Smart Cities: Security and Privacy Challenges

Henrique Paz, Joana Afonso Gomes, João Neves

Outubro 2019

University of Minho, Department of Informatics, 4710-057 Braga, Portugal

e-mail: a84372,a84912,a81366@alunos.uminho.pt

Abstract: Hoje em dia é possível a interconexão digital de objetos quotidianos físicos com a Internet, passando por veículos, prédios, sensores e conexões com a rede. Isto gera uma enorme quantidade de dados, que podem ser aproveitados para garantir a segurança e a eficiência dadas aplicações e dos serviços para os residentes das cidades (***Smart Cities***). A existência destas *Smart Cities* depende de uma gerência eficaz desses dados fortemente interligados durante o seu ciclo de vida, com **aspetos transversais de segurança e privacidade dos dados**, e ainda infraestruturas de suporte.

1 Introdução

Neste ensaio identificaremos **técnicas usadas** para segurança e privacidade de dados e discutimos as tecnologias de rede e computação que permitem a existências das *Smart Cities*, indicando as suas **limitações** e **desafios** de pesquisa.

2 Segurança e privacidade das *Smart Cities*

As *Smart Cities* nascem da confluência dos seus cidadãos, infraestruturas e tecnologias de informação e comunicação, a fim de melhorar o gerenciamento dos recursos. Isto apresenta, portanto, muitos benefícios, mas surgem também vários **desafios no que toca à segurança e à privacidade**, quando não são implementados adequadamente. Apesar dos riscos associados à segurança serem uma parte inerente se qualquer sistema tecnológico do género, no caso das *Smart Cities* o impacto torna-se bastante mais relevante, dada a simbiose das infraestruturas com as tecnologias. Isto porque se, por exemplo, uma conta

de e-mail for hackeada, pode causar problemas a um único indíviduo, mas se acontecer o mesmo com uma *Smart Grid*[1], poderá paralisar uma cidade inteira.

Uma manifestação real deste tipo de ameaças foi o ***worm***[2] **de Stuxnet**. Acredita-se que tenha sido criado para atingir o programa nuclear iraniano e, até ser descoberto, já havia inutilizado mais de 30% das centrífugas das instalações nucleares.

Imagem 1: *Cartoon* do *worm* de *Stuxnet*
Fonte: *https://www.nytimes.com*

É difícil analisar os desafios à segurança e à privacidade das *Smart Cities*, dada a complexidade dos sistemas e ao envolvimento de vários participantes, sendo afetadas por fatores tecnológicos, socioeconómicos e governamentais. Focar-nos-emos mais na discussão de alguns possíveis **desafios tecnológicos**, os seus componentes e possíveis soluções.

2.1 Desafios e ameaças

As *Smart Cities* conduzem a uma nova fase da Internet e das comunicações e, com isso, a uma nova era de ameaças à *cyber*-segurança. Nelas milhões de dispositivos coletam, armazenam e processam dados de forma omnipresente, usando o hardware incorporado. A heterogeneidade das tecnologias nas *Smart Cities* torna a segurança e a privacidade um problema multidimensional, para o qual as soluções tradicionais podem não resultar, já que vários aspetos as tornam vulneráveis a ameaças que são incomuns nas redes cibernéticas tradicionais. Ataques em *Smart Cities* podem surgir da integração de diferentes tecnologias que são predispostas a problemas de incompatibilidade e, em alguns casos, não são contruídas com as questões da segurança em mente. Outro aspeto vulnerável é a natureza de distribuição física das redes destas cidades, que podem

[1] Rede elétrica inteligente que usa a tecnologia da informação para fazer com que o sistema seja mais eficiente, econômica e energeticamente (**Ver mais à frente**).

[2] Semelhante ao vírus, mas enquanto este infecta um programa e necessita deste programa hospedeiro para se alastrar, o *worm* é um programa completo e não precisa de outro para se propagar.

incorporar um grande número de pequenos dispositivos e sensores, introduzindo novas ameaças à segurança e à privacidade, já que aumentam a superfície de ataque. Para além disso, o uso deste tipo de dispositivos de baixo custo e proprietários aumenta o risco destes problemas, em situações como, por exemplo, ladrões que usam imagens de câmeras, dados de sensores de movimento, microfones embutidos ou registo de luzes para descobrir quando os habitantes não estão em casa. Outro problema destas opções mais baratas é a possibilidade de não terem capacidade para suportar as soluções criptográficas necessárias para contrariar ameaças.

Analisaremos de seguida ameaças e desafios de quatro componentes essenciais das *Smart Cities*.

2.1.1 *Smart Grids* (SG)

As redes elétricas evoluíram imenso desde a sua criação, porém a que permaneceu como a rede clássica foi a de fluxo unidirecional, que tem várias falhas e não é adequada para a sociedade atual. Considerando que é difícil para os distribuidores prever com precisão do pico de utilização, precisam de gerar energia a mais para sustentar a procura durante os horários de pico, o que resulta em poluição ambiental e contribuição para o aquecimento global. Para além disso, as redes elétricas tradicionais não têm a capacidade de informar os consumidores sobre o uso de energia, o que os poderia ajudar a planear e controlar o gasto, aumentando a eficiência. Para tentar superar estes problemas, foi proposta a estrutura para uma nova geração de sistemas de energia elétrica, denominada *Smart Grids*, que cria uma infraestrutura de comunicação bidirecional que suporta novas aplicações como um sistema medidor avançado, resposta a pedidos, gerenciamento da rede de distribuição e reconhecimento de toda a área.

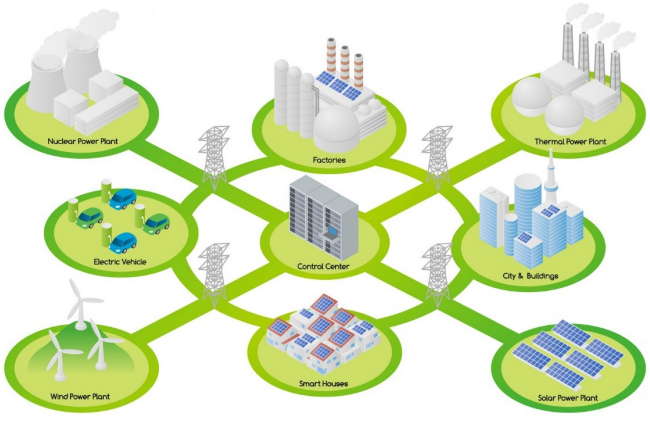

Imagem 2: Exemplo de uma *Smart Grid*
Fonte: *https://www.smartcitiesworld.net*

Embora isto nos permitisse **usar a rede com muito mais eficiência**, o adicional sistema bidirecional de comunicações será **mais suscetível a *cyber*-ataques**.

Um dos problemas dos SG é a sua natureza de distribuição, dado que estão distribuídos por várias centenas de quilómetros quadrados, com várias subestações, sendo que cada uma pode funcionar como entrada direta para a rede, pondo em causa a segurança física dos mesmos.

Existem várias soluções propostas para os desafios acima mencionados, **sistemas de deteção de intrusões ativos e passivos**. Estes, embora eficientes nas redes clássicas de computadores, ainda têm limitações na **ICS** (***Internet Connection Sharing***) que precisam de ser abordados. Já há projetos para usar uma Shadow Security Unit capaz de intercetar de forma transparentes os canais de comunicação e processar linhas I/O para monitorar a segurança do sistema. Essas soluções são baratas e não intrusivas.

Foram propostos dispositivos de impressão digital para monitorar a segurança da ICS, que são adequados para as SG, pois as redes são distribuídas e manter a segurança física é muito complicado.

2.1.2 *Smart Mobility* (SM)

SM é a aplicação de soluções TIC para resolver problemas de mobilidade (poluição, acidentes, congestionamento de tráfego...) que os cidadãos enfrentam. Essas questões têm consequências tanto sociais (ex: todos os anos mais de 1.2 milhões de vidas são perdidas a nível mundial devido a acidentes de trânsito) como económicas (ex: os congestionamentos nas estradas nos EUA custam $37.5 biliões a cada ano). Apesar de todas as vantagens, a SM não é isenta de desafios, visto que as consequências de falhas de segurança nos seus sistemas podem ser fatais.

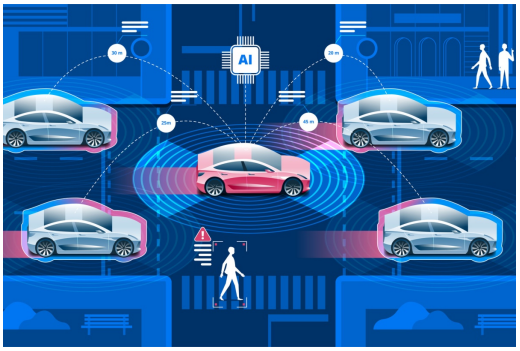

Imagem 3: Aplicações da *Smart Mobility*
Fonte: *https://www.smartcitiesworld.net*

Imagine-se, por exemplo, que alguém mal-intencionado faz um veículo em movimento rápido na estrada travar com força para evitar colidir com um veículo imaginário à sua frente. Isso pode ser fatal se houver veículos atrás do veículo em questão.

Para entender a SM, é necessário abarcar uma gama ampla de sistemas e tecnologias. Proteger um sistema heterogéneo é uma tarefa árdua. Para identificar melhor potenciais ameaças à segurança e estimar a performance da segurança do sistema, é preciso identificar objetivos e requisitos. Na ITS (*Intelligent Transportation Systems* / Sistemas Inteligentes de Transporte), os dados trocados não devem ser sujeitos a modificações intencionais ou não intencionais. Se tal acontecer, é possível a utilizadores mal-intencionados aproveitarem-se do sistema (ex: ***Sybil attack***, cf. Tabela 1), resultando em graves consequências (por exemplo, a falsificação de certificados dificulta a identificação de veículos mal-intencionados em caso de disputas). Os ataques ***Denial of Services* (DoS)** e **DDoS** (cf. Tabela 1) são as ameaças mais sérias à disponibilidade dos serviços.

Os utilizadores da ITS dependem de serviços fornecidos pelo sistema, e a ausência deles pode ter consequências diretas (tais como inundações e obstruções ou impedimento/atraso da recessão de mensagens básicas de segurança - *Basic Safety Messages* (BSM) – por veículos na autoestrada, que podem ser fatais). Ataques à integridade dos sistemas de ITS incluem ataques de adulteração de dados (por exemplo, ataques ***man-in-the-middle*** ou **ataques de *replay***, cf. Tabela 1), uso/acesso não autorizado (Ex: **ataques de *replay***, cf. Tabela 1), e ataques de adulteração por difusão.

A disponibilidade dos serviços ITS é importante porque os utilizadores dependem dos serviços oferecidos para tomar decisões (por exemplo, pedestres serem avisados da aproximação de um veículo). Um ataque malicioso que impessa ou atrase a propagação de mensagens pode ter consequências fatais. Os ataques à disponibilidade não são necessariamente complexos. Ataques simples como interferências podem impedir ou atrasar a entrega de mensagens em redes wireless, de que os ITS dependem. Os ataques à disponibilidade do sistema (*attacks on availability*) incluem a já referida interferência, *floddin*, DoS, DDoS e *Sybil attacks*.

2.1.3 *Smart Homes* (Casas Inteligentes)

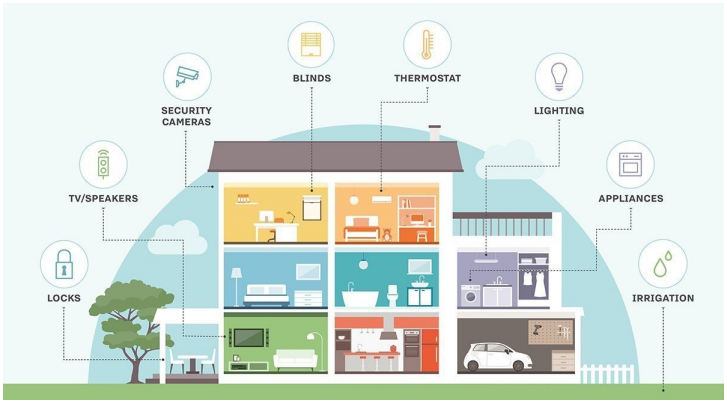

Imagem 4: Aspetos das *Smart Houses*
Fonte: *https://internetofthingsagenda.techtarget.com*

As *smart homes* são outro componente das *Smart Cities* que representa enormes ameaças à segurança e à privacidade. Os eletrodomésticos estão-se a tornar mais inteligentes a cada dia e, em breve, os cidadãos poderão controlar todos os aspetos das suas casas, local e remotamente, por meio de *smart home systems*. O *Google Home* e a *Amazon Echo* são dois dos mais recentes *gadgets* que permitem os utilizadores controlarem algumas partes das suas casas. *Smart TVs* equipadas com microfones e câmeras, câmeras de segurança com sensores de movimento, termostatos, lâmpadas (ex: *Philips Hue Lights*), frigoríficos, fechaduras de portas e persianas inteligentes já existem em muitas residências. Apesar de tais sistemas serem valiosos e nos conseguirem ajudar a gerenciar melhor as nossas casas, os seus aspetos de segurança e privacidade não estão a ser bem estudados, sendo muitos desses dispositivos produzidos por fabricantes que não os têm em conta. Um estudo em que foi analisada a estrutura de programação da SmartThings (que pertence à *Samsung*) afirma que 55% das *smart apps* na sua loja são superprivilegiadas, no sentido em que podem aceder a funcionalidades que não usam e, assim, estarem facilmente expostas a entidades maliciosas.

Com base em documentos publicados pela *WikiLeaks*[3], a CIA já possui a capacidade e as ferramentas para *hackear* qualquer *smart applicance* que esteja presente nas nossas casas. Tal não é surpreendente dado os recursos da CIA, mas esses ataques não são assim tão difíceis dada a falta de segurança dos dispositivos, sendo que testes mostraram ser relativamente simples, por exemplo,

[3]organização sem fins lucrativos, sediada na Suécia, que publica, na sua página, publicações de fontes anónimas, documentos, fotos e informações confidenciais, *vazadas* de governos ou empresas, sobre assuntos sensíveis.

trocar códigos de fechaduras ou introduzir alarmes falsos. Isto é preocupante e perigoso, visto que a sociedade caminha para um predomínio das *Smart Homes* a um ritmo muito rápido.

Usuários mal-intencionados podem beneficiar bastante da recolha de dados de dispositivos pessoais usados nestas casas. Por exemplo, os dados obtidos podem ser usados para traçar o perfil e rastrear o usuário, ou para iniciar outros tipos de ataques.

A diferença mais curiosa entre os ataques tradicionais à segurança e privacidade dos computadores e os ataques às *Smart Homes* é o número de maneiras diferentes como essas pessoas podem obter acesso. Os *ladrões* conseguem determinar onde e quando roubar baseando-se em registos de câmeras de segurança, sensores de movimento ou padrões no uso da energia, obtendo acesso às residências-alvo explorando os pontos fracos das fechaduras *inteligentes*. Estes ataques podem causar não só danos financeiros como também enormes invasões à privacidade.

Para combater ataques a *smart homes* será preciso introduzir melhores padrões de *hardware*, para que os sensores e outros dispositivos não fiquem vulneráveis a ataques comuns. Para além disso, os fabricantes de eletrodomésticos têm que melhorar a segurança dos seus *softwares*. Os dispositivos devem ser possíveis e fáceis de atualizar de forma remota e de instalar novos *patches* [4].

[4] Programas de computador criados para atualizar ou corrigir um software de forma a melhorar sua usabilidade ou performance.

2.1.4 *Smart Governance*

SmartGorvernance consiste em apoiar a integração e a colaboração de diferentes agências do governo e combinar os seus processos, assim centralizando o local da informação, resultando em operações mais eficientes, melhor manuseamento dos dados comuns e melhor regulação. No geral é uma boa implementação, já que assim temos políticas melhores e mais eficientes para o público em geral. Encontramos no entanto bastantes desafios na sua implementação, tais como:

1. *Fonte dos dados e características*
   Os dados são gerados de diferentes tipos de fontes e em diferentes formatos. Só o tentar encapsular estes diferentes é um processo muito complexo que faz com que seja muito difícil gerir a grande quantidade e complexidade dos diferentes tipos de dados.

2. *Partilha de dados*
   Como diferentes tipos de dados estão espalhados por diferentes agências, cada uma com políticas e condições de privacidade diferentes, torna-se difícil permitir a partilha de dados sem infringir os direitos de cada cidadão. Assim é necessário ter **regulações mais estritas** para combater esse tipo de infrações.

3. *Segurança acrescentada de cada ramo*
   A partilha de informações desta escala entre agências diferentes requer uma segurança aumentada sobre essas agências para não ocorrer fugas de informação devida à falta de segurança. Para além disso, também é necessário reforçar a segurança na navegação de informação entre ramos, para não acontecer o mesmo.

Ataque	Descrição e contramedidas
Alteração e modificação de dados	Usuários mal-intencionados podem quebrar a integridade dos dados alterando, excluindo ou fabricando o seu conteúdo. **Public Key Infrastructure** (infraestrutura de chave pública), ou **PKI**, pode ser usada para combater esses ataques.
Ataque Mascarado (*Masquerade attack*	Ataque que utiliza uma identidade falsa para ganhar acesso não autorizado a informação de computadores pessoais, através do acesso à informação, seja usando *passwords* e *logins* roubados, localizando falhas em programas, ou a contornar o processo de autenticação (que deverá estar devidamente protegido para procurar evitar este tipo de ataques). Podem ser desencadeados por alguém dentro da organização ou por um *outsider* no caso de esta estar conectada a uma rede pública.
Ataque de repetição (*Replay attack*, a.k.a. *Playback Attack*)	É uma forma de ataque em que uma transmissão de dados válidos é repetida ou atrasada maliciosamente/de forma fraudulenta. Este é executado pelo criador ou por um *adversary.** *Em criptografia, um adversário é uma entidade maliciosa cujo objetivo é impedir que os usuários do sistema atinjam seu objetivo (passando pela privacidade, integridade e disponibilidade de dados), tentando descobrir dados secretos, corrompendo alguns dos dados no sistema, falsificando a identidade de um remetente ou destinatário de uma mensagem, ou forçando o tempo de inatividade do sistema.
Man-in-the-middle	O invasor retransmite e, possivelmente, altera as comunicações entre duas entidades que acreditam estar a comunicar diretamente uma com a outra. Um exemplo deste ataque é a escuta não-autorizada, em que o atacante faz comunicações independentes com as vítimas e transmite mensagens entre elas, fazendo-as acreditar que estão a ter uma conversa privada uma com a outra, quando na realidade a conversa inteira está a ser controlada por outra pessoa. Esta pessoa tem que ser capaz de intercetar todas as mensagens, o que é simples em muitas circunstâncias (por ex., se o invasor estiver dentro do alcance da receção de um ponto de acesso *Wi-Fi* não encriptado).

Tabela 1: Ameaças à segurança e contramedidas.

Ataque	Descrição e contramedidas
Sybil attack	Tipo de ataque visto em redes *peer-to-peer*** nos quais um nó da rede opera ativamente várias identidades ao mesmo tempo. O objetivo principal é ganhar a maior parte do poder da rede e realizar ações ilegais no sistema. Uma identidade única (um computador) tem a capacidade de criar e comandar várias identidades (contas de utilizador, contas baseadas endereços IP...). Para observadores de fora, estas diversas identidades falsas parecem únicas e reais. **Arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.
GPS spoofing **(Manipulação da transmissão e transação)**	Uma emissora de rádio localizado perto do alvo é usada para interferir com um sinal de GPS legítimo. O atacante consegue impedir a transmissão de dados ou enviar coordenadas erradas.
Broadcast and transaction tampering **(falsificação do sinal GPS)**	Introdução de dados falsos no sistema usando a transmissão (*broadcast*) de mensagens. Na manipulação das transações, o utilizador malicioso pode corromper os dados transmitidos ou criar uma resposta alternativa a utilizadores inocentes e que de nada suspeitam. Usar autenticações e certificados digitais pode prevenir estes ataques.
DoS (Denial-of-service attack)	O autor do crime procura fazer os recursos de uma máquina ou de uma rede indisponíveis para os utilizadores a que são destinadas, temporária ou indefinidamente interrompendo os serviços de um hospedeiro (host) ligado à *Internet*. Isto é normalmente conseguido enchendo a máquina ou rede com solicitações desnecessárias, numa tentativa de provocar a sobrecarga dos sistemas e prevenir alguns ou todos os pedidos reais de serem atendidos. **Nota: DDoS Attack (distributed denial-of-service attack):** O tráfico de informação que invade a vítima origina-se de diferentes fontes. Isto faz com que seja efetivamente impossível de parar o ataque simplesmente bloqueando a fonte única.

Table 1: Ameaças à segurança e contramedidas (continuação).

Ataque	Descrição e contramedidas
Malware	Programa de computador destinado a infiltrar-se num sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não). Pode aparecer na forma de código executável, scripts de conteúdo ativo, ou outros softwares. *Malware* é um termo geral utilizado para se referir a uma variedade de formas de *software* hostil ou intrusivo (tais como **Cavalos de Troia, vírus** ou **worms**) Podem ser prevenidos usando *software* **anti-vírus** e mantendo-o atualizado.
Ataque de força bruta	É um ataque criptoanalítico que pode, em teoria, ser usado contra quaisquer dados criptografados (exceto para dados criptografados de uma maneira segura na teoria da informação). Pode ser usado quando não é possível tomar vantagem de outras fraquezas que tornariam a tarefa mais fácil. Consiste na verificação sistemática de todas as possíveis chaves e senhas até que as corretas sejam encontradas. No pior dos casos, isto envolveria percorrer todo o espaço de busca. *Passwords* mais longas têm mais valores possíveis, tornando-as exponencialmente mais difíceis de serem decifradas que as mais pequenas.
Ataque de temporização (*Timing attack*)	O atacante tenta comprometer um sistema criptográfico analisando o tempo gasto para executar determinados algoritmos. Toda a operação lógica leva um tempo computacional para ser executada e este tempo pode variar em relação à entrada fornecida; utilizando medições precisas do tempo gasto em cada operação pode-se tirar vantagens, inferindo determinadas informações. A quantidade de informações que pode ser exposta depende de diversas variáveis: o sistema criptográfico utilizado, o tempo de execução do CPU, os algoritmos utilizados, detalhes de implementação, medidas contra ataques de temporização, a exatidão da medida de tempo, etc.

Table 1: Ameaças à segurança e contramedidas (continuação).

3 *Privacy Framework*

Uma *Framework* é construída para, de uma forma hipotética, vermos se e como as *Smart Cities* e a enorme quantidade de dados urbanos têm cuidados de preocupação pela privacidade entre as pessoas destas cidades. A *Framework* é construída baseada em 2 dimensões recorrentes, na pesquisa sobre as preocupações das pessoas com a privacidade: uma representa o que as pessoas percebem de dados pessoais, a outra representa a divergência da preocupação das pessoas, relacionada com a finalidade para o qual os dados são colectados, sendo o contraste entre os objetivos de serviço e de vigilância os mais importantes. Essas duas dimensões produzem uma estrutura 2x2 que propõe quais as tecnologias e aplicativos de dados em *Smart Cities*, provavelmente suscitarão preocupações com a privacidade das pessoas

A duas primeiras dimensões que as pessoas se preocupam em relação à privacidade, tirando o tipo de dados e o propósito destes, pode ser representado num 2+2 esquema que identifica 4 tipos de possíveis ideias que a população pode ter acerca do conteúdo das *Smart Cities*.

O resultado é demonstrado no gráfico e na tabela seguintes.

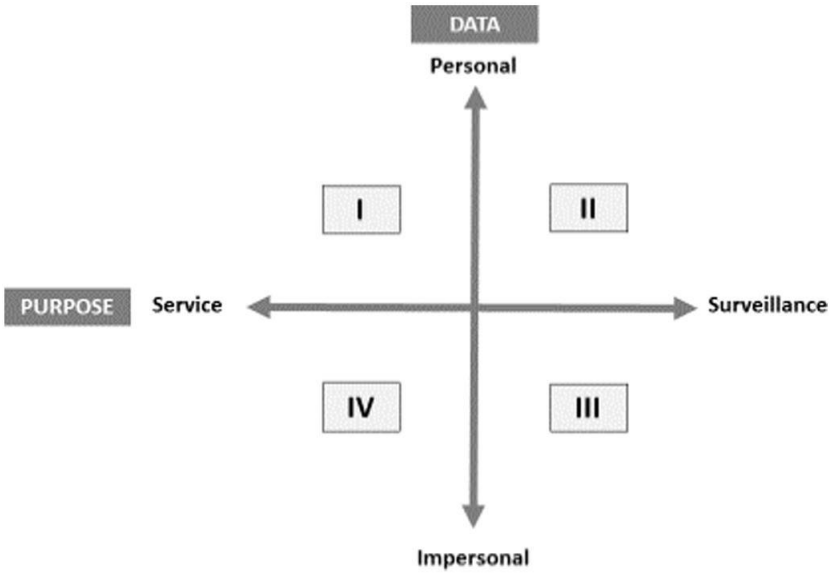

Imagem 5: Desafios à privacidade
Fonte: *https://www.sciencedirect.com/science*

Setor	Domínio	Tipo de Dados	Exemplo de aplicações
Infraestruturas	Transporte e gerência de ativos	Monitorizar dados, registar dados	Padrões de tráfego e congestionamento, painéis em tempo real
Saúde	Saúde, qualidade de vida, bem-estar, esperança de vida	Dados de saúde, dados de pesquisa, registo de vida	Localização de níveis de ruído específicos e problemas sociais de saúde em bairros específicos
Comércio	Oportunidades de negócios, marketing, serviços baseados em localização	Dados abertos do governo	Mapas de investimento para atrair novos negócios

Table 2: Smart Cities por setores.

4 Conclusão

Smart City é um conceito que está cada vez mais a tornar-se realidade. Porém, com este novo conceito vêm vários desafios, principalmente no que diz respeito à segurança e à privacidade de cada indivíduo.

Com este ensaio concluímos, então, que construir uma *Smart City* completamente segura e que respeite a privacidade de cada um é um desafio difícil de superar, mas se aplicarmos as devidas políticas e agirmos com precaução, irá melhorar as vidas de cada habitante que nela poderá viver.

5 Referências

5.1 Artigos

1. ***Smart Cities: A Survey on Data Management, Security and Enabling Technologies***
   Ammar Gharaibeh, Member, Mohammad A. Salahuddin, Sayed J. Hussini, Abdallah Khreishah, Issa Khalil, Mohsen Guizani e Ala Al-Fuqaha

2. ***Applications of big data to smart cities*** (https://jisajournal.springeropen.com)
   Eiman Al Nuaimi, Hind Al Neyadi, Nader Mohamed Jameela Al-Jaroodi

3. ***Privacy concerns in smart cities*** (https://www.sciencedirect.com/science/article/pii/S0740624X16300818)
   J. Ramon Gil-Garcia, Jing Zhang, Gabriel Puron-Cid

4. Detecção em tempo-real de ataques de neação de serviço na rede de origem usando um classificador bayesiano simples (https://sites.google.com/site/rcorcs/technical-reports/undergraduatedegreedissertationmajorpaperportuguese)
   Rodrigo Rocha

5.2 *Webgrafia*

- https://www.techopedia.com
- https://www.geeksforgeeks.org
- https://www.csoonline.com
- https://www.nytimes.com
- https://www.consumidor.ftc.gov