Sensorização em Dispositivos Móveis: Questões Éticas e de Privacidade

Diogo Rebelo[pg50327] and Daniel Xavier[pg50310]

[1] Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal
[2] email:{pg50327,pg50310}@alunos.uminho.pt

Abstract. Com o crescente uso de dispositivos móveis em todo o mundo, a sua sensorização tornou-se uma área de pesquisa em rápido crescimento. A sensorização permite que dispositivos móveis reúnam dados sobre utilizadores, incluindo dados de localização, saúde, movimento e outras informações. No entanto, a recolha de dados também levanta questões importantes de privacidade e ética. Este artigo apresenta, em interligação com a computação ubíqua, uma análise detalhada dos principais aspetos definidores da sensorização em dispositivos móveis, casos e experiências concretas de uso, bem como os seus prós e contras. Por fim, o artigo conclui com uma análise crítica sobre o seu uso e a sua relação com questões éticas e de privacidade, com sugestões para melhorar as políticas e regulamentações. São também abordadas algumas aplicações no mundo real.

Keywords: Dispositivos Móveis · Sensorização · Privacidade · Ética · Computação Ubíqua · Casos de Uso de *Mobile Sensing* · Políticas e Regulamentações · *Crowd Sensing*

1 Introdução

Em constante transformação e atualização, o *Mobile Sensing* é uma área de investigação que mudou significativamente a forma como os dados são utilizados. O *Mobile Sensing* está de tal modo presente no nosso dia-a-dia que é inevitável interligá-lo com a Computação Ubíqua. Esta tem como objetivo tornar a interação humano-computador "invisível", ou seja, integrar a informática com as ações e comportamentos naturais das pessoas. Não invisível, como se não se pudesse ver, mas, sim de uma forma que as pessoas nem se apercebem que estão a dar comandos a um computador, tornando-se assim omnipresente. Com o aumento crescente da tecnologia móvel, essa integração tornou-se ainda mais intensa, permitindo a comunicação e interação contínua entre pessoas, dispositivos e serviços em ambientes diversos.

No entanto, essa coleta de dados móveis levanta preocupações éticas e de privacidade, uma vez que as informações reunidas podem incluir dados pessoais sensíveis, como localização, atividades, preferências e histórico de uso do dispositivo. Essas informações podem ser usadas para fins legítimos, como melhorar a qualidade de serviços, bem como para fins nefastos, como rastreamento de comportamento e invasão de privacidade. É aqui que a ética e a privacidade entram em cena, uma vez que é crucial que essa coleta seja feita com respeito à privacidade dos utilizadores e de acordo com as leis e normas definidas. O desafio está em encontrar um equilíbrio entre a coleta de dados úteis e a proteção da privacidade individual, isto é, sem comprometer a privacidade dos utilizadores. [1] Por conseguinte, o artigo irá explorar este domínio, começando por fazer uma correta definição caracterização dos mesmos.

De seguida, aprofundar-se-ão alguns casos de uso e aplicações, bem como vários desafios e oportunidades.

Finalmente, são analisadas as principais conclusões e aspetos relevantes sobre o trabalho futuro.

2 Definição e Caraterização

2.1 Mobile Sensing

Define-se *Mobile Sensing* o uso de sensores presentes nos mais diversos dispositivos móveis, como telemóveis, *tablets*, *smartwatches*, ou até mesmo um carro, para reunir dados do ambiente em que estão presentes. Esses sensores podem ser dos mais diversos, desde câmaras, microfones, acelerómetros, giroscópios, GPS, entre outros.

A ideia é que esses dispositivos, que fazem cada vez mais parte do nosso quotidiano, possam ser utilizados como ferramentas para angariar dados em tempo real de forma não intrusiva e acessível, que possam ser utilizados para tomar decisões informadas e melhorar a qualidade de vida das pessoas. Além disso, a aplicação de técnicas de *machine learning* e inteligência artificial pode auxiliar na interpretação desses dados e na tomada dessas decisões [2].

Deste modo, ao longo do artigo é primordial entender a correta aplicação dos sensores, avaliar as limitações desses dispositivos e como eles podem afetar a qualidade dos dados. Além disso, torna-se inevitável considerar questões éticas e de privacidade. [3].

2.2 Tipos, Categorias e Áreas de Aplicação

Não há dúvidas de que "os dados são o novo petróleo", e os sensores oferecem a forma perfeita para o extrair e utilizá-los em nosso proveito. Como se ilustra na figura os sensores utilizados em *mobile sensing* são dos mais diversos tipos e com os mais variados propósitos.

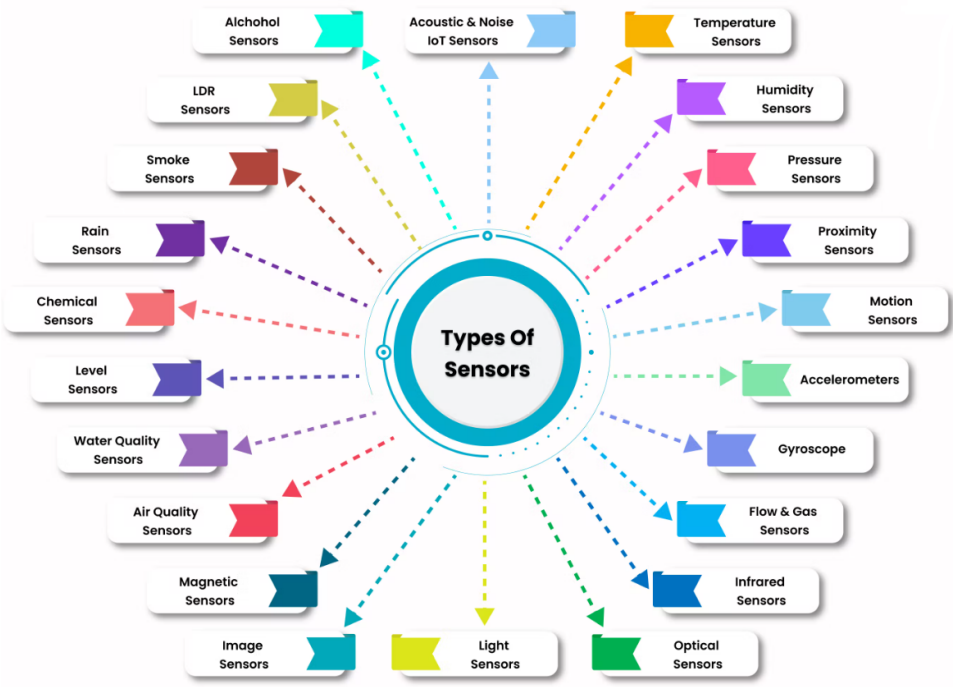

Fig. 1: Tipos de sensores [4]

Todos em algum momento e propósito são importantes, contudo destacam-se:

- **Sensor de Luz**: estes são sensores fotoelétricos que convertem energia luminosa (fotões) em energia elétrica. Têm várias aplicações em segurança e controlo de luminosidade, incluindo definições de luz ambiente em telemóveis e computadores portáteis. Então, medem a quantidade de luz à qual o dispositivo está exposto. Caso de uso: os sensores de luz são uma parte valiosa da agricultura, onde ajudam a medir a quantidade de luz absorvida pelo solo e, portanto, a rapidez com que as plantas podem crescer nesse solo.
- **Sensor de infravermelhos**: são uma alternativa rentável aos sensores de movimento. Todos os objetos emitem alguma quantidade de radiação térmica, que é aquilo a que estes sensores podem detetar e reagir. Atualmente, a maioria dos dispositivos móveis incorpora estes sensores na sua arquitetura. Caso de uso: rastreiam a pressão e o fluxo sanguíneo de um paciente ou monitorizam os níveis de aptidão física através da inclusão num *smartwatch*.
- **Acelerómetro**: são utilizados para para medir a aceleração própria de um sistema, o que por sua vez permite a medição da sua inclinação e vibração. Este sensor mede a força de aceleração ao longo dos eixos x, y, z, do dispositivo. Caso de uso: os acelerómetros são frequentemente utilizados em contextos industriais, onde medem se as máquinas estão a funcionar corretamente, rastreando as suas vibrações.
- **Giroscópio**: no passado, alguns dispositivos só tinham acelerómetros, cuja capacidade de medir a posição ou o movimento do dispositivo é limitada. A chegada do giroscópio significa maior quantidade de informação gerada na posição e movimento do terminal, dado que são adicionadas novas dimensões

que medem a rotação ou as voltas que são dadas. São comummente conhecidos como sensores de velocidade angular. O princípio de um giroscópio é utilizar a gravidade da Terra para rastrear o movimento angular de um objeto. Caso de uso: populares na conceção de jogos móveis, e permitem ao telefone detetar se o jogo está no modo retrato ou paisagem (e, portanto, a melhor forma de jogar o jogo).

Concetualmente, existem cinco categorias de sensores (embora a maioria dos artigos de documentação mencionem apenas os três primeiros, com alguns a reconhecerem sensores compostos):

- **Posição do dispositivo**: recolhe informação sobre a posição do dispositivo. Exemplos: sensores de orientação, magnetómetro.
- **Sensores de movimento**: detetam alterações nas forças em torno dos três eixos do dispositivo. Exemplos: giroscópio, acelerómetro.
- **Sensores ambientais**: concentram-se na informação sobre o ambiente do dispositivo. Exemplos: sensor de temperatura ambiente, sensor de deteção de luz, sensor de humidade, barómetro.
- **Sensores mistos ou compostos**: recolhem e integram dados de dois ou mais sensores num dispositivo. Exemplos: contador de passos, sensor vetorial rotacional
- **Sensores internos**: detetam e comunicam alterações relacionadas com o próprio dispositivo. Exemplos: carga de bateria.

Essas categorias não são mutuamente exclusivas e com sensores base ou sensores compostos, os programadores podem gerar aplicações complexas, que podem estar cientes do seu ambiente, entrada especial, e ações dos utilizadores.

Algumas das áreas de *mobile sensing* incluem saúde e bem-estar, segurança, mobilidade urbana, meio ambiente e agricultura.

Na área de saúde e bem-estar, sensores em dispositivos móveis podem ser usados para controlar a atividade física, sono, batimentos cardíacos, níveis de stress, entre outros aspetos relacionados à saúde [5].

Em relação à segurança, os sistemas de segurança ativa e passiva em veículos, como o *Honda SENSING*, usam sensores para alertar os motoristas sobre potenciais perigos na estrada [6].

Na mobilidade urbana, os sensores em dispositivos móveis podem ajudar na monitorização do tráfego, qualidade do ar e a poluição sonora nas cidades. Além disso, esses sensores podem ser usados para fornecer informações em tempo real sobre transportes públicos e congestionamento nas estradas, facilitando a navegação e reduzindo o tempo de deslocamento [5].

Na área do meio ambiente, sensores em dispositivos móveis podem ajudar a monitorizar o clima, a qualidade do ar e a qualidade da água, podendo também ser usados para ajudar os agricultores a controlar a humidade, a temperatura e a qualidade do solo.

A partir do momento em que a recolha de dados pessoais acontece em grande escala, ou seja, a partir de um grande número de pessoas, surge o *Mobile Crowd Sensing*, um termo muito bem definido por entidades relevantes. Segundo o *Institute of Electrical and Electronics Engineers* (IEEE), a MCS é definida como "uma abordagem que utiliza dispositivos móveis para recolher informações e conhecimentos de uma grande variedade de fontes, incluindo sensores de dispositivos móveis, e

para criar novas informações e conhecimentos que anteriormente eram impossíveis de se obter". Já a *Association for Computing Machinery* (ACM) define MCS como "uma técnica para recolha de dados em grande escala usando dispositivos móveis [...] para medir e coletar dados do ambiente ou do comportamento humano para inferir e prever eventos".

2.3 Ética e Privacidade em *Mobile Sensing*

Praticamente todos os *Mobile Sensing Systems* (MSSs) recolhem leituras de sensores relacionadas com os participantes e/ou os seus ambientes.

Obviamente, os dados recolhidos podem ser utilizados para extrair ou inferir informações sensíveis sobre a *"vida privada, hábitos, actos e relações"* de um utilizador - a definição básica de privacidade por [7].

Simultaneamente, os dados dos sensores contribuídos são vitais para qualquer aplicação, e a sua deficiência põe em perigo o sucesso dos sistemas. Os administradores precisam, portanto, de aumentar a sensibilização dos utilizadores para as consequências da divulgação de dados do sensor, bem como fornecer soluções para manter a privacidade do utilizador, a fim de assegurar a durabilidade da participação dos usuários na coleta de dados por meio de sensores, e impedir os participantes de optarem pela não participação.

Nesta secção, discutimos assim a noção de privacidade e ética com uma análise de privacidade para determinar atores e processos que representam ameaças à privacidade dos participantes, antes de destacar possíveis consequências resultantes da divulgação de informações sensíveis.

Análise da privacidade Baseia-se na análise da teoria da integridade contextual [8], que compreende as dimensões de adequação e distribuição.

A adequabilidade define-se como a revelação de uma determinada informação ser adequada num dado contexto, enquanto a distribuição se centra na ocorrência de uma transferência de informação de uma parte para outra. O conceito de integridade contextual define as violações da adequação ou distribuição como violações da privacidade de um utilizador.

As diferenças sócio-culturais e contextuais têm um forte impacto sobre a perceção individual da sensibilidade dos dados. Por exemplo, os utilizadores tomam diferentes decisões de privacidade, dependendo do número de destinatários dos seus dados [9].

Por conseguinte examinam-se as principais ameaças e potenciais consequências sociais da sensorização:

- **Tempo e Localização**: os recetores GPS incorporados na maioria dos dispositivos móveis atuais proporcionam coordenadas de localização. Contudo, na ausência do GPS (devido à falta de cobertura ou se o utilizador não quer revelar informações de localização de granulação fina), o *Wi-Fi* ou triangulação baseada em antenas pode ser utilizada para obter informações de localização de granulação grosseira. Informação contextual recolhida de outros sensores incorporados (tais como pontos de interesse, luz e ruído) também podem ser usados para identificar a localização de uma pessoa [10];

- **Amostras de Som e Áudios**: os dispositivos podem também comportar-se como "espiões" inteligentes no caso de gravações automatizadas. A interação dedicada do utilizador é necessária para impedir que os pedidos registem conversas privadas sobre assuntos íntimos ou confidenciais. Mesmo em locais públicos, o reconhecimento de padrões sonoros característicos que são exclusivos para certos eventos e locais podem permitir que os atacantes determinem o contexto corrente de um participante-alvo.
- **Imagens e Vídeos**: o conteúdo das fotografias e vídeos gravados é também suscetível de revelar informações pessoais sobre os participantes e o seu ambiente. Em todos os cenários, em que a câmara é orientada longe do participante, rostos de outras pessoas nas proximidades são possivelmente capturados nas imagens, e, portanto, as conclusões sobre o número e a identidade das relações sociais do participante podem ser desenhadas. Por exemplo, imagens a mostrar pontos de interesse podem facilmente estabelecer a presença dos envolvidos nesses locais comprometendo a sua segurança.
- **Aceleração**: as leituras do acelerómetro em bruto podem parecer menos ameaçadoras ao revelarem informações privadas sobre os participantes. No entanto, esta hipótese nem sempre é verdadeira e muitas vezes pode apenas serve como uma falsa sensação de segurança. Por exemplo, se o dispositivo for transportado na anca, podem ser inferidas informações sobre a marcha, e assim possíveis indicações sobre a identidade de um utilizador [11];
- **Dados de Ambiente**: o registo de partículas e concentrações de gás ou pressão barométrica não pode ameaçar diretamente a privacidade dos participantes por si só. No entanto, a combinação de dados de composição de ar com informações secundárias, como a temperatura, pode permitir a identificação da localização dos participantes com um alto nível de precisão, chegando ao ponto de identificar salas dentro de edifícios onde a localização pode ser imprecisa devido à falta de sinais de GPS ou outros serviços de localização;
- **Dados Biométricos**: os dados biométricos dos sensores podem ser utilizados para um diagnóstico da fisiologia atual de um utilizador. Por exemplo, a informação médica vazada pode ser utilizada pelo seguro de saúde de empresas ou empregadores para revogar contratos, se as condições fisiológicas dos participantes forem identificados.

Medidas Uma medida importante é o consentimento informado, onde os utilizadores são informados prévia e claramente sobre como seus dados serão coletados, usados e partilhados. Além disso, devem ter a opção de revogar o consentimento a qualquer momento.

Outra medida importante é a minimização de dados, onde os sensores reúnem apenas os dados necessários para fornecer seus serviços. A recolha deve limitar-se aos dados que são diretamente relevantes para o objetivo da aplicação. [12]

Por outro lado, é necessária a anonimização dos dados, onde as aplicações removem todas as informações que possam identificar um utilizador individual antes de partilhar dados com terceiros. A criptografia também é essencial para proteger a privacidade dos utilizadores, garantindo que a comunicação entre os dispositivo móvel e o servidor seja criptografada para evitar que os dados sejam intercetados por terceiros.[13]

Por fim, o armazenamento seguro de dados também é crucial, para evitar o acesso não autorizado, através da utilização de criptografia de dados em repouso e a autenticação de utilizadores autorizados. Além disso, as aplicações devem ser revistas regularmente para garantir que as medidas de segurança sejam eficazes. Estas medidas são analisadas em profundidade adiante.

3 Casos de Uso e algumas aplicações

De forma a contemplar uma maior variedade em relação às áreas que são alvo de estudo, providenciando uma melhor compreensão do estado da arte, segue-se um conjunto de casos de uso. Para cada um, é realizada uma descrição, com posterior análise das vantagens e desvantagens (riscos) em contextos éticos.

3.1 Saúde e bem-estar

Os dispositivos móveis podem ser utilizados para monitorizar a saúde e bem-estar dos utilizadores, coletando informações valiosas como frequência cardíaca, níveis de atividade física, sono e dieta. Depois de coletados, os dados são armazenados, sendo, depois, efetuada a respetiva análise, a partir da geração de *insights* personalizados e recomendações para melhorar a saúde. Neste âmbito, é relevante destacar que a utilização de *smartwatches* no setor da saúde tem crescido significativamente nos últimos anos, sendo que uma prova é, por exemplo, o facto de estes dados poderem ser compartilhados com médicos e profissionais de saúde, permitindo que eles monitorizem a saúde dos seus pacientes remotamente. Além disso, estes dispositivos permitem alertar os utilizadores sobre mudanças nos seus sinais vitais, algo especialmente útil para pessoas com condições de saúde crónicas, como doenças cardíacas ou pulmonares.

Ora, apesar disso, existem preocupações éticas relativas a cada fase deste fluxo dos dados, nomeadamente, quanto ao consentimento informado (aquando da coleta), à privacidade dos dados médicos (no armazenamento), e às potenciais discriminações [14] e fins das respetivas informações de saúde (numa pós-análise). Assim sendo, esta análise prende-se com a importância de garantir que a coleta, armazenamento e uso destes dados sejam realizados com ética e transparência, de modo a proteger a privacidade e os direitos de cada indivíduo.

Este domínio da *Mobile Health* (mHealth) encontra-se em constante investigação, nomeadamente, no âmbito de uma pesquisa sobre doenças alcoólicas (*Alcohol Use Disorders* - AUDs), foi de interesse, por exemplo, encontrar estratégias de sensorização, que permitissem tirar partido das vantagens que o campo oferece, mantendo a privacidade dos participantes, e naturalmente, não pondo em causa a própria pesquisa [15]:

Fase	Risco	Solução
Coleta Armazenamento Utilização	Consentimento	Informar claramente os indivíduos sobre que dados estão a ser coletados, o que se pode inferir a partir dos mesmos e que usos serão efetuados. De seguida, questionar sobre o consentimento.
Armazenamento Utilização	Vazamentos	Existência de uma *password, pin*, etc.
Utilização	Transmissão de dados	Utilizar mensagens não sensíveis no contacto dos indivíduos
Armazenamento Utilização	Acessibilidade de dados	Armazenar dados em duas localizações para garantir disponibilidade.

Table 1: Mitigação de riscos associados à privacidade dos indivíduos nas diferentes fases do fluxo dos dados [15].

É também já utilizada a autenticação de dois fatores e tipos de encriptação de dados, que contribuem para maior proteção destes.

Um outro estudo [16] investigou sobre a utilidade dos principais sensores de *smartphones* [17] na saúde, compreendendo o modo como os dados dos "pacientes virtuais" são postos em causa, e o atual estado da arte:

- **Acelerómetro:**
  - **Utilidades:**
    - Deteção de atividade física e/ou sedentária;
    - Relação da atividade física com o bem-estar mental.
  - **Vantagens (+) e Desvantagens (-):**
    - \+ Relativamente sensível à privacidade;
    - – Muito influenciado negativamente pelo posicionamento do dispositivo.
- **Luz Ambiente:**
  - **Utilidades:**
    - Compreensão do ambiente circundante;
    - Medição de quantidade de horas sem luz e relação com o estado de espírito/mental.
  - **Vantagens e Desvantagens:**
    - – Inferência muito limitada, mesmo quando combinada com outros sensores;
    - – Influenciado razoavelmente pelo posicionamento do dispositivo.
- **Câmara:** captura de imagens e vídeos.
  - **Utilidades:**
    - Captura de imagens faciais e relação com as emoções;
    - Rastreio do movimento ocular e inferência sobre as emoções.
  - **Vantagens e Desvantagens:**
    - – Monitorização do comportamento do indivíduo;
    - – Altas preocupações de privacidade, especialmente devido à gravação de vídeo.

3.2 Assistência a desastres e resposta a emergências

O *Mobile Sensing* pode ser também utilizado para monitorizar e responder a desastres naturais e emergências, através do rastreio da localização dos utilizadores, e das condições ambientais, fornecendo informações em tempo real. As principais preocupações éticas incluem a privacidade dos dados, o uso indevido de informações

para fins mal-intencionados e a responsabilidade das empresas de tecnologia na gestão de crises.

Os sensores mostram-se relevantes neste âmbito, porque permite obter informação valiosa a baixo custo sobre a gestão de desastres. Esta gestão é iniciada através de *crowd reporters*, isto é, utilizadores que reportam o incidente através das capacidades de sensorização do dispositivo, sendo a ocorrência verificada por um agente oficial. Este conceito é alvo de discussão entre a comunidade científica [18], sendo considerado como um sensor indireto humano. Então, tendo em conta as principais categorias na qual se classificam os problemas de gestão de desastres, é possível analisar a relação com algumas questões éticas muito relacionadas com o conteúdo sensível que os sensores possam coletar, especialmente, em situações de desastres [19].

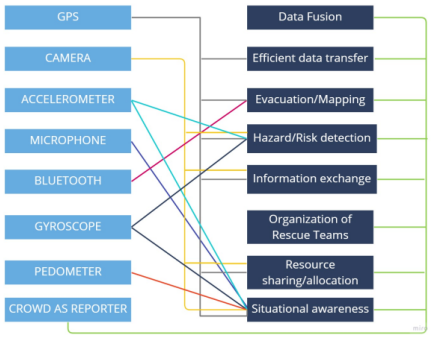

Fig. 2: Sensores utilizados nas várias categorias de gestão de desastres. [18]

Deteção de perigos e riscos em áreas afetadas por desastres Alguns autores [20] propõem, por exemplo, um sistema que usa *smartphones* como sensores distribuídos para detetar colapsos de edifícios usando o acelerómetro. Já outros [21] discutem a identificação dos principais locais e tipos de danos, usando dados de imagem coletiva de satélites e drones. Nesta direção, surge a necessidade de gerar um mapeamento de risco da comunidade, usando sinais de GPS dos *smartphones* dos cidadãos para estimar movimentos futuros e calcular fatores de risco para as comunidades com antecedência. Essas imagens coletivas incluem fotografias aéreas, mapas de calor e outras formas de visualização de dados que ajudam a identificar áreas que foram mais afetadas pelo desastre. Contudo, levantam-se preocupações éticas de privacidade, como a necessidade de mais informações para garantir a veracidade dos dados transmitidos e o desafio de motivar os utilizadores a compartilhar informações.

Mapeamento e Evacuação A maioria dos estudos neste âmbito propõem soluções que usam sensores de *smartphones* para auxiliar na evacuação e mapeamento durante um desastre. Temos o exemplo de Bhattacharjee e outros [22], que propõem um sistema de construção de mapas pós-desastre que coleta dados de sensores GPS para construir mapas de pedestres para guiar as vítimas a lugares mais seguros; a utilização de uma técnica de *Bluetooth Low Energy* (BLE) autónoma de baixo custo, para guiar os utilizadores a saídas de emergência. Esta técnica é uma

tecnologia de comunicação sem fio de curto alcance, que foi criada para reduzir o consumo de energia em dispositivos móveis. Esta técnica socorre-se de sensores de movimento instalados nas saídas de emergência, fornecendo uma visualização em tempo real das rotas de evacuação e informações relevantes para equipas de resgate.

De um modo geral, estas soluções levantam questões éticas e de privacidade, especialmente em termos de coleta e uso de dados confidenciais do utilizador durante um desastre, sendo necessário garantir anonimização dos dados, os quais devem ser tratados de forma que não seja possível identificar as pessoas que os forneceram. Neste âmbito, existem estudos que discutem uma arquitetura possível para os sensores embutidos nos dispositivos móveis, nomeadamente, através de um *Anonymizer*, um *autoencoder* pré-treinado que transforma a informação antes de a mesma ser partilhada [23]. Esta é uma técnica de privacidade que permite compartilhar dados pessoais de forma segura, garantindo que os dados continuam encriptados e anónimos. Os dados são codificados e alvo de criptografia antes da partilha. Após essa partilha, os dados podem não continuar encriptados, todavia, devem ser igualmente anónimos, já que, para poderem ser utilizados para análise e pesquisa, não podem ser vinculados a indivíduos específicos.

4 Desafios e Oportunidades

Como foi possível observar anteriormente, embora toda esta tecnologia ofereça inúmeros benefícios, ela acaba por levantar questões éticas significativas. O desafio está em encontrar maneiras de equilibrar os potenciais benefícios com a necessidade de proteger a privacidade e a segurança individuais. Uma vez que o foco são as questões de privacidade, analisam-se aspetos relevantes nesse sentido.

4.1 Recolha de dados nas grandes cidades

Um dos principais desafios é a coleta de dados precisos e confiáveis em ambientes urbanos densamente povoados. Ruídos e interferências eletromagnéticas podem afetar a precisão dos sensores, levando a dados imprecisos e potencialmente prejudiciais[24]. É importante ter em conta a própria infraestrutura necessária para implementar a sensorização em dispositivos móveis nas mesmas, sendo indispensável garantir que haja cobertura de rede suficiente para permitir a transmissão de dados em tempo real, além de garantir a segurança da rede contra ataques cibernéticos [25].

Apesar desses desafios, esta tecnologia tem um enorme potencial para melhorar a qualidade de vida nas grandes cidades. Desde a monitorização da qualidade do ar até à gestão do tráfego urbano, contribuindo para a criação de cidades mais inteligentes e sustentáveis [26].

4.2 *Mobile Crowd Sensing* (MCS)

Os artigos [27] [28] [29] sintetizam de uma forma clara os principais conceitos subjacentes ao MCS, expondo, para as várias tarefas onde há recolha de dados por sensores, pontos onde podem existir ameaças à privacidade dos participantes, e apresenta, de seguida, algumas estratégia de proteção dos dados:

- ***Temporal Cloaking*:** técnica utilizada na transmissão ótica de dados como forma de os esconder através da criação de uma "lacuna"/intervalo no tempo: manipula-se o domínio de tempo do sinal da luz, para criar uma janela de ocultação temporal, onde os dados são indetetáveis;
- ***Spatio-temporal Cloaking*:** é uma extensão da técnica anterior, mas com uma extensão da janela temporal no espaço: com a vantagem adicional de ocultar não apenas o momento, mas também o local dos eventos.
- ***Private Information Retrieval*:** técnica usada para recuperar informações de um banco de dados sem revelar a identidade do utilizador ou as informações recuperadas;
- ***Policy-based Privacy Preferences*:** *framework* para gerir preferências de privacidade em sistemas distribuídos. Envolve a definição de políticas que especificam como os dados do utilizador podem ser obtidos e usados em diferentes contextos.

A tabela seguinte consegue resumir as medidas descritas anteriormente, relacionando-as com as soluções apresentadas.

Privacy Threats	Tasking Scenarios	Countermeasures
Task Tracing	Pulling specific tasks Coordinated task assignment Push-based tasks with notification	Anonymization Temporal Cloaking
Location-based Inference	Spatial tasks	Spatio-temporal cloaking Private information retrieval
Narrow Tasking	All tasking schemes	Policy-based Privacy Preferences
Selective Tasking	Coordinated task assignment Push-based tasks	Policy-based Privacy Preferences
Collusion Attacks	All tasking schemes	Policy-based Privacy Preferences

Fig. 3: Principais ameaças em MCS, nas várias tarefas, e estratégias de resolução [27]

É possível observar que, quando é realizado um ataque que pretende obter informação sobre que tarefas (e de que forma) estão a ser realizadas - casos de tarefas coordenadas, por exemplo-, a medida comum de proteção é a utilização de anonimização ou *Temporal Cloaking*. Em contrapartida, quando o objetivo é saber a localização de alguém, já é necessário adicionar *Cloaking* Espacial, que vai encriptar a informação a nível espacial. Em relação a *Narrow e Selective Tasking*, técnicas que envolvem a atribuição de tarefas específicas e limitadas a um indivíduo ou grupo, socorre-se à utilização de políticas de privacidade (com preferência gerida pelo utilizador) como contra medida.

5 *Mobile Sensing* no Mundo Real

Existem várias aplicações do *Mobile Sensing* no mundo real.

No âmbito da monitorização ambiental, nomeadamente, monitorização de tráfego, previsão do tempo e medição de níveis de ruído em áreas urbanas. Um exemplo específico de aplicação é a monitorização de catástrofes: detetar e monitorizar eventos como terremotos, inundações e deslizamentos de terra, como se observou anteriormente. [30] [31] [32]

Na área de logística, um bom exemplo é monitorizar a localização de bens e mercadorias, algo especialmente útil em situações de transporte internacional, onde

a mercadoria pode passar por várias etapas até chegar ao seu destino final. Sensores RFID (Identificação por Radiofrequência) e GPS são comummente usados para este meio [31].

No campo da saúde, várias aplicações móveis podem ser utilizadas para monitorizar sinais vitais e compartilhar informações com profissionais de saúde em tempo real, permitindo um cuidado mais personalizado e eficiente. A tecnologia móvel também tem sido fundamental para a disseminação de informações e serviços de saúde em áreas mais remotas e carentes de recursos médicos. No Brasil, por exemplo, a tecnologia móvel tem ajudado a expandir o acesso a serviços de saúde em áreas rurais e comunidades carentes. Para além disso, a tecnologia de sensores biomédicos miniaturizados e inteligentes, que coletam dados sobre a atividade muscular, a pressão arterial, a temperatura corporal e muito mais [32], permite monitorizar a saúde humana em tempo real, garantindo mais eficiência em situações de emergência médica. Com base na plataforma *MobiSens*, foram desenvolvidas aplicações para este fim, como o *Mobile Lifelogger* e o *SensCare* para cuidados assistidos [30].

6 Conclusão e Trabalho Futuro

A sensorização tem inúmeras vantagens e oferece muitas oportunidades para melhorar a vida das pessoas, desde a monitorização da saúde até à gestão de transportes na área logística. Então, existe uma grande variedade de sensores que podem ser utilizados a baixo custo em diversas áreas.

Contudo, ainda existem barreiras a ultrapassar como os desafios éticos e de privacidade significativos. Neste contexto, concluiu-se que os utilizadores devem ser informados de forma clara e precisa sobre como seus dados são coletados, usados e protegidos, e ter o direito de controlar suas informações, ao longo das várias fases do fluxo dos seus dados.

Deste modo, é essencial consciencializar os utilizadores sobre os seus direitos virtuais, mas também que identidades governamentais e empresariais consigam garantir a privacidade e segurança dos dados pessoais dos cidadãos.

Quanto ao estado da arte, os pesquisadores e desenvolvedores de dispositivos devem também adotar medidas adequadas para garantir a segurança dos dados e evitar o uso indevido ou partilha não autorizado.

Além disso, as regulamentações e políticas devem ser atualizadas para acompanhar a rápida evolução da tecnologia e garantir a proteção dos direitos. A abordagem equilibrada entre o desenvolvimento tecnológico e a ética e privacidade deve ser considerada como uma responsabilidade partilhada entre todos os envolvidos, incluindo desenvolvedores, reguladores e utilizadores finais.

Em relação a trabalho futuro, analisaram-se inúmeros desafios que urgem ser ultrapassados de modo a que a segurança dos dados dos indivíduos seja bem conseguida, desde alterações à própria infraestrutura das grandes cidades, tornando a coleta de dados mais confiável e precisa nas grandes cidades, até a adoção completa de técnicas de encriptação em contextos de MCS, como já ocorre em vários países. A sensorização em dispositivos móveis é uma área em constante desenvolvimento que proporcionará uma variedade enorme de alterações à vida quotidiana da população em geral.

Siglas e Acrónimos

mHealth *Mobile Health*
AUDs *Alcohol Use Disorders*
MCS *Mobile Crowd Sensing*
BLE *Bluetooth Low Energy*
MSSs *Mobile Sensing Systems*
IEEE *Institute of Electrical and Electronics Engineers*

Referências

1. *Computação ubíqua – Wikipédia, a enciclopédia livre.*
2. José Bidarra. "O Papel do Mobile Learning na Educação 1". In: ().
3. *What is Mobile Sensing — IGI Global.*
4. *An All-Inclusive Guide On The Top IoT Sensors In The Market.*
5. Francisco Laport-López, Emilio Serrano, Javier Bajo, and Andrew T. Campbell. "A review of mobile sensing systems, applications, and opportunities". In: *Knowledge and Information Systems* 62 (1 Jan. 2020), 145–174. ISSN: 02193116.
6. *Sistemas de segurança: Conheça o Honda SENSING — Honda Portugal.*
7. Samuel D Warren and Louis D Brandeis. "The Right to Privacy". In: *Law Review* 4 (5 1890), 193–220.
8. *"Privacy as Contextual Integrity" by Helen Nissenbaum.*
9. Karen P. Tang, Jialiu Lin, Jason I. Hong, Daniel P. Siewiorek, and Norman Sadeh. "Rethinking location sharing: exploring the implications of social-driven vs. purpose-driven location sharing". In: *Proceedings of the 12th ACM international conference on Ubiquitous computing* (2010), 85–94.
10. Anthony LaMarca, Yatin Chawathe, Sunny Consolvo, Jeffrey Hightower, Ian Smith, James Scott, Timothy Sohn, James Howard, Jeff Hughes, Fred Potter, Jason Tabert, Pauline Powledge, Gaetano Borriello, and Bill Schilit. "Place lab: Device positioning using radio beacons in the wild". In: *Lecture Notes in Computer Science* 3468 (2005), 116–133. ISSN: 03029743.
11. Cesar Torres-Huitzil and Andres Alvarez-Landero. "Accelerometer-Based Human Activity Recognition in Smartphones for Healthcare Services". In: (2015), 147–169.
12. Moshaddique Al Ameen, Jingwei Liu, and Kyungsup Kwak. "Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications". In: ().
13. Gao Liu, Zheng Yan, and Witold Pedrycz. "Data collection for attack detection and security measurement in Mobile Ad Hoc Networks: A survey". In: *Journal of Network and Computer Applications* 105 (Mar. 2018), 105–122. ISSN: 1084-8045.
14. *Os efeitos da inteligência artificial na vida profissional das mulheres.* ISBN: 9786586603248.
15. Jennifer Yttri, Wendy Nilsen, and Shifali Arora. *Privacy and Security in Mobile Health (mHealth) Research.*
16. Pranav Kulkarni, Reuben Kirkham, and Roisin McNaney. *Opportunities for Smartphone Sensing in E-Health Research: A Narrative Review.* May 2022.

17. Ming Liu. "A study of mobile sensing using smartphones". In: *International Journal of Distributed Sensor Networks* 2013 (2013). ISSN: 15501329.
18. Didem Cicek and Burak Kantarci. *Use of Mobile Crowdsensing in Disaster Management: A Systematic Review, Challenges, and Open Issues*. Feb. 2023.
19. Francisco Laport-López, Emilio Serrano, Javier Bajo, and Andrew T. Campbell. "A review of mobile sensing systems, applications, and opportunities". In: *Knowledge and Information Systems* 62 (1 Jan. 2020), 145–174. ISSN: 02193116.
20. Aku Visuri, Zeyun Zhu, Denzil Ferreira, Shin'ichi Konomi, and Vassilis Kostakos. "Smartphone detection of collapsed buildings during earthquakes". In: Association for Computing Machinery, Inc, Sept. 2017, 557–562. ISBN: 9781450351904.
21. Yoonjo Choi, Namhun Kim, Seunghwan Hong, Junsu Bae, Ilsuk Park, and Hong Gyoo Sohn. "Critical image identification via incident-type definition using smartphone data during an emergency: A case study of the 2020 heavy rainfall event in Korea". In: *Sensors* 21 (10 May 2021). ISSN: 14248220.
22. Christodoulos Asiminidis, Georgios Kokkonis, and Sotirios Kontogiannis. "BLE Sniffing for Crowd Sensing and Directionality Scanning of Mobile Devices Inside Tunnels". In: Institute of Electrical and Electronics Engineers Inc., Oct. 2020, 54–58. ISBN: 9781728185644.
23. Mohammad Malekzadeh, Richard G. Clegg, Andrea Cavallaro, and Hamed Haddadi. "Mobile sensor data anonymization". In: Association for Computing Machinery, Inc, Apr. 2019, 49–58. ISBN: 9781450362832.
24. Xiangjie Kong, Xiaoteng Liu, Behrouz Jedari, Menglin Li, Liangtian Wan, and Feng Xia. "Mobile Crowdsourcing in Smart Cities: Technologies, Applications, and Future Challenges". In: *IEEE Internet of Things Journal* 6 (5 Oct. 2019), 8095–8113. ISSN: 23274662.
25. Raghu K. Ganti, Fan Ye, and Hui Lei. "Mobile crowdsensing: Current state and future challenges". In: *IEEE Communications Magazine* 49 (11 Nov. 2011), 32–39. ISSN: 01636804.
26. Jinwei Liu, Haiying Shen, and Xiang Zhang. *A Survey of Mobile Crowdsensing Techniques: A Critical Component for The Internet of Things*.
27. Layla Pournajaf, Li Xiong, Daniel A Garcia-Ulloa, and Vaidy Sunderam. *A Survey on Privacy in Mobile Crowd Sensing Task Management*.
28. Djallel Eddine Boubiche, Muhammad Imran, Aneela Maqsood, and Muhammad Shoaib. "Mobile crowd sensing – Taxonomy, applications, challenges, and solutions". In: *Computers in Human Behavior* 101 (Dec. 2019), 352–370. ISSN: 07475632.
29. Xiang Sheng, Jian Tang, Xuejie Xiao, and Guoliang Xue. "Sensing as a service: Challenges, solutions and future directions". In: *IEEE Sensors Journal* 13 (10 2013), 3733–3741. ISSN: 1530437X.
30. Pang Wu, Jiang Zhu, and Joy Ying Zhang. "MobiSens: A versatile mobile sensing platform for real-world applications". In: vol. 18. Kluwer Academic Publishers, Feb. 2013, 60–80.
31. Jennifer R Kwapisz, Gary M Weiss, and Samuel A Moore. *Activity Recognition using Cell Phone Accelerometers*. 2010. ISBN: 9781450302241.
32. Bruno Biagianti. "What Can Mobile Sensing and Assessment Strategies Capture About Human Subjectivity?" In: *Frontiers in Digital Health* 4 (Apr. 2022). ISSN: 2673253X.