Capítulo 1

Técnicas de Privacidade de Dados de Localização

Javam C. Machado, Eduardo R. Duarte Neto, and Manuel E. Bento Filho [1]

Abstract

The development of mobile devices has led to the growing popularity of location services, allowing unknown or untrusted servers to collect a large amount of information from the user's location data, which has raised serious concerns about the privacy of the user's sensitive information in the use of these services. Thus, maintaining user privacy while ensuring the quality of service is a complex problem that has received much attention in recent years. The objective of this chapter is to describe the problem of violating individuals' location privacy, presenting their main concepts, the inherent threats and pointing out in detail the main techniques in the literature for preserving privacy in location services. Finally, we will highlight research opportunities in the area and present relevant conclusions on the subject.

Resumo

O desenvolvimento dos dispositivos móveis tem proporcionado o crescimento da popularidade dos serviços de localização, permitindo que servidores desconhecidos ou não confiáveis coletem uma grande quantidade de informação dos usuários a partir de seus dados de localizações, o que tem gerado sérios questionamentos sobre a privacidade das informações sensíveis dos usuários no uso destes serviços. Sendo assim, manter a privacidade dos usuário, e simultaneamente, garantir a qualidade do serviço é um problema complexo que tem recebido bastante atenção nos últimos anos. Este capítulo tem por objetivo descrever o problema da violação de privacidade de dados de localização dos indivíduos, apresentando seus principais conceitos, os riscos inerentes e apontando de forma detalhada as principais técnicas existentes na literatura para a preservação de privacidade em serviços de localização. Por fim, iremos destacar oportunidades de pesquisas na área e apresentar conclusões relevantes sobre o tema.

[1]LSBD/DC – Universidade Federal do Ceará

1.1. Introdução

Com o passar dos anos a quantidade de dados coletados por aplicativos a fim de prover serviços tem crescido bastante. Estes dados são muito valiosos para os diversos tipos de organizações, sejam elas de saúde, varejo, dentre outras. Por exemplo, muitas empresas da área de varejo traçam estratégias de vendas de acordo com o perfil de seus consumidores, através da análise dos dados de seus consumidores, assim, potencializando o lucro da empresa. Já na área de saúde é possível identificar quais regiões estão mais sujeitas ou não a uma doença. Esse tipo de análise só é possível graças à análise de dados privados de indivíduos. Entretanto, isto leva a sérios riscos de exposição de dados sensíveis dos indivíduos. Logo, encontrar uma forma de permitir esta análise sem que haja riscos a exposição dos mesmos tem sido objeto de estudo na área de privacidade de dados.

O desenvolvimento dos dispositivos móveis tem contribuído bastante para a popularidade dos serviços baseado em localização (LBS), que utilizam de informações de localização para atender seus usuários. Através dos sensores destes dispositivos, as coordenadas de latitude e longitude são obtidas e utilizadas por estes serviços. Segundo Schiller [27], os serviços de localização são definidos como serviços que integram a localização ou posição de um dispositivo móvel a outras informações, de modo a fornecer valor agregado a um usuário. Estes numerosos serviços, tais como navegação, redes sociais, serviços de recomendação, jogos de realidade aumentada, entre outros, tem sido desenvolvidos e integrados às atividades diárias das pessoas, provendo informações úteis sobre seus arredores e sendo capazes de responder perguntas do dia a dia como: qual a melhor rota a ser percorrida para um determinado endereço? Quais os pontos turísticos mais próximos da minha localização atual? Em quanto tempo o táxi que eu solicitei irá demorar para chegar em meu apartamento?

O uso das informações geradas pelos serviços de localização pode beneficiar várias aplicações. De fato, muitas empresas e agências governamentais tem obtido conhecimento sobre os dados associados às atividades praticadas nas localizações, seja para melhorar o serviço prestado, para o lançamento de um novo produto, ou até mesmo para gerar uma nova política pela empresa. Entretanto, acessar dados de localizações de usuários desses serviços, mesmo que com permissão, levanta severas preocupações de privacidade para a maioria dos usuários. Dessa forma, a utilização de serviços baseados em localização pode levar a sérios riscos de violação de privacidade devido a provedores de serviços não confiáveis [20], que podem expor os dados de localização de seus usuários ou até mesmo vender suas informações de localizações a terceiros [35]. De posse dessas informações, os dados obtidos por terceiros são utilizados para descoberta de dados sensíveis dos usuários, *i.e.*, dados de saúde, crenças religiosas, ideologias políticas, questões raciais, preferências sexuais, dentre várias outras.

A Figura 1.1 ilustra um típico exemplo de violação de privacidade no uso de serviços de localização. Em questão, o usuário Bob ao longo do tempo realiza várias requisições a um serviço baseado em localização. No tempo t_1 Bob estava próximo ao pronto-socorro de um hospital, já em um tempo t_2 Bob realiza uma nova consulta próxima a um laboratório de patologia, em outros dois momentos sua localização também esta próximo à localizações associadas a área de saúde. Considerando que é de conhecimento do provedor do serviço as requisições feitas pelos usuários, o próprio provedor

facilmente consegue inferir, com alta probabilidade, que Bob possui algum tipo de doença em razão das localizações enviadas por ele ao provedor, revelando uma informação sensível do usuário. Desta forma, considerando que o provedor de serviço pode não ser confiável, o risco de uma violação de privacidade, portanto, é bastante alto, deixando o usuário exposto.

Figura 1.1. Exemplo de requisições realizadas próximas a hospitais e clínicas, permitindo inferências de dados sensíveis do usuário.

A aplicação de modelos de privacidade sobre requisições de usuários é imprescindível para evitar que as localizações dos indivíduos não sejam identificadas pelos provedores no uso destes serviços. Todavia, em geral os modelos de privacidade acabam provocando mudanças nos dados, afetando diretamente a sua utilidade, com impacto direto na qualidade do serviço. Portanto, gerenciar essa solução de compromisso (*trade-off*, Figura 1.2) entre privacidade dos indivíduos e utilidade dos seus dados se torna um outro grande desafio. Desta forma, vários modelos de privacidade de dados têm sido propostos por pesquisadores com o objetivo de resolver esta questão.

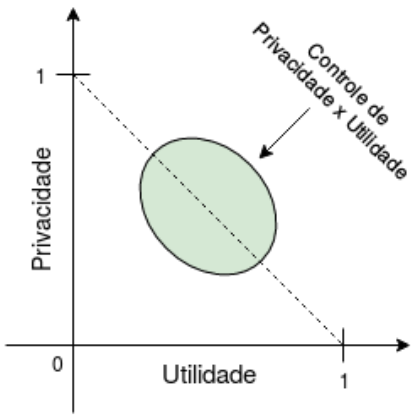

Figura 1.2. Trade-off entre privacidade e utilidade

Este capítulo tem por objetivo introduzir os fundamentos e técnicas para preservação da privacidade de dados dos indivíduos, procurando apresentar os riscos mais comuns

e as técnicas mais populares na solução do problema. Em seguida, apresentaremos um aprofundamento sobre o tema privacidade de dados de localização, apontando os conceitos básicos sobre dados de localização, os tipos de ataques a que estão sujeitos, e os principais modelos de preservação de privacidade de dados de localização na atualidade. A Seção 1.2 apresenta os princípios básicos sobre o tema, que tipos de dados estão sujeitos a violação, e como a preservação de privacidade pode ser alcançada. A Seção 1.3 apresenta os principais tipos de ataque utilizados para violação à privacidade dos indivíduos. Os modelos sintáticos mais populares para preservação de privacidade são descritos na Seção 1.4. A Seção 1.5 apresenta o modelo de privacidade diferencial. Na Seção 1.6 apresentamos o tema privacidade de localização, descrevendo o modelo de serviços de localização, bem como as características dos dados de localização. A Seção 1.7 descreve os principais tipos de ataque que dados de localização estão sujeitos. Os modelos de privacidade em dados de localização são descritos na Seção 1.8. E por fim, a Seção 1.9 apresenta as considerações finais do capítulo.

1.2. Privacidade de Dados

Privacidade é o direito que um indivíduo tem de manter seus assuntos pessoais e relacionamentos secretos [8]. É um consenso entre os pesquisadores que a privacidade é um assunto complexo, com muitas questões envolvidas. Sendo bastante comum confundir os conceitos de privacidade e segurança. Apesar de privacidade e segurança serem temas relacionados, suas definições tratam de pontos bem distintos. Em se tratando de dados, a segurança visa regular o acesso durante todo o ciclo de vida do dado, enquanto a privacidade define como será realizado esse acesso, em geral 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 se refere 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. A privacidade aqui, está associada a regras de controle de acesso efetivas, que permitem a revelação da informação apenas por usuários autorizados. Contudo, a privacidade dos indivíduos não está garantida apenas com o controle de acesso eficiente, visto que os usuários com acesso àquelas informações podem ser maliciosos, e assim capazes de divulgar informações sensíveis acerca daqueles indivíduos.

Com o desenvolvimento dos dispositivos móveis, a quantidade de dados coletados para o uso dos diversos serviços existentes tem crescido bastante, tornando a privacidade de dados muitas vezes uma moeda de troca, onde o usuário abre mão da sua privacidade em favor da prestação destes serviços. Nesse contexto, é importante identificar quais os tipos de dados não devem ser divulgados, a fim de garantir a aplicação de técnicas que permitam a proteção destes dados. Todavia os dados essenciais aos serviços devem ser fornecidos ao provedor para que este possa prestar o serviço na qualidade necessária ao usuário.

1.2.1. Privacidade em Microdados

Em geral, os dados são representados por uma tabela, onde cada linha corresponde a um registro do conjunto de dados e as colunas a atributos destes registros. A estes dados assim representados dá-se o nome de microdados. Neles cada registro corresponde a um

indivíduo e os atributos se referem a características ou propriedades do indivíduos. Por sua vez, no contexto de privacidade, os atributos podem ser classificados em [14]:

1. **Identificadores explícitos**: são aqueles atributos que identificam de maneira única os indivíduos, como "CPF", "nome", etc., e devem ser removidos antes da publicação dos dados;

2. **Semi-identificadores**: são aqueles que não são identificadores explícitos, mas podem identificar o usuário, quando relacionados. "Data de nascimento"e "CEP"são exemplos de atributos semi-identificadores;

3. **Atributos sensíveis**: possuem informações sensíveis a cerca dos indivíduos, como "doença", salário", etc.;

4. **Atributos não sensíveis**: são aqueles que não se enquadram em nenhuma das categorias citadas anteriormente.

Os atributos sensíveis são aqueles de maior interesse no nosso contexto porque apresentam potenciais danos ao seus donos em caso de divulgação. Por esse motivo, tais atributos necessitam ser protegidos. A Tabela 1.1 ilustra um exemplo de registros de indivíduos contendo atributos identificadores explícitos e semi-identificadores, que precisam ser protegidos.

Identificadores Explícitos		**Semi-identificadores**			
ID	**Nome**	**Idade**	**Gênero**	**Endereço**	**Telefone**
1	Isabela	22	Feminino	Av. I	99998 1324
2	João	25	Masculino	Av. K	99998 1454
3	Iago	25	Masculino	Av. K	99998 3245
4	Maria	31	Feminino	Rua J	99998 3465

Tabela 1.1. Exemplos de identificadores explícitos e semi-identificadores em dados tabulados de indivíduos.

1.2.2. Proteção e Privacidade de Dados

A fim de estabelecer a confiança dos indivíduos e o consentimento para a utilização dos seus dados, faz-se necessário garantir a proteção dos dados pessoais coletados. A abordagem mais promissora para solucionar o problema da preservação de privacidade consiste em anonimizar os dados antes de sua liberação para uso [15], visando impedir a exposição de dados sensíveis dos indivíduos. No processo de anonimização, um conjunto de dados D é transformado em um conjunto de dados D', por meio de modificações sobre os dados. Esta transformação se dá por meio de técnicas de *generalização*, *supressão* e *pertubação*.

A generalização modifica os atributos semi-identificadores dos registros por valores mais gerais, aumentando a incerteza de um adversário associar um indivíduo a seus dados, ou a atributos sensíveis, no conjunto de dados. Na abordagem mais comum de

generalização, o valor de um atributo semi-identificador que se deseja proteger nos diferentes registros é substituído por um valor generalizado. A Figura 1.3 ilustra o processo de generalização sobre o atributo Telefone dos registros da Tabela 1.1, onde, nas folhas da árvore, têm-se os valores originais para o atributo Telefone. No segundo nível agrupam-se os telefones cujos 6 primeiros dígitos correspondem, enquanto que no nível seguinte em direção ao topo da hierarquia são agrupados os telefones cujos 5 primeiros dígitos correspondem.

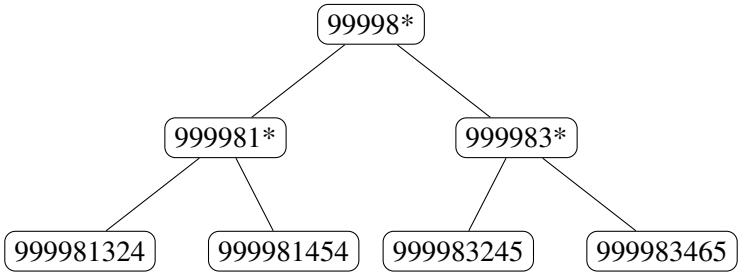

Figura 1.3. Exemplos de generalização do atributo semi-identificador Telefone.

Voltando à Tabela 1.1, após passar por um processo de anonimização por generalização dos valores do atributo Telefone até o topo da hierarquia, a publicação dos dados definidos como semi-identificadores poderia ser realizada de acordo com os valores observados na Tabela 1.2. Veja que este processo dificulta a re-identificação de um dos indivíduos caso seja de conhecimento externo o número do telefone deste indivíduo.

Identificadores Explícitos		**Semi-identificadores**			
ID	**Nome**	**Idade**	**Gênero**	**Endereço**	**Telefone**
1	Isabela	22	Feminino	Av. I	99998*
2	João	25	Masculino	Av. K	99998*
3	Iago	25	Masculino	Av. K	99998*
4	Maria	31	Feminino	Rua J	99998*

Tabela 1.2. Exemplo de semi-identificador anonimizado por generalização.

A supressão de dados remove valores ou substitui um ou mais valores de um conjunto de dados por algum valor especial, possibilitando a não descoberta de semi-identificadores por adversários. Alguns dos principais tipos de supressão:

- **Supressão de registro**: a supressão de registro remove um registro inteiro do conjunto de dados, consequentemente nenhum valor de atributo é disponibilizado para uso [5, 19].
- **Supressão de valor**: a supressão de valor remove ou substitui todas as ocorrências de um valor de um atributo semi-identificador por um valor especial, como "*". Por exemplo, em uma tabela de funcionários de uma empresa, os valores de atributo salário abaixo de R$ 30.000,00, podem ser removidos ou substituídos por "*", enquanto os demais valores não sofrem distorções [33, 34].

- **Supressão de células**: nessa técnica, apenas algumas instâncias de valores de um atributo são removidas ou substituídas por um valor especial, caracterizando uma *supressão local* [23]. Por exemplo, pode-se remover apenas metade dos valores de atributo salário abaixo de R$ 30.000,00, em uma tabela de empregados. Assim, instâncias de salário podem conter valores abaixo ou acima de R$ 30.000,00, além de valores suprimidos. Entretanto, essa estratégia pode levar a inconsistências em eventuais análises de dados.

Por último, mas, não menos importante, a perturbação substitui 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 sobre os dados perturbados. As técnicas mais comuns de perturbação de dados são:

- **Adição de ruído**: essa técnica é aplicada comumente sobre atributos numéricos. Ela substitui o valor original "v" de um atributo por "$v + r$", em que "r" é um valor, chamado de ruído, escolhido aleatoriamente a partir de uma distribuição. O valor "v" do atributo também pode ser substituído por "$v \times r$". Os valores dos atributos são portanto, perturbados com um determinado nível de ruído, que pode ser adicionado ou multiplicado pelo valor original de cada atributo [31];

- **Permutação de dados**: nesta abordagem os valores de um mesmo atributo de dois registros diferentes são permutados. Isso mantém algumas características estatísticas dos dados, como frequência dos atributos e contagem [10]. Essa técnica não altera o domínio dos atributos, mas as possíveis permutações de valores diferentes podem levar a valores nos registros sem sentido, e com isso, informações equivocadas;

- **Geração de dados sintéticos**: nesta técnica, um modelo estático é inicialmente gerado a partir do conjunto de dados e, após isso, são gerados dados sintéticos que seguem o modelo gerado [1]. Esses dados sintéticos são os que devem ser disponibilizados para o uso final. A vantagem desta técnica é que todas as propriedades estatísticas dos dados são mantidas. Entretanto, pode-se gerar também alguns valores sem sentido e que não são condizentes com o mundo real.

Uma vez anonimizado os dados, através de técnicas de generalização, supressão ou perturbação, é possível permitir o compartilhamento de informações com outras entidades, as quais poderão utilizá-las para diversas finalidades, sem que haja violação de privacidade. Todavia, a modificação dos dados originais no processo de anonimização causa perda de utilidade dos mesmos. Portanto, é necessário encontrar um equilíbrio entre a proteção desejada e a utilidade dos dados, a fim de se permitir operações de agregação ou mesmo análise dos dados.

1.3. Ataques à Privacidade

O objetivo dos modelos de privacidade é preservar ao máximo possível a privacidade dos donos dos registros em um conjunto de dados. Já o objetivo do atacante, se opondo a

isso, é justamente utilizar de todos os recursos a sua disposição para retirar o máximo de informação dos registros. Dessa forma, o atacante muitas vezes necessita de conhecimentos prévios que o auxiliem a fazer inferências sobre o conjunto de dados. Por exemplo, o adversário que trabalha no mesmo local da vítima, pode possuir conhecimento sobre a mesma, tais como, endereço residencial e cargo na empresa, permitindo a inferência de informações sensíveis, como localização, opção sexual, etc. Em se tratando de publicação de dados, o atacante pode ter acesso a outros conjuntos de dados previamente publicados, e assim, cruzar referências para descobrir novas informações sensíveis da vítima. Portanto, podemos concluir que o conhecimento do adversário é imensurável e imprevisível e deve ser levado em consideração nas soluções de preservação de privacidade, apesar de suas características.

Um adversário é capaz de violar a privacidade dos usuários por meio de diversos ataques que citaremos a seguir:

- **Ataque de Ligação ao Registro:** este ataque tem por objetivo re-identificar o registro de um usuário, cujas informações pertencem ao conjunto de dados publicado;
- **Ataque de Ligação ao Atributo:** o objetivo do adversário é ser capaz de inferir atributos sensíveis do usuário mesmo sem re-identificar seu registro, com base nos valores sensíveis relacionados ao grupo que o usuário pertence.
- **Ataque de Ligação à Tabela:** este tipo de ataque assume que o adversário sabe que o registro do usuário foi publicado. Neste ataque o intuito é inferir se a vítima está presente ou ausente nos dados publicados.
- **Ataque Probabilístico:** este ataque tem o foco de destacar como o adversário mudaria seu pensamento probabilístico sobre um usuário depois de ter acesso ao conjunto de dados disponível.

1.4. Modelos de Privacidade Sintático

Os modelos de privacidade sintáticos procuram garantir a privacidade dos indivíduos ao exigir que, após o processo de anonimização, o conjunto de dados vai atender certas condições específicas da técnica aplicada. Para isto, estes modelos, usualmente aplicam uma transformação nos registros por meio de técnicas de supressão e/ou generalização até que esta condição seja alcançada. Iremos apresentar alguns dos modelos de privacidade sintático mais utilizados em preservação de dados.

1.4.1. k-anonimato

O k-anonimato é o modelo de privacidade mais conhecido no campo da anonimização de dados [30]. Esse modelo assegura que, para cada combinação de valores de semi-identificadores, existem pelo menos k registros no conjunto de dados, formando uma classe de equivalência. O k-anonimato atua sobre o princípio da indistinguibilidade, isto é, cada registro em um conjunto de dados k-anônimo é indistinguível de pelo menos outros $k-1$ registros em relação ao conjunto de semi-identificadores. Assim, garante-se que cada registro não pode ser ligado a um indivíduo por um adversário com probabilidade maior que $\frac{1}{k}$.

O valor de k define o nível de privacidade e, consequentemente, afeta diretamente a perda de utilidade. Assim, um valor de k grande implica em uma maior proteção dos dados, entretanto, diminui a utilidade dos mesmos, por ser necessário adicionar grande volume de ruído a fim de se alcançar classes de equivalência com pelo menos k registros. É importante ressaltar que não existem abordagens analíticas para determinar um valor ótimo para o parâmetro k [9], sendo este um problema NP-difícil [23]. Dessa forma, cabe aos *dataholders* esta complexa tarefa quando da aplicação do processo de anonimização por k-anonimato sobre um conjunto de dados.

A Tabela 1.3 ilustra a aplicação do modelo k-anonimato para $k = 2$. São atributos identificadores explícitos Placa, Motorista e CPF enquanto que são atributos sensíveis Tipo de Multa e Valor da Multa. Os atributos restantes semi-identificadores: Data de Nascimento e Data da Infração.

	Placa	**Motorista**	**CPF**	**Data de Nascimento**	**Data da Infração**	**Tipo de Multa**	**Valor da Multa (R$)**
1	UVW-1840	Gigi	223.512.956	14/03/1980	03/01/2013	1	170
2	AXO-2064	André Luis	523.512.511	04/03/1980	03/01/2013	2	250
3	AUG-1046	Juçara Silva	123.998.687	24/05/1980	03/01/2013	1	170
4	FBI-1001	Bruno Lima	230.320.523	20/04/1982	04/01/2013	1	170
5	ACO-6241	Abu Ali	221.320.876	20/05/1982	04/01/2013	2	250
6	ABA-5012	Pedro Ramires	210.329.890	13/05/1982	05/01/2013	2	250
7	HBV-2002	Eduardo Neto	538.687.045	15/05/1982	05/01/2013	1	170

Tabela 1.3. Dados sobre infrações de trânsito.

Em um processo de anonimização dos dados da Tabela 1.3 são aplicadas a supressão nos identificadores explícitos e a generalização nos atributos sensíveis, gerando a Tabela anonimizada 1.4. Nesta tabela podemos perceber quatro classes de equivalência para os semi-identificadores: Classe A = "$03/1980, 01/2013$" nas linhas 1 e 2; Classe B = "$05/1980, 01/2013$" registro 3; Classe C = "$04/1982, 01/2013$" com o registro 4 e Classe D = "$05/1982, 01/2013$" nas linhas 5, 6 e 7. Observe, que mesmo após aplicar um processo inicial de anonimização, o k-anonimato ainda não foi alcançado, já que as classes B e C, não possuem uma quantidade mínima requerida de 2 registros, sendo, portanto, necessário, algum novo processo de transformação. Uma estratégia, seria então remover os registros 3 e 4, como podemos observar na Tabela 1.5. Desta forma, agora observamos apenas 2 classes de equivalência, contendo a quantidade mínima de dois registros por classe, garantindo o k-anonimato.

1.4.2. l-diversidade

Assim como o k-anonimato, o l-diversidade age sobre o princípio da indistinguibilidade. Entretanto, o k-anonimato apesar de apresentar uma alta eficácia na prevenção contra ataques de ligação ao registro, não se mostra adequado contra ataques de ligação ao atributo, *i.e.*, ataques em que um adversário procura inferir informações sensíveis sobre registros mesmo sem identificá-los. Tomamos como exemplo a Tabela 1.5 que garante o k-anonimato, para $k = 2$, contendo pelo menos dois registros em cada uma das classes de equivalência. Observe, que se o atacante tiver conhecimento que o usuário Pedro Ramires nasceu em 05/1982, e recebeu uma infração em janeiro de 2013, ele poderá inferir com

	Placa	Motorista	CPF	Data de Nascimento	Data da Infração	Tipo de Multa	Valor da Multa (R$)
1	*	*	*	03/1980	01/2013	1	170
2	*	*	*	03/1980	01/2013	2	250
3	*	*	*	05/1980	01/2013	1	170
4	*	*	*	04/1982	01/2013	1	170
5	*	*	*	05/1982	01/2013	2	250
6	*	*	*	05/1982	01/2013	2	250
7	*	*	*	05/1982	01/2013	1	170

Tabela 1.4. Dados sobre informações de trânsito anonimizados.

	Placa	Motorista	CPF	Data de Nascimento	Data da Infração	Tipo de Multa	Valor da Multa (R$)
1	*	*	*	03/1980	01/2013	1	170
2	*	*	*	03/1980	01/2013	2	250
3	*	*	*	*	*	*	*
4	*	*	*	*	*	*	*
5	*	*	*	05/1982	01/2013	2	250
6	*	*	*	05/1982	01/2013	2	250
7	*	*	*	05/1982	01/2013	1	170

Tabela 1.5. Tabela no modelo *2*-anonimato.

uma probabilidade de $\frac{2}{3}$ que a multa recebida por Pedro foi de 250 reais. Superior à $\frac{1}{2}$, desejada pelo modelo k-anonimato.

O l-diversidade busca prover proteção contra ataques de ligação ao atributo, garantindo que para cada classe de equivalência, exista pelo menos l valores distintos para cada atributo sensível. Assim, o que se pretende é que um atacante, mesmo com conhecimento prévio sobre a classe de equivalência de um registro, não seja capaz de inferir o atributo sensível do mesmo com probabilidade maior que $\frac{1}{l}$.

Tomando por exemplo a Tabela 1.6, onde a probabilidade de se identificar que o indivíduo tem asma, valor do atributo sensível "Doença", caso o atacante tenha conhecimento de que o CEP do indivíduo é 540040, é de 100%, superior a $\frac{1}{4}$ exigido pelo modelo 4-anonimato. Convertendo a Tabela 1.6 para o modelo 3-diversidade, não é preciso fazer nenhuma alteração nos registros da classe A (linhas 1 a 4), pois esta já possui no mínimo 3 valores distintos para o atributo sensível. Entretanto, a classe B (linhas 5 a 8) possui todos os valores de atributos sensíveis iguais. Uma solução simples seria suprimir os registros das linha 5 a 8. Outra solução seria modificar os valores do atributo sensível destas linhas por valores diferentes que garantam a diversidade, conforme Tabela a 1.7 que atende, portanto, o modelo 4-anonimato e 3-diversidade.

Outros modelos foram propostos como uma extensão do l-diversidade, como o t-proximidade [21] e o p-sensibilidade [32], com a finalidade de prover uma maior garantia de preservação de privacidade tanto contra ataques de ligação ao registro, como ao atributo.

	Idade	CEP	Cidade	Doença
1	<70	560001	*	Sinusite
2	<70	560001	*	Gripe
3	<70	560001	*	Zika
4	<70	560001	*	Hérnia
5	<35	540040	*	Asma
6	<35	540040	*	Asma
7	<35	540040	*	Asma
8	<35	540040	*	Asma

Tabela 1.6. *4*-anonimato

	Idade	CEP	Cidade	Doença
1	<70	560001	*	Sinusite
2	<70	560001	*	Gripe
3	<70	560001	*	Zika
4	<70	560001	*	Hérnia
5	<35	540040	*	Sinusite
6	<35	540040	*	Zika
7	<35	540040	*	Asma
8	<35	540040	*	Asma

Tabela 1.7. *4*-anonimato e *3*-diversidade.

1.4.3. δ-presença

O δ-presença, uma extensão ao k-anonimato, é um modelo que busca proteger a privacidade de dados dos indivíduos contra ataques de ligação à tabela [24]. O modelo define o limite $\delta = \delta_{max}, \delta_{min}$ para a probabilidade de um adversário inferir a a presença de um indivíduo na tabela. Desta forma, indiretamente, o modelo também garante a privacidade contra ataques de ligação ao registro e ao atributo, uma vez que a probabilidade de um ataque de ligação ao registro ou ao atributo sensível ser bem sucedido está limitado por δ_{max}.

Para ilustrar um ataque de ligação à tabela, imagine um atacante que tem conhecimento sobre a Tabela A (1.8), no formato 4-anônimo, com duas classes de equivalência: E_1 (Vendedor, Feminino, [30,35]), 5 indivíduos; E_2 (Professor, Masculino,[35-40]), 4 indivíduos. Caso a Tabela B (1.9) seja publicada, onde todos os indivíduos de B estão em A, é possível identificar que a probabilidade de a vendedora Maria estar na Tabela B é de $\frac{4}{5}$, uma vez que há 5 registros na mesma classe de equivalência de Maria (E_1 em A), e que em B há apenas 4 registros na classe de equivalência E_1.

Nome	Profissão	Gênero	Idade
Lucas	Professor	Masculino	[35-40)
Isaías	Professor	Masculino	[35-40)
João	Professor	Masculino	[35-40)
Mateus	Professor	Masculino	[35-40)
Maria	Vendedor	Feminino	[30-35)
Fátima	Vendedor	Feminino	[30-35)
Marta	Vendedor	Feminino	[30-35)
Irene	Vendedor	Feminino	[30-35)
Natália	Vendedor	Feminino	[30-35)

Tabela 1.8. Tabela no formato *4*-anonimato.

Profissão	Gênero	Idade	Multa
Professor	Masculino	[35-40)	250
Professor	Masculino	[35-40)	300
Professor	Masculino	[35-40)	250
Vendedor	Feminino	[30-35)	250
Vendedor	Feminino	[30-35)	300
Vendedor	Feminino	[30-35)	450
Vendedor	Feminino	[30-35)	250

Tabela 1.9. Tabela de pacientes no formato *3*-anonimato.

A Tabela 1.10 apresenta a aplicação do δ-presença para um $\delta_{max} = \frac{1}{2}$, através da supressão de registros. As linhas 2, 5 e 6 foram removidas. Desta forma, a probabilidade de se identificar a presença de qualquer indivíduo da Tabela 1.8 na Tabela 1.9 é inferior ou igual a $\frac{1}{2}$.

Profissão	**Gênero**	**Idade**	**Multa**
Professor	Masculino	[35-40)	250
*	*	*	*
Professor	Masculino	[35-40)	250
Vendedor	Feminino	[30-35)	250
*	*	*	*
*	*	*	*
Vendedor	Feminino	[30-35)	250

Tabela 1.10. Tabela de pacientes no formato 3-anonimato e δ-presença.

1.5. Modelo de Privacidade Diferencial

Diferentemente dos modelos apresentados até agora, que buscam garantir a preservação de privacidade dos indivíduos na publicação de dados em formato tabulado , o modelo de Privacidade Deferencial procura garantir a preservação de privacidade na publicação de resultados de consultas. Seu objetivo é evitar que o conhecimento adversário do atacante aumente a probabilidade de se expor os indivíduos do conjunto de dados, ou seja, evitando ataques probabilísticos. Para isto, as respostas destas consultas são perturbadas, com a adição de ruído, como forma de garantir a privacidade dos indivíduos.

Proposta por Dwork [11], a Privacidade Diferencial (PD) consiste em um modelo matemático que oferece sólidas garantias de privacidade. A PD é um modelo semântico, cujo objetivo é garantir a utilidade dos dados ao mesmo tempo que fornece proteção contra ataques de conhecimento prévio. Em um contexto geral, seu objetivo é proteger os dados dos usuários na publicação de informação agregada sobre o conjunto de dados. Para isto, este método requer que a adição ou remoção de um único indivíduo tenha um efeito insignificante sobre a resposta de uma requisição. De forma mais precisa, a PD requer que, para quaisquer dois conjuntos de dados vizinhos (conjuntos de dados que se diferenciam em apenas um registro, Figura 1.4), a probabilidade de uma consulta sobre estes conjuntos retornar o mesmo valor v deve estar limitada por $exp(\varepsilon)$. Tipicamente, alcança-se ε-Privacidade Diferencial ao adicionar um ruído aleatório controlado à resposta das consultas, utilizando para isto de um mecanismo, Figura 1.5.

ID	Peso (Kg)	Altura (m)
1	87,2	1,70
2	81,2	1,62
3	74,2	1,75
4	60,0	1,61
5	78,5	1,58

(a)

ID	Peso (Kg)	Altura (m)
1	87,2	1,70
2	81,2	1,62
4	60,0	1,61
5	78,5	1,58

(b)

Figura 1.4. Exemplo de conjuntos de dados vizinhos.

Um mecanismo M garante ε-Privacidade Diferencial se para quaisquer conjuntos de dados vizinhos D_1 e D_2,

$$Pr[M(D_1)] \leq exp(\varepsilon) \times Pr[M(D_2)],$$

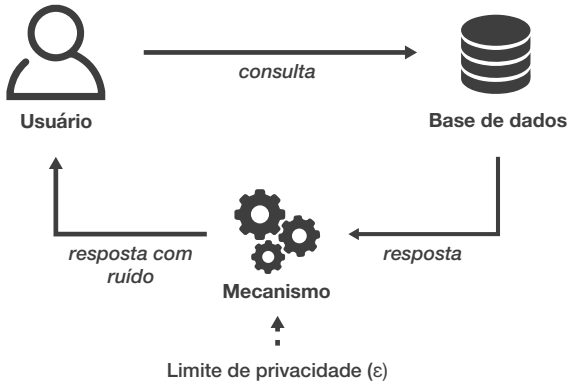

Figura 1.5. Ambiente interativo no modelo de Privacidade Diferencial.

onde Pr é a probabilidade da resposta adicionada de ruído aplicado por M. Isto é, a diferença entre as probabilidades de uma consulta retornar o mesmo valor v em dois conjuntos de dados vizinhos é limitada por ε.

1.5.1. Mecanismo

Como já dito anteriormente, o mecanismo é o responsável pela adição de ruído controlado à resposta da consulta a fim de garantir ε-Privacidade Diferencial. A quantidade de ruído necessária depende do tipo de consulta f aplicada sobre o conjunto de dados D. Isto é importante para introduzirmos o conceito de sensibilidade de uma função de consulta, que vai medir, justamente, quanta diferença na resposta da consulta um usuário faz ao ser removido ou adicionado a D. Desta forma, podemos definir a sensibilidade da função f como sendo:

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

para todo D_1, D_2 diferindo de no máximo um elemento, ou seja, D_1 e D_2 são vizinhos [12]. A Figura 1.6 ilustra um conjunto de dados simples D. Para uma consulta f sobre D que retorna a soma de imóveis, a resposta é 14. A Figura 1.7 apresenta conjuntos de dados vizinhos e sua respectivas respostas para a mesma consulta f. Podemos então calcular a sensibilidade de Δf sobre D como 7, que é a maior diferença entre as respostas da consulta f sobre os conjuntos de dados vizinhos.

ID	Nome	N° de Imóveis
1	José	4
2	Antônio	2
3	Raimundo	7
4	Francisco	1

Figura 1.6. Exemplo de conjunto de dados original contendo o número de imóveis de cada indivíduo (Fonte: [8]).

O mecanismo de Laplace é normalmente utilizado para alcançar a Privacidade Diferencial em consultas sobre dados numéricos que retornam valores agregados. A adição de ruído segue uma função de densidade de probabilidade de uma variável aleatória com

ID	Nome	N° de Imóveis
2	Antônio	2
3	Raimundo	7
4	Francisco	1

$f(D_1) = 2 + 7 + 1 = 10$

ID	Nome	N° de Imóveis
1	José	4
3	Raimundo	7
4	Francisco	1

$f(D_2) = 4 + 7 + 1 = 12$

ID	Nome	N° de Imóveis
1	José	4
2	Antônio	2
4	Francisco	1

$f(D_3) = 4 + 2 + 1 = 7$

ID	Nome	N° de Imóveis
1	José	4
2	Antônio	2
3	Raimundo	7

$f(D_4) = 4 + 2 + 7 = 13$

Figura 1.7. Conjuntos de dados vizinhos gerados a partir da base original e suas respectivas respostas da consulta f (Fonte: [8]).

distribuição de Laplace com média μ e escala b de forma que

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

A Figura 1.8 mostra a distribuição de probabilidades de respostas desejada em um modelo ε-Privacidade Diferencial quando aplicado sobre dois conjuntos de dados vizinhos D_1 e D_2 utilizando o mecanismo de Laplace.

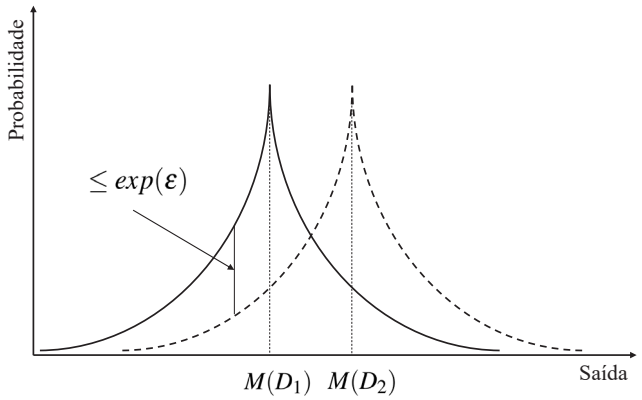

Figura 1.8. Probabilidades de saída de um algoritmo aleatório M sobre os conjuntos de dados vizinhos D_1 e D_2.

Apresentemos agora a definição formal do mecanismo de Laplace (Definição 1).

Definição 1 *Dada uma função de consulta $f : D \to \Re$, o mecanismo de Laplace M:*

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

Ruído	*f(D) + ruído*	*Pr(f(D) + ruído)%*
-4,58	9,42	3,70
-0,15	13,85	6,98
12,15	26,15	1,25
-6,43	7,57	2,85
2,89	16,89	4,72

Tabela 1.11. Cinco possíveis valores de ruído, resposta e probabilidade de ocorrência após a aplicação da Privacidade Diferencial.

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

Considere a Tabela 1.11. Ela apresenta cinco possíveis ruídos aplicados pelo mecanismo de Laplace para a mesma consulta f sobre o conjunto de dados da Tabela 1.6, o ruído de $-4,58$ possui uma probabilidade de ocorrência de $3,70\%$, resultando em uma resposta anonimizada de $9,42$ imóveis, frente à resposta 14 que seria retornada caso o ruído não tivesse sido adicionado pelo mecanismo. Observe que repetidas execuções da consulta f retornam valores distintos devido a aleatoriedade do ruído adicionado pelo mecanismo de Laplace à resposta de cada execução.

1.6. Privacidade de Localização

O desenvolvimento dos dispositivos móveis tem contribuído para um crescimento na popularidade dos serviços de localização. Serviços que, como o próprio nome diz, dependem da localização dos usuários para sua prestação. São alguns exemplos dos mais comuns serviços de localização:

- **Navegação**: permite o usuário obter direções para um ponto de interesse geograficamente localizado. Os dados de localização do usuário são coletados para prover instruções de direção em tempo real. São algumas aplicações: Google Maps e Waze.
- **Aplicações de tempo (clima)**: estes serviços provêm condições do tempo, bem como previsões. A localização do usuário é usada para obter informações relevantes sobre o clima do local atual.
- **Jogos**: utilizam a localização do usuário no contexto do ambiente virtual do jogo. Os mais recentes usam tecnologia de realidade aumentada, onde a movimentação do usuário em tempo real se reflete no jogo. Exemplo desse tipo de jogo é Pokemon GO.
- **Serviços de Recomendação**: estes serviços utilizam da localização do usuário para enviar recomendações de locais de interesse próximos. São exemplos: Foursquare e Yelp.

Apesar da popularidade destes serviços, a natureza dos dados de localização tem levado a sérios questionamentos quanto a preservação da privacidade dos usuários no

uso destes serviços. Por carregarem consigo muita informação, estes dados são capazes de potencializar violações de privacidade, requisitando assim a utilização de técnicas de anonimização a fim de garantir a preservação de privacidade dos indivíduos.

Há um consenso entre os pesquisadores que a privacidade é um assunto complexo, com muitas questões envolvidas, sendo um direito dos indivíduos a ser preservado [8]. Entretanto, o que temos muitas vezes visto na prática, é a privacidade dos usuários sendo utilizada como moeda de troca nos serviços de localização, nos quais o usuário fornece informações pessoais para fazer uso dos serviços. Nesta seção iremos apresentar os principais fundamentos em preservação de dados de localização, destacando a natureza deste tipo de dado, alguns dos principais tipos de ataques a dados de localização, e as técnicas usadas para preservar a privacidade dos indivíduos que fazem uso desse tipo de serviço.

1.6.1. Dados de Localização

O vazamento da informação de localização dos usuários pode permitir uma série de ataques de indivíduos maliciosos, que vão desde vigilância física e perseguição, até roubo de identidade. Outro risco é o de inferências de informações sensíveis. Estes ataques são possíveis devido a natureza dos dados de localização, que carregam consigo muita informação. Por exemplo, se a informação de uma localização de um indivíduo indicar um hospital. Neste caso o dado já sugere uma série de informações relacionadas ao local, por exemplo, doenças, horário de funcionamento, profissão, visita a conhecidos, dentre outras.

As informações de localização são obtidas por meio de sistemas de posicionamento global (GPS), que estão contidos na maioria dos aparelhos celulares da atualidade, o que tem impulsionado o crescimento de serviços baseados em localização (LBS). Estes serviços fornecem valor agregado aos seus usuários através da integração da localização ou posição de seus dispositivos móveis a outras informações. A popularidade destes serviços tem aumentado vertiginosamente a quantidade de informações de localização coletadas, o que por si só tem ampliado os riscos de quebra de privacidade.

A Figura 1.9 ilustra um típico serviço baseado em localização. São alguns componentes básicos de um LBS:

- **GPS**: permite determinar a localização dos objetos envolvidos, *i.e.*, usuários, ou outra entidade qualquer. O GPS é o mais popular sistema de posicionamento. Ele é um mecanismo de posicionamento por satélite que fornece a um aparelho receptor a sua posição.

- **Usuários**: são participantes que irão usufruir do serviço baseado em localização prestado. Através de dispositivos como *smartphones*, *notebooks*, *wearables*, os usuários se conectam ao meio de comunicação e enviam requisições ao provedor do serviço

- **Rede de comunicação**: é o meio através do qual acontece o tráfego de informações entre os participantes. Normalmente o meio utilizado é a rede de banda larga móvel, como a 4G.

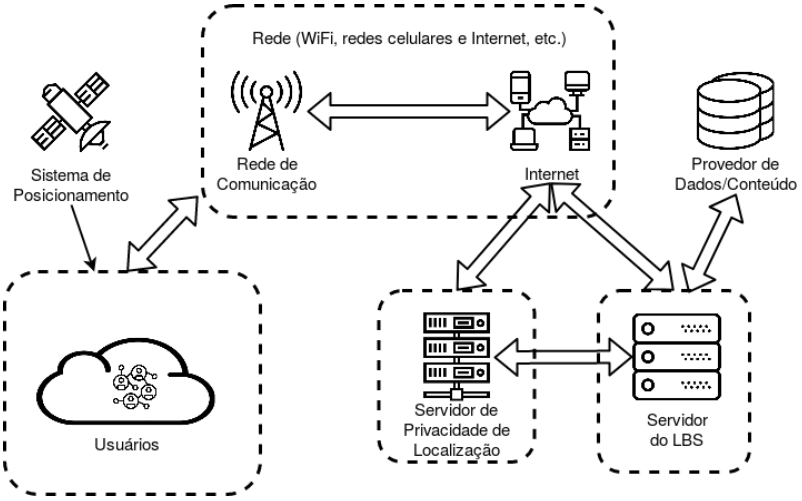

Figura 1.9. Modelo de sistema de serviços baseados em localização

Figura 1.10. Três atributos da informação de localização

- **Servidor do LBS**: é o responsável por receber as requisições dos usuários e prestar o serviço baseado em localização de acordo com sua natureza, seja para encontrar uma localização, seja para auxiliar na navegação do usuário, ou um outro tipo de serviço qualquer que utiliza a informação de localização enviada na requisição.

- **Provedor de Conteúdo/Dados**: provedor de Conteúdo/Dados fornecem dados e conteúdo ao servidor LBS. Alguns provedores de LBS possuem seus próprios dados e conteúdo, enquanto outros usam um terceiro para fornecer esse serviço.

- **Servidor de Privacidade**: o servidor de privacidade de localização executa os algoritmos de preservação de privacidade, como anonimização e criptografia e pode ser de propriedade e operado pelo provedor LBS ou por terceiros.

Essas informações de localização são constituídas de três partes, que podem ser observadas na Figura 1.10, identidade, tempo e posição.

A *identidade* pode ser um endereço de email, nome ou qualquer outra informação que torne um indivíduo distinguível dos outros. Ela pode ser: *(i)* consistente, que é aquela requisitada obrigatoriamente para o acesso a um LBS, como um nome de usuário; *(ii)*

inconsistente, quando pode haver o uso de pseudônimos; *(iii)* anônima, onde há a ausência de uma identificação.

O *tempo* é referente ao momento a qual as localizações estão associadas. Em geral, os serviços de localização associam as localizações a marcos de tempo. Esta informação temporal pode ser classificada como acumulada ou corrente. As aplicações em tempo acumulado não publicam as informações de localização em tempo real, mais em um tempo posterior ao atual. Um exemplo destas aplicações é o sistema de rastreio do *Fitbit*, que coleta as informações percorrida pelos usuários, mas só publica a trajetória computada depois de encerrado a atividade [22]. As aplicações em tempo real publicam as informações de localizações associados ao marco de tempo atual, de forma imediata.

A *informação espacial (posição)* é o principal meio para determinar a localização do usuário. As localizações podem ser descritas como um conjunto de coordenadas (latitude e longitude), ou por alguma outra forma de informação que pode ser vinculada a um local. As localizações podem ser únicas, quando não são correlacionadas umas com as outras, ou podem formar uma trajetória no caso em que são fortemente correlacionadas, o que acaba por gerar maiores riscos de exposição.

As localizações também podem ser classificadas em diretas ou indiretas. Os LBS tradicionais usam localizações diretas definidas por coordenadas de GPS, ou seja, utilizam o padrão adotado na realidade, em que a localização é composta de latitude e longitude. As localizações indiretas são aquelas estabelecidas com base na proximidade física, substituindo-se a localização exata pelo ponto de interesse mais próximo (POI) - entidade que representa uma localização, dotada de informação complementar sobre a mesma, como o nome do estabelecimento, horário de funcionamento, endereço, entres outras.

A privacidade de localização pode ser definida como a proteção desses três atributos que formam a informação de localização de uma pessoa. Blumberg e Eckersley [7] definem privacidade de localização como a capacidade de um indivíduo de se deslocar no espaço público com a expectativa de que, em circunstâncias normais, sua localização não será sistematicamente e secretamente registrada para uso posterior. Entretanto, é importante destacar que a garantia de privacidade de localização de indivíduos não é absoluta, uma vez que, no momento que você sai de casa, sua privacidade já está sendo exposta. Por exemplo, ao sair de casa, seu vizinho pode saber a hora que você chega em casa, que horas sai para trabalhar, se você tem algum tipo de animal de estimação, além de possíveis outras informações. Desta forma, pode-se identificar dois requisitos principais da privacidade de localização dos indivíduos: a expectativa de privacidade dos indivíduo de "circunstâncias normais", ou seja, o que o indivíduo espera em termos de exposição da sua localização, e a maneira como as informações são coletadas e usadas. A expectativa de privacidade de uma pessoa pode mudar com o tempo, assim como a forma como as informações de localização são coletadas e usadas também mudam. Logo, para avaliar a privacidade de localização do indivíduo, seus principais requisitos devem ser definidos do ponto de vista dos usuários.

Com isso, temos dois fatores que servem de base para avaliar a privacidade do indivíduo quanto a suas localizações. Estes fatores são caracterizados pelos seguintes pronomes interrogativos:

- *Como*: Como as informações são reveladas? É revelado secretamente ou publicamente? É criptografado ou não? E como a informação será usada?

- *Que*: Que tipo de informação é revelada? Por exemplo, um conjunto de coordenadas, um momento do tempo, a identidade do usuário anexada, dentre outros.

1.7. Tipos de Ataques

Um atacante é qualquer entidade que possa ter acesso aos dados de localização de um ou de vários indivíduos. Sendo assim, um adversário pode ser desde o próprio provedor do serviço de localização, ou até mesmo um cientista de dados que tenha acesso a uma publicação dos dados [26]. Na maioria das vezes, o atacante é considerado honesto, mas curioso [16]. Ou seja, o provedor do serviço ou um cientista de dados, potenciais adversários, se comportam conforme se espera deles na prestação do serviço, entretanto, eles são capazes de explorar de todas as formas possíveis quaisquer dados que tenham acesso. Para exemplificar, vamos supor um serviço de localização onde o usuário busca informações sobre uma determinada loja de animais. O provedor do serviço irá prestar este serviço, informando ao usuário todas as informações disponíveis sobre a loja requisitada. Estas informações são coletadas pelo provedor do serviço e podem ser usadas para obter outras informações que lhe permitam tirar algum proveito, como por exemplo, traçar o perfil do usuário e enviar sugestões de propagandas e serviços de seu interesse, atividades que vão além daquela fornecida pelo serviço.

Por ser carregado de informação, o conhecimento adversário torna os usuários ainda mais vulneráveis a ataques. Entretanto, o poder desse conhecimento vai depender se estes dados sofreram ou não algum tipo de transformação, tais como supressão, generalização ou pertubação já apresentados na Seção 1.2. Em se tratando de dados de localização, o conhecimento de contexto pode gerar potenciais riscos de violação de privacidade. São exemplos de conhecimento de contexto: o número de usuários em uma área em um determinada hora do dia; a relação entre diferentes usuários; as restrições de localização de uma determinada área, como rede de ruas, área de preservação; a distribuição e a probabilidade estatística associada às localizações.

Desta forma, em função da expectativa de privacidade dos indivíduos e na forma como as informações de localização são coletadas e usadas, um atacante e seu ataque podem ser caracterizados por "como" se obtem a informação, "como" o ataque é lançado, "que" informação ou conhecimento se detem, e "que/quem" é o alvo.

Em particular, assume-se que o atacante possui qualquer base de dados que contém conhecimentos adicionais sobre a semântica das informações de localização dos usuários. Além disso, o provedor do LBS pode identificar que o usuário está utilizando alguma técnica de preservação de privacidade de localização a fim de garantir a utilização do serviço sem expor sua localização real.

1.7.1. Ataque de Identidade

Os ataques de identidade, também chamados de ataques de desanonimização, procuram cruzar conhecimentos adversários de diversas fontes a fim de determinar a identidade do alvo. São alguns exemplos deste tipo de ataque:

- **Ataque de identificação pessoal**: através do conhecimento prévio pessoal de um indivíduo, busca-se identificar o indivíduo dentro do conjunto de dados, a fim de se obter toda a informação a ele associada no conjunto de dados. Considere o exemplo: o atacante tem o conhecimento sobre o endereço residencial de um indivíduo. Através dele, mesmo em um conjunto de dados anonimizado, se o atributo endereço não tiver sido protegido, o atacante poderá identificar o dono do registro em função do endereço residencial exposto.

- **Ataque de presença agregada**: identificar a identidade com base na relação entre dois indivíduos ou através de uma propriedade agregadora, por exemplo pessoas agrupadas próximas a um evento, uma estação de Pokemon Go, ou uma loja com ofertas, dentre outros eventos.

1.7.2. Ataque de Localização

Os ataques de localização consistem em identificar as informações espaciais e temporais referentes a um indivíduo. São alguns exemplos de ataques de localização: *(i)* ataque a localizações sensíveis procura identificar localizações importantes, como residência ou local de trabalho; *(ii)* ataque de revelação de presença ou ausência determina se um usuário está presente ou ausente em determinadas localizações em um determinado horário do dia; *(iii)* ataque de rastreamento identifica uma sequência de eventos para rastrear um usuário.

1.7.3. Métodos de Ataque

Os métodos de ataque dizem respeito à forma como o ataque é realizado. São alguns destes métodos:

- **Ataques de vinculação de contexto**: é a forma mais comum em ataques de localização. O conhecimento de contexto é combinado com a informação de localização obtida para se chegar à localização precisa da vítima em um ataque de localização. Por exemplo, um indivíduo ao realizar um *check-in* em um hospital, preenche seus dados informando seu endereço residencial. Se um atacante tiver conhecimento do endereço residencial do indivíduo, ele poderá usá-lo para identificar este indivíduo na lista de *check-in* do hospital.

- **Ataques probabilísticos**: este tipo de ataque é baseado na coleta de informações estatísticas sobre o ambiente [28]. Pode ser aplicado tanto para ataques de identidade, como de localização. Sendo assim, a localização do usuário pode ser inferida em razão da probabilidade do usuário estar em uma determinada localização em um horário preciso.

- **Ataque de conluio de usuários maliciosos**: é realizado por usuários que usam o mesmo provedor de serviços baseado em localização, que colidem para realizar vários ataques. Por exemplo, usuários em conluio utilizam sua posição para obter, do serviço, a distância da vítima, e baseado nisso calculam a exata localização da vítima.

1.8. Modelos de Privacidade em Serviços de Localização

Como já citado nas seções anteriores, a exposição dos dados de localizações a agentes maliciosos pode levar a sérios riscos de violação de privacidade. Portanto, diversas técnicas de privacidade foram propostas a fim de mitigar o problema. Nesta seção, iremos agrupar algumas das principais técnicas de preservação de privacidade de dados de localização em dois modelos: modelos de anonimização e modelos de ofuscação.

1.8.1. Anonimização

As técnicas de anonimização em privacidade de localização buscam impedir ataques de ligação, ou seja, conforme discutido na Seção 1.3, buscam proteger a ligação entre a identidade do usuário e a informação de localização do mesmo [22], dificultando a re-identificação dos indivíduos. Em outras palavras, o objetivo é garantir que os dados de localização de um usuário, dentro de um conjunto de dados, não poderão ser ligados à identidade de seu dono. São exemplos de técnicas de anonimização: o k-Anonimato de localizações e as Zonas de Mixagem.

1.8.1.1. k-anonimato de Localizações

Conforme discutido na Seção 1.4.1, o k-anonimato foi proposto por Sweeney et al. [30] com o objetivo de prevenir ataques de ligação ao registro, alcançando a preservação de privacidade através de generalização ou supressão de dados. Em sua forma original, esse modelo assegura que, para cada combinação de k atributos semi-identificadores, existem pelo menos k registros distintos no conjunto de dados publicado, formando uma classe de equivalência.

Em privacidade de localização, um sujeito é tido k-anônimo se sua localização é indistinguível da localização de outros $k-1$ usuários. Portanto, a probabilidade de um usuário malicioso violar a privacidade de um indivíduo através de um ataque não poderá ser maior do que $\frac{1}{k}$.

Vale a pena lembrar que o parâmetro k do modelo é responsável por balancear a utilidade e a privacidade dos dados. Assim, quanto maior o valor de k, maior será a privacidade dos dados e, consequentemente, menor sua utilidade, o que pode ser um problema em serviços de localização, pois a precisão da localização afeta diretamente a qualidade do serviço. Desta forma, encontrar um equilíbrio entre privacidade e utilidade se faz ainda mais importante no contexto de LBS. Entretanto, encontrar um valor ótimo para o parâmetro k é um problema NP-difícil, como citado na Seção 1.4.1. Desta forma, os responsáveis pela anonimização devem especificar o grau de privacidade desejada em função desse parâmetro.

O conceito básico da aplicação do k-anonimato em dados de localização requer que o LBS seja operado por uma terceira entidade confiável, o anonimizador, responsável por anonimizar as localizações das requisições. Este anonimizador tem conhecimento da localização de todos os usuários que usam o serviço. Dessa forma, sempre que um usuário necessita realizar uma requisição, enviando sua localização, o anonimizador calcula um conjunto de k usuários e reporta uma área de ofuscação contendo k posições, incluindo a

localização da requisição do usuário.

A Figura 1.11 ilustra uma abordagem da utilização dessa técnica, para um $k = 3$, onde o usuário em laranja deseja enviar uma requisição ao LBS. Um terceiro confiável responsável por anonimizar a sua localização, agrupa o usuário e sua localização, com outras $k-1$ localizações, enviando uma requisição ao LBS contendo k localizações no total. Este, por sua vez, irá responder a requisição em função de cada uma das localizações enviadas. Como o terceiro confiável tem conhecimento das localizações dos usuários, ele irá filtrar a resposta referente a localização real presente na requisição, enviando-a ao usuário. Assim, para um atacante, a localização do usuário pode ser qualquer uma das k localizações que fazem parte da requisição, garantindo que a probabilidade de se identificar a localização do usuário não seja superior a $\frac{1}{k}$.

Figura 1.11. Processo de anonimização utilizando k-anonimato.

1.8.1.2. Zona de Mixagem

A zona de mixagem é outra abordagem que procura proteger a privacidade do usuário contra ataques de ligação, ao evitar que seja possível vincular a identidade dos usuários à sua localização. Entretanto, diferente do k-anonimato, a zona de mixagem pode ser aplicada sem qualquer informação de identidade do usuário. O conceito de zona de mixagem foi proposto por Beresford et al. [6]. Ele propõe um *framework*, onde os usuários utilizam pseudo-ids que são modificados constantemente garantindo que estes não sejam identificados no uso de serviços de localização. Sendo assim, a real identidade do usuário é protegida através do uso de pseudônimos.

As zonas de mixagens são definidas como áreas circulares de raio r, onde todo usuário dentro da zona possui um único pseudo-id, não registrado por nenhuma das aplicações cobertas por ela. Em outras palavras, esta técnica procura garantir a indistinguibilidade dos usuários no uso de qualquer das aplicações dentro da zona, através do uso de pseudo-ids e a não presença de qualquer informação de localização presente na requisição. Assim, como o k-anonimato, a técnica de zona de mixagem em sua forma clássica exige a figura de um terceiro confiável, responsável pela anonimização. Na zona de mixagem,

este terceiro confiável tem o papel de gerenciar os pseudo-ids dos usuários, garantindo que sempre que um usuário entre na zona de mixagem, ele possua um pseudo-id único que não tenha sido registrado por nenhuma aplicação. Desta forma, como não há a presença de localizações presentes na requisição, todas as aplicações que proveem serviços de localização dentro da zona veem os usuários em uma mesma localização definida pela zona de mixagem de alguma forma, como por exemplo um centroide que represente a zona.

A Figura 1.12 ilustra a aplicação da técnica de zona de mixagem. No primeiro quadro, o usuário ao entrar na zona de mixagem 1 obtém um pseudo-id único, não registrado por nenhuma aplicação, e só então passa a dispor de qualquer aplicação coberta pela zona de mixagem. Ao se deslocar para a zona de mixagem 2, no quadro 2, o usuário obtém um novo pseudo-id, também único e não registrado, e passa a utilizar dos serviços cobertos dentro dessa nova zona.

Figura 1.12. Processo de anonimização utilizando zona de mixagem.

1.8.2. Ofuscação

Diferente dos modelos de anonimização, os modelos de ofuscação atuam sobre os dados de localização em si, reduzindo sua precisão a fim de preservar a privacidade de localização dos usuários [22]. As principais técnicas de ofuscação são: técnica de Localizações falsas, Ofuscação de localização e Privacidade Diferencial (PD).

1.8.2.1. Localizações Falsas

Uma típica requisição feita a provedores de serviços de localização é composta de dois componentes básicos: *(i)* **informação de localização** é toda a informação contida na requisição referente a localização enviada na consulta. De forma geral e simplificada, é a

localização composta por suas coordenadas geográficas de latitude e longitude; *(ii)* **conteúdo de requisição** é a solicitação do serviço a ser prestado, por exemplo, a solicitação do hospital mais próximo dada a localização contida na informação de localização.

A técnica de localização falsas proposta por Kido et al. [18] procura garantir a privacidade dos dados de localização do usuário através de um processo de sanitização da *informação de localização* presente na requisição do usuário aos provedores de serviços de localização. Assim, numa requisição, a localização do usuário é acompanhada de múltiplas localizações falsas, cujo objetivo é mascarar a localização verdadeira do usuário.

Diferentemente dos modelos tradicionais de k-anonimato e zona de mixagem, a técnica de seleção de localizações falsas não necessita da presença de servidores confiáveis, diminuindo o risco de exposição. O processo de sanitização é de responsabilidade dos dispositivos móveis dos próprios usuários, que são responsáveis por selecionar, através de um mecanismo aleatório, as localizações falsas que irão compor a informação de localização da requisição de seus usuários. O objetivo é garantir que a probabilidade de se identificar a localização real dentre aquelas presentes na requisição não seja maior que $\frac{1}{k}$, onde k é o grau de privacidade desejado para uma requisição com uma quantidade de k localizações presentes.

Figura 1.13. Técnica de Localizações Falsas.

A Figura 1.13 ilustra a aplicação da técnica de Localizações falsas, onde o usuário, por intermédio de seu dispositivo, envia uma requisição anonimizada ao provedor de serviço. O processo de anonimização seleciona $k-1$ localizações, em preto, que serão enviadas na informação de localização da requisição, juntamente com a localização real do usuário, em laranja. O servidor receberá a requisição contendo k localizações, e responderá a solicitação contida no conteúdo de requisição, tendo como referência cada uma das localizações presentes na informação de localização. O dispositivo então filtra a resposta referente à localização real.

O mecanismo de seleção aleatória das localizações falsas é fundamental para garantir a privacidade de localização do usuário, uma vez que esta técnica, assim como as técnicas que abordam o modelo de anonimização estão sujeitas a ataques de conhecimento, que, conforme discutido na seção 1.7, utilizam de conhecimentos prévios para

inferir dados sensíveis dos usuários. Desta forma, várias abordagens foram propostas, a fim de solucionar este problema e garantir uma seleção de localizações falsas que minimize o risco de exposição dos dados de localização do usuário, utilizando para isto, do próprio conhecimento prévio disponível ao provedor de serviço [29, 25].

1.8.2.2. Ofuscação de Localizações

A técnica de ofuscação de localização procura garantir a preservação de privacidade do usuário através da redução deliberada da precisão da localização do mesmo. Em sua abordagem tradicional apresentada por Ardagna *et al.* [3, 4], o usuário ao realizar uma requisição ao LBS, ao invés de enviar suas coordenadas de localização real (x_u,y_u), envia uma área circular $Area(r,x_c,y_c)$, centralizada nas coordenadas geográficas (x_c,y_c) e raio r, onde a probabilidade de a localização do usuário estar presente dentro dessa área é igual a 1. A Figura 1.14 ilustra uma requisição anonimizada pela técnica de ofuscação, onde o usuário, com localização em laranja, ao enviar sua requisição, envia como informação de localização uma área circular de raio r, centrada nas coordenadas do ponto central em preto na figura, semelhante a todos os outros usuários presentes na área de ofuscação.

Figura 1.14. Técnica de Ofuscação de Localização usando área circular.

Outra abordagem desta técnica é proposta por Gutscher [17], onde a precisão da localização real é reduzida através de simples operações geométricas (i.e., rotação, translação) sobre suas coordenadas geográficas antes de serem enviadas na requisição ao provedor LBS. A Figura 1.15 ilustra a aplicação desta técnica através de uma simples operação de translação onde a localização enviada na requisição é substituída pela localização em laranja.

1.8.2.3. Privacidade Diferencial para Localizações

Como já explanado na Seção 1.5, o modelo de Privacidade Diferencial foi proposto com o objetivo de garantir a utilidade dos dados, ao mesmo tempo que fornece proteção contra ataques municiados por conhecimento adversário.

No contexto de dados de localização diversas abordagens que utilizam privacidade diferencial foram propostas. Os modelos propostos em [2, 13] procuram estender a no-

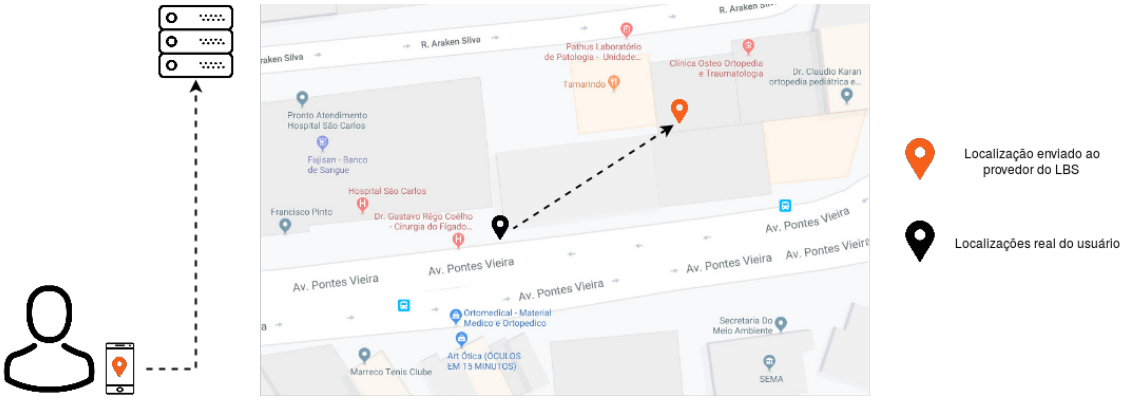

Figura 1.15. Técnica de Ofuscação de Localização usando operações geométricas.

ção utilizada na abordagem original de Privacidade Diferencial sobre conjuntos de dados vizinhos para o contexto de localização. Assim, duas localizações são ditas vizinhas se a distância física entre elas é menor ou igual a um raio r. Desta forma, é definida uma área de raio $r > 0$, onde supostamente a localização do usuário dentro desta área esta protegida. O nível de privacidade, portanto, depende diretamente de r e é alcançado através da adição de um ruído controlado à localização do usuário. Ou seja, um r grande implica em uma maior proteção à privacidade do usuário, entretanto, a adição do ruído tende a ser maior, diminuindo a utilidade dos dados e consequentemente, a qualidade do serviço. Já um r pequeno garante uma maior qualidade do serviço já que a adição do ruído é menor, entretanto, a proximidade das localizações pode afetar a garantia de privacidade do usuário. A Figura 1.16 apresenta em azul um conjunto de localizações vizinhas da localização l em preto, e em vermelho localizações que estão a uma distância da localização l maior que r, portanto, não vizinhas de l.

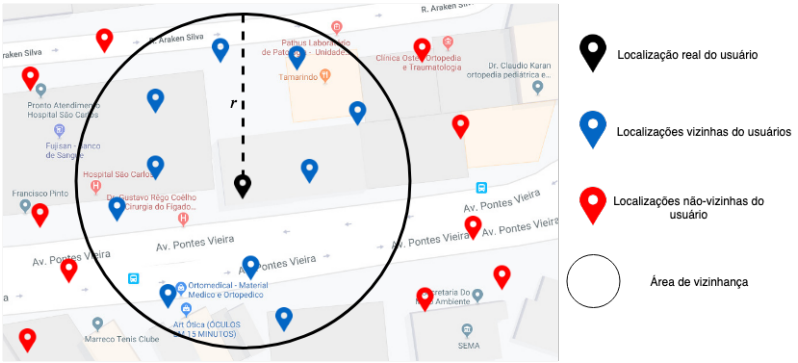

Figura 1.16. Localizações vizinhas.

Podemos, agora, definir (r,ε)-privacidade de localização para localizações vizinhas da mesma forma que definido no modelo padrão de privacidade diferencial para conjuntos de dados vizinhos. Assim, um mecanismo responsável pela adição de ruído satisfaz (r,ε)-privacidade de localização se quaisquer duas localizações dentro do raio r são indistinguíveis quando observadas as saídas do mecanismo K para estas localizações.

Definição 2 *(r,ε)-privacidade de localização: Para um raio $r > 0$ e $\varepsilon > 0$, um mecanismo*

$K : X \rightarrow E^2$ satisfaz (r,ε)-privacidade de localização), se e somente se, para todo i,j $\in X$ com d(i,j)$\leq$ r,

$$P(K(i) \in S) \leq exp^{\varepsilon} P(K(j) \in S) \quad \forall S \subseteq E^2$$

De acordo com a definição, a probabilidade de a localização retornada pelo mecanismo K aplicado sobre a localização i é semelhante a probabilidade de a localização retornada pelo mecanismo K quando aplicado por uma localização vizinha j, limitada pela exponencial de ε.

A Figura 1.17 ilustra a aplicação do processo de anonimização garantindo (r, ε)-*privacidade de localização*. O Mecanismo irá adicionar um ruído controlado às coordenadas da localização real do usuário. Este processo irá garantir uma nova localização anonimizada à uma distância de no máximo r da localização real.

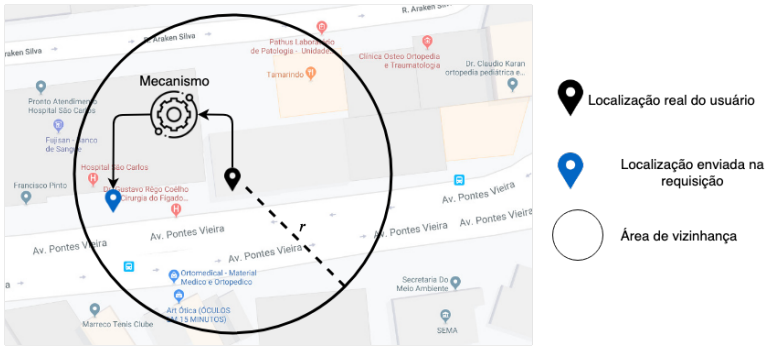

Figura 1.17. Anonimização por $(r-\varepsilon)$-privacidade de localização.

1.9. Conclusão

Este capítulo conclui que a preservação da privacidade de dados acerca de indivíduos é um problema desafiador. Técnicas de anonimização têm sido utilizadas para a disponibilização de dados sensíveis, procurando encontrar o melhor balanceamento entre privacidade e utilidade que atenda às diversas partes envolvidas no processo de disponibilização de dados. Diferentes tipos de ataques à privacidade têm sido empregados por usuários maliciosos com a intenção de violar informações sensíveis de bases de dados abertas. Para tal fim, os atacantes utilizam conhecimento que muitas vezes é imensurável, devido aos diversos cenários em que informações podem ser obtidas. No contexto de dados de localização, este risco se potencializa, em virtude das informações agregadas ao dado geográfico buscado quando de uma solicitação a um serviço de localização, que servem de munição para os agentes maliciosos. Este capítulo apresentou as principais técnicas no estado da arte em preservação de privacidade de dados de localização. Os modelos de anonimização buscam proteger contra ataques de ligação ao registro, ou seja, prevenir a vinculação entre a identidade do usuário e sua localização, evitando a re-identificação de indivíduos, geralmente utilizando técnicas de supressão e generalização. Os modelos de ofuscação, por sua vez, buscam proteger a localização em si, garantindo que esta não seja revelada, mesmo no uso de serviços de localização. A Privacidade Diferencial se destaca por fornecer soluções de preservação de privacidade, onde um ruído aleatório controlado

é adicionado a localização do usuário, garantindo que a localização real do usuário estará protegida independentemente do conhecimento do atacante.

Finalmente, entendemos que o problema da garantia de privacidade de dados de localização dos usuários de LBS continua cientificamente relevante. A busca por um ponto ideal na curva de solução de compromisso entre privacidade do indivíduo e a utilidade do dado fornecido para esse tipo de serviço deve pautar os próximos passos da pesquisa. Este aspecto é particularmente importante no contexto de LBS pois a qualidade do serviço é dependente da precisão do dado de localização, portanto o envio de dado perturbado para o provedor de serviço tende a impactar negativamente na qualidade. Tanto o paradigma de anonimização sintática, quanto o modelo de Privacidade Diferencial apresentam aspectos de revisão que devem ser vistos como oportunidades de pesquisas e desenvolvimento. Avanços em ambos os paradigmas são necessários para garantir que o futuro ofereça cada vez mais proteção à privacidade de indivíduos e ao mesmo tempo haja dados úteis e disponíveis para pesquisadores, testadores e analistas de dados.

Agradecimentos

Esta trabalho foi parcialmente financiada pela Lenovo, como parte do seu investimento em pesquisa e desenvolvimento de acordo com a Lei de Informática, pela CAPES (1836136), CNPq (122201/2018-3) e pelo LSBD/UFC.

Referências

[1] Aggarwal, C. C. and Philip, S. Y. (2008). A framework for condensation-based anonymization of string data. *Data Mining and Knowledge Discovery*, 16(3):251–275.

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

[3] Ardagna, C. A., Cremonini, M., Damiani, E., De Capitani di Vimercati, S., and Samarati, P. (2007). Location privacy protection through obfuscation-based techniques. In Barker, S. and Ahn, G.-J., editors, *Data and Applications Security XXI*, pages 47–60.

[4] Ardagna, C. A., Cremonini, M., De Capitani di Vimercati, S., and Samarati, P. (2011). An obfuscation-based approach for protecting location privacy. *IEEE Transactions on Dependable and Secure Computing*, 8(1):13–27.

[5] Bayardo, R. J. and Agrawal, R. (2005). Data privacy through optimal k-anonymization. In *21st International conference on data engineering (ICDE'05)*, pages 217–228.

[6] Beresford, A. R. and Stajano, F. (2003). Location privacy in pervasive computing. *IEEE Pervasive computing*, (1):46–55.

[7] Blumberg, A. J. and Eckersley, P. (2009). On locational privacy, and how to avoid losing it forever. *Electronic frontier foundation*, 10(11).

[8] Brito, F. T. and Machado, J. C. (2017). Preservação de privacidade de dados: Fundamentos, técnicas e aplicações. In Delicato, F. C., Pires, P. F., and Silveira, I. F., editors, *Jornadas de A tualização em Informática 2017*. Sociedade Brasileira de Computação - SBC.

[9] Dewri, R., Ray, I., Ray, I., and Whitley, D. (2008). On the optimal selection of k in the k-anonymity problem. In *24th ICDE International Conference on Data Engineering*, pages 1364–1366, Cancun,Mexico.

[10] Domingo-Ferrer, J. and Torra, V. (2001). A quantitative comparison of disclosure control methods for microdata. *Confidentiality, disclosure and data access: theory and practical applications for statistical agencies*, pages 111–134.

[11] Dwork, C. (2006). Differential privacy. In *33rd International Colloquium on Automata, Languages and Programming*, pages 1–12, Venice, Italy.

[12] Dwork, C (2008). *Differential privacy: a survey of results. InInternational conference on theory and applications of models of computation (pp. 1–19).*

[13] Elsalamouny, E. and Gambs, S. (2016). Differential Privacy Models for Location-Based Services. *Transactions on Data Privacy*, 9(1):15 – 48.

[14] Fung, B. C., Wang, K., Fu, A. W.-C., and Yu, P. S. (2010a). *Introduction to Privacy-Preserving Data Publishing: Concepts and Techniques*. Chapman & Hall/CRC, 1st edition. ISBN 978-1-4200-9148-9.

[15] Fung, B. C. M., Wang, K., Chen, R., and Yu, P. S. (2010b). Privacy-preserving data publishing: A survey of recent developments. *ACM Computing Surveys*, 42(4):1–53.

[16] Goldreich, O. (2003). Cryptography and cryptographic protocols. *Distributed Computing*, 16(2-3):177–199.

[17] Gutscher, A. (2006). Coordinate transformation - a solution for the privacy problem of location based services? In *Proceedings 20th IEEE International Parallel Distributed Processing Symposium*, pages 7 pp.–.

[18] Kido, H., Yanagisawa, Y., and Satoh, T. (2005). An anonymous communication technique using dummies for location-based services. In *Proceedings of the Int. Conf. on Pervasive Services, ICPS'05*, pages 88–97. IEEE.

[19] LeFevre, K., DeWitt, D. J., and Ramakrishnan, R. (2005). Incognito: Efficient full-domain k-anonymity. In *Proceedings of the 2005 ACM SIGMOD international conference on Management of data*, pages 49–60. ACM.

[20] Li, H., Sun, L., Zhu, H., Lu, X., and Cheng, X. (2014). Achieving privacy preservation in wifi fingerprint-based localization. In *INFOCOM, 2014 Proceedings IEEE*, pages 2337–2345. IEEE.

[21] Li, N., Li, T., and Venkatasubramanian, S. (2007). t-closeness: Privacy beyond k-anonymity and l-diversity. In *2007 IEEE 23rd International Conference on Data Engineering*, pages 106–115. IEEE.

[22] Liu, B., Zhou, W., Zhu, T., Gao, L., and Xiang, Y. (2018). Location privacy and its applications: A systematic study. *IEEE Access*, 6:17606–17624.

[23] Meyerson, A. and Williams, R. (2004). On the complexity of optimal k-anonymity. In *Proceedings of the twenty-third ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, pages 223–228. ACM.

[24] Nergiz, M. E., Atzori, M., and Clifton, C. (2007). Hiding the presence of individuals from shared databases. In *Proceedings of the 2007 ACM SIGMOD International Conference on Management of Data*, SIGMOD '07, pages 665–676, New York, NY, USA. ACM.

[25] Neto, E. R. D., Mendonça, A. L. C., Brito, F. T., and Machado, J. C. (2018). Privlbs: uma abordagem para preservação de privacidade de dados em serviços baseados em localização. In *Brazilian Symposium on Databases SBBD*, Rio de janeiro, Brazil.

[26] Primault, V., Boutet, A., Mokhtar, S. B., and Brunie, L. (2018). The long road to computational location privacy: A survey. *IEEE Communications Surveys & Tutorials*.

[27] Schiller, J. and Voisard, A. (2004). *Location-based services*. Elsevier.

[28] Shokri, R., Theodorakopoulos, G., Le Boudec, J.-Y., and Hubaux, J.-P. (2011). Quantifying location privacy. In *2011 IEEE symposium on security and privacy*, pages 247–262. IEEE.

[29] Sun, G., Chang, V., Ramachandran, M., Sun, Z., Li, G., Yu, H., and Liao, D. (2017). Efficient location privacy algorithm for internet of things (iot) services and applications. *Journal of Network and Computer Applications*, 89:3–13.

[30] Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557–570.

[31] Tan, V. Y. F. and Ng, S.-K. (2007). Generic probability density function reconstruction for randomization in privacy-preserving data mining. In *International Workshop on Machine Learning and Data Mining in Pattern Recognition*, pages 76–90. Springer.

[32] Truta, T. M., Campan, A., and Meyer, P. (2007). Generating microdata with p-sensitive k-anonymity property. In *Workshop on Secure Data Management*, pages 124–141. Springer.

[33] Wang, K., Fung, B. C., and Yu, P. S. (2005). Template-based privacy preservation in classification problems. In *Fifth IEEE International Conference on Data Mining (ICDM'05)*, pages 8–pp. IEEE.

[34] Wong, R. C.-W. and Fu, A. W.-C. (2010). Privacy-preserving data publishing: An overview. *Synthesis Lectures on Data Management*, 2(1):1–138.

[35] Zhu, X., Chi, H., Niu, B., Zhang, W., Li, Z., and Li, H. (2013). Mobicache: When k-anonymity meets cache. In *Global Communications Conference (GLOBECOM), 2013 IEEE*, pages 820–825, Atlanta, GA, USA. IEEE.