. In: SPRINGER. **International Conference on Theory and Applications of Models of Computation**. [S.l.], 2008. p. 1–19.

DWORK, C.; LEI, J. Differential privacy and robust statistics. In: ACM. **Proceedings of the forty-first annual ACM symposium on Theory of computing**. [S.l.], 2009. p. 371–380.

DWORK, C.; SMITH, A. Differential privacy for statistics: What we know and what we want to learn. **Journal of Privacy and Confidentiality**, v. 1, n. 2, p. 2, 2010.

EUROPEU, P. **Lei de Proteção dos dados pessoais**. 2017. Disponível em: <http://www.europarl.europa.eu>.

FACEBOOK. **Facebook.com. Company info**. 2017. Disponível em: <http://newsroom.fb.com/company-info/>.

FEDER, T.; NABAR, S. U.; TERZI, E. Anonymizing graphs. **arXiv preprint arXiv:0810.5578**, 2008.

FILHO, F. W.; LÓSCIO, B. F. **Web semântica: conceitos e tecnologias**. 2015.

FOAF. **FOAF Vocabulary Specification**. 2017. Disponível em: <http://xmlns.com/foaf/spec/>.

FUNG, B.; WANG, K.; CHEN, R.; YU, P. S. Privacy-preserving data publishing: A survey of recent developments. **ACM Computing Surveys (CSUR)**, ACM, v. 42, n. 4, p. 14, 2010.

FUNG, B.; WANG, K.; CHEN, R.; YU, P. S. Privacy-preserving data publishing: A survey of recent developments. **ACM Computing Surveys (CSUR)**, ACM, v. 42, n. 4, p. 14, 2010.

GENG, Q.; VISWANATH, P. The optimal mechanism in differential privacy. **arXiv preprint arXiv:1212.1186**, 2012.

GRAU, B. C.; KOSTYLEV, E. V. Logical foundations of privacy-preserving publishing of linked data. In: **AAAI**. [S.l.: s.n.], 2016. p. 943–949.

HAN, J.; PEI, J.; KAMBER, M. **Data mining: concepts and techniques**. [S.l.]: Elsevier, 2011.

HAY, M.; LI, C.; MIKLAU, G.; JENSEN, D. Accurate estimation of the degree distribution of private networks. In: IEEE. **Data Mining, 2009. ICDM'09. Ninth IEEE International Conference on**. [S.l.], 2009. p. 169–178.

HAY, M.; SRIVASTAVA, S.; WEIS, P. Privacy and anonymity in graph data. 2006.

HORROCKS, I. Owl: A description logic based ontology language. In: SPRINGER. **ICLP**. [S.l.], 2005. v. 3668, p. 1–4.

ISOTANI, S.; BITTENCOURT, I. I. **Dados Abertos Conectados: Em busca da Web do Conhecimento**. [S.l.]: Novatec Editora, 2015.

IYENGAR, V. S. Transforming data to satisfy privacy constraints. In: ACM. **Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining**. [S.l.], 2002. p. 279–288.

JENA, A. **A free and open source Java framework for building Semantic Web and Linked Data applications**. 2017. Disponível em: <https://jena.apache.org/>.

KARWA, V.; RASKHODNIKOVA, S.; SMITH, A.; YAROSLAVTSEV, G. Private analysis of graph structure. In: . [S.l.: s.n.], 2011. v. 4, n. 11, p. 1146–1157.

KASIVISWANATHAN, S. P.; NISSIM, K.; RASKHODNIKOVA, S.; SMITH, A. Analyzing graphs with node differential privacy. In: **Theory of Cryptography**. [S.l.]: Springer, 2013. p. 457–476.

KHANDELWAL, A.; BAO, J.; KAGAL, L.; JACOBI, I.; DING, L.; HENDLER, J. A. Analyzing the air language: A semantic web (production) rule language. In: SPRINGER. **RR**. [S.l.], 2010. p. 58–72.

LEE, J.; CLIFTON, C. How much is enough? choosing e for differential privacy. **Information Security**, Springer, v. 7001, p. 325–340, 2011.

LESKOVEC, J.; KREVL, A. **SNAP Datasets: Stanford Large Network Dataset Collection**. 2014. <http://snap.stanford.edu/data>.

LI, C.; HAY, M.; RASTOGI, V.; MIKLAU, G.; MCGREGOR, A. Optimizing linear counting queries under differential privacy. In: ACM. **Proceedings of the twenty-ninth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems**. [S.l.], 2010. p. 123–134.

LI, N.; LI, T.; VENKATASUBRAMANIAN, S. t-closeness: Privacy beyond k-anonymity and l-diversity. In: IEEE. **Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on**. [S.l.], 2007. p. 106–115.

LI, Y.; SHEN, H. Anonymizing graphs against weight-based attacks. In: IEEE. **Data Mining Workshops (ICDMW), 2010 IEEE International Conference on**. [S.l.], 2010. p. 491–498.

LINKEDIN. **LinkedIn: A maior rede profissional do mundo**. 2017. Disponível em: <https://br.linkedin.com/>.

LIU, K.; TERZI, E. Towards identity anonymization on graphs. In: ACM. **Proceedings of the 2008 ACM SIGMOD international conference on Management of data**. [S.l.], 2008. p. 93–106.

MACHANAVAJJHALA, A.; GEHRKE, J.; KIFER, D.; VENKITASUBRAMANIAM, M. l-diversity: Privacy beyond k-anonymity. In: IEEE. **Data Engineering, 2006. ICDE'06. Proceedings of the 22nd International Conference on**. [S.l.], 2006. p. 24–24.

MAYIL, S.; VANITHA, M. A review on privacy preserving in social network. **International Journal of Scientific Engineering Research**, 2017.

NABAR, S. U.; MARTHI, B.; KENTHAPADI, K.; MISHRA, N.; MOTWANI, R. Towards robustness in query auditing. In: VLDB ENDOWMENT. **Proceedings of the 32nd international conference on Very large data bases**. [S.l.], 2006. p. 151–162.

NARAYANAN, A.; SHMATIKOV, V. De-anonymizing social networks. In: IEEE. **Security and Privacy, 2009 30th IEEE Symposium on**. [S.l.], 2009. p. 173–187.

NEO4J. **Neo4j Graph Database**. 2017. Disponível em: <https://neo4j.com/>.

NGUYEN, H. H.; KIM, J.; KIM, Y. Differential privacy in practice. **Journal of Computing Science and Engineering**, Nguyen Hiep H.; Kim Jong; Kim Yoonho, v. 7, n. 3, p. 177–186, 2013.

NISSIM, K.; RASKHODNIKOVA, S.; SMITH, A. Smooth sensitivity and sampling in private data analysis. In: ACM. **Proceedings of the thirty-ninth annual ACM symposium on Theory of computing**. [S.l.], 2007. p. 75–84.

PRUD, E.; SEABORNE, A. *et al.* Sparql query language for rdf. 2006.

SANKAR, L.; RAJAGOPALAN, S. R.; POOR, H. V. Utility-privacy tradeoffs in databases: An information-theoretic approach. **IEEE Transactions on Information Forensics and Security**, IEEE, v. 8, n. 6, p. 838–852, 2013.

SARATHY, R.; MURALIDHAR, K. Evaluating laplace noise addition to satisfy differential privacy for numeric data. **Trans. Data Privacy**, v. 4, n. 1, p. 1–17, 2011.

SHADBOLT, N.; BERNERS-LEE, T.; HALL, W. The semantic web revisited. **IEEE intelligent systems**, IEEE, v. 21, n. 3, p. 96–101, 2006.

SHOARAN, M.; THOMO, A.; WEBER, J. H. Differential privacy in practice. In: SPRINGER. **Secure Data Management**. [S.l.], 2012. p. 14–24.

SILVA, R. R. C.; LEAL, B. C.; BRITO, F. T.; VIDAL, V. M.; MACHADO, J. C. A differentially private approach for querying rdf data of social networks. In: ACM. **Proceedings of the 21st International Database Engineering & Applications Symposium**. [S.l.], 2017. p. 74–81.

SWEENEY, L. k-anonymity: A model for protecting privacy. **International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems**, World Scientific, v. 10, n. 05, p. 557–570, 2002.

TASK, C.; CLIFTON, C. A guide to differential privacy theory in social network analysis. In: IEEE COMPUTER SOCIETY. **Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012)**. [S.l.], 2012. p. 411–417.

TECH, C. **Twitter is now losing users in the U.S.** 2017. Disponível em: <http://money.cnn.com/2017/07/27/technology/business/twitter-earnings/index.html>.

VIDAL, V. M.; CASANOVA, M. A.; MENENDEZ, E. S.; ARRUDA, N.; PEQUENO, V. M.; LEME, L. A. P. Using changesets for incremental maintenance of linkset views. In: SPRINGER. **International Conference on Web Information Systems Engineering**. [S.l.], 2016. p. 196–204.

WANG, Y.; WU, X. Preserving differential privacy in degree-correlation based graph generation. **Transactions on data privacy**, NIH Public Access, v. 6, n. 2, p. 127, 2013.

WONG, R. C.; FU, A. W. **Privacy-Preserving Data Publishing: An Overview**. [S.l.]: Morgan & Claypool Publishers, 2010. (Synthesis Lectures on Data Management).

XIAO, X.; BENDER, G.; HAY, M.; GEHRKE, J. ireduct: Differential privacy with reduced relative errors. In: ACM. **Proceedings of the 2011 ACM SIGMOD International Conference on Management of data**. [S.l.], 2011. p. 229–240.

ZHELEVA, E.; GETOOR, L. Privacy in social networks: A survey. In: **Social network data analytics**. [S.l.]: Springer, 2011. p. 277–306.