Instituto Politécnico de Setúbal

Escola Superior de Ciências Empresariais

Internet das coisas: O desafio da privacidade

Estudo de caso

Pedro Miguel Pereira Santos

Dissertação apresentada para cumprimento dos requisitos necessários à obtenção do grau de

MESTRE EM SISTEMAS DE INFORMAÇÃO ORGANIZACIONAIS

Orientadora: Professora Doutora Ana Mendes

Setúbal, 2016

[Esta página foi deixada em branco intencionalmente]

Dedicatória

Dedico este trabalho ao meu avô (*in memoriam*), que foi para mim uma referência de trabalho e ambição. Sei que está a olhar por mim e pela minha família, e por isso este trabalho é em sua homenagem.

À minha família e amigos, por compreenderem as minhas repetidas ausência, pelo apoio, amor, amizade, carinho, disponibilidade e preocupação que sempre mostraram, tanto ao longo da elaboração desta dissertação, como da própria vida em si.

A mim, pela minha persistência, resiliência e vontade de concretizar os meus sonhos e objetivos.

Por último, deixo uma frase de alguém que ao longo da minha carreira académica e profissional me inspira a ser melhor e a concretizar os meus objetivos.

"*Aqueles que são loucos o suficiente para pensar que podem mudar o mundo, são os únicos que o podem fazer.*"

Steve Jobs

Agradecimentos

Após a conclusão desta dissertação em Sistemas de Informação Organizacionais, gostaria de agradecer a um conjunto de pessoas, pelo que me deram ao longo desta grande mas bonita jornada.

Aos docentes, em especial à Professora Ana Mendes, por toda a disponibilidade, apoio e sugestões, que me permitiram elaborar uma melhor e mais organizada dissertação, bem como pela sua disponibilidade em ajudar a clarificar todas as dúvidas que surgiram durante o trabalho. O meu obrigado não é apenas pela orientação desta dissertação, mas sim por todo o apoio, aprendizagem e conhecimentos dispendidos ao longo do Mestrado e da Licenciatura, o que me levou a sugerir a Professora como minha orientadora. O meu muito obrigado por tudo.

Aos meus colegas de Mestrado, pelo apoio, confraternidade, disponibilidade e partilha de informação e conhecimentos costantes durante a elaboração da dissertação e de todo o Mestrado.

Às organizações que demonstraram interesse e disponibilidade em responder às minhas dúvidas e questionários, entre as quais o SAS, Microsoft, IBM, Cisco e Oracle.

Um eterno obrigado a todos por esta linda caminhada.

Resumo

A Internet das Coisas (IoC), ou *Internet of Things* (IoT), em inglês, é o termo utilizado para *design*ar a conectividade entre vários tipos de objetos do dia-a-dia sensíveis à internet, desde eletrodomésticos, carros, roupas, sapatos, remédios, etc., com sensores capazes de captar aspetos do mundo real e enviá-los a plataformas que recebem estas informações e as utilizam de forma inteligente, moldando uma rede de objetos interligados. Conceptualmente é a possibilidade de conectar o mundo físico com o mundo digital através da internet. Assim, será possível registar dados ligados às nossas ações de maneira mais assertiva e usar essas informações a nosso favor, de forma a integrar processos, serviços e aplicações.

O avanço deste advento traz consigo importantes vulnerabilidades sociais e materiais. O ciberespaço expõe os seus utilizadores a novas situações de risco e a outras que, embora já existam no mundo físico, potenciam-se no mundo virtual, fruto da maior exposição e alcance que as tecnologias proporcionam. Por isso, sem fortes alicerces de segurança, os ataques e falhas na IoT irão superar qualquer um dos seus benefícios.

Esta dissertação tem como objetivo auscultar e entender a maneira como algumas organizações fornecedoras, consultoras, e utilizadores finais da IoT estão a abordar o desafio da privacidade e segurança dos dados. Para a sua elaboração foi feita uma investigação da literatura referente ao novo paradigma da IoT, bem como um conjunto de reuniões e disponibilização de questionários a organizações envolvidas nesta temática. Foi também utilizado o *software* SAS Contextual Analysis de modo a encontrar padrões e relações sobre o posicionamento do mercado global, em específico das organizações fornecedoras de produtos para a IoT, através da documentação por si disponibilizada. Estas análises e questionários procuram não só entender a forma como, através de uma amostra de empresas e dados, os fornecedores de IoT se estão a posicionar para dar resposta às necessidades de privacidade de dados nos seus produtos, mas também fazer uma comparação dessas análises com a análise de analistas e consultoras de TI a esses mesmos produtos. Tal como constatado na dissertação, de uma maneira geral os consumidores conseguem pesar os custos da perda de privacidade em contrapartida dos benefícios das novas funcionalidades e outras vantagens a estas associadas. No entanto, será essencial que os fabricantes mantenham a confiança dos consumidores, fazendo depender a sua privacidade e segurança o mínimo possível da sua iniciativa, apostando num desenho e conceção dos produtos que integre esta preocupação.

A estratégia metodológica utilizada para a elaboração desta dissertação foi a estratégia mista, pois as análises efetuadas envolvem a interpretação, mas também apresentam uma tendência para a quantificação. Esta metodologia preocupa-se principalmente tanto com o sentido e entendimento, como também pela mensuração. O método utilizado foi o Estudo de Caso, visto que, para Yin (1990), o estudo de caso é considerado uma estratégia em que podem ser utilizados dados qualitativos ou quantitativos (trabalho de campo, arquivos, relatórios, entrevistas, observações, etc.), e é especialmente adequada quando procuramos compreender, explorar ou descrever acontecimentos e contextos complexos, nos quais estão simultaneamente envolvidos diversos factores.

Palavras-Chave: Internet das Coisas, Informação, Privacidade, Segurança, Internet, Sensores

Abstract

The Internet of Things (IoC), or Internet of Things (IoT), in English, is the term used to describe the connectivity between various types of objects of day-to-day sensitive to the internet, from home appliances, cars, clothes, shoes, medicines, etc., with sensors capable of capturing real-world aspects and send them to platforms that receive this information and use them intelligently, shaping a network of interconnected objects. Conceptually is the ability to connect the physical world with the digital world through the internet. Thus, you can record data linked to our actions more assertively and use this information to our advantage, to integrate processes, services and applications.

The advancement of this advent brings important social vulnerabilities and materials. Cyberspace exposes its users to new situations of risk and others that, although there are in the physical world, potentiate in the virtual world, the greater exposure and reach fruit that technologies provide. So without strong security foundation, attacks and failures in IoT will surpass any of its benefits.

This thesis aims to listen and understand the way some provider organizations, consultants, and end users of IoT are addressing the challenge of privacy and data security. For its preparation was made a research of the literature on the new paradigm of IoT, as well as a series of meetings and providing questionnaires to organizations involved in this issue. It also used the Contextual Analysis SAS software to find patterns and relationships for the global market positioning, in particular the organizations supplying products to the IOT through the documentation provided by itself. These tests and questionnaires seek not only to understand how, through a sample of companies and data, IoT providers are positioning themselves to meet the data privacy requirements in its products, but also make a comparison of these analyzes analysis of IT analysts and consultants to the same goods. As noted in the dissertation of general consumers can weigh the cost of loss of privacy in return for the benefits of the new features and other advantages associated with these. However, it is essential that manufacturers maintain consumer confidence, by linking your privacy and security as little as possible of its initiative, focusing on a design and design of products incorporating this concern.

The methodological strategy used for the preparation of this work was the mixed strategy, because the analyzes involve the interpretation, but also have a tendency to quantify. This methodology is mainly concerned with both the meaning and understanding, as well as the measurement. The method used was the case study, as to Yin (1990), the case study is considered a strategy that can be used qualitative or quantitative data (field work, files, reports, interviews, observations, etc.), and it is especially appropriate when trying to understand, explore or describe events and complex contexts in which are simultaneously involved several factors.

Keywords: Internet of Things, Information, Privacy, Security, Internet, Sensors

Índice Geral

Índice Figuras

Índice Tabelas

Índice Gráficos

Lista de Siglas e Acrónimos

ADN	*Ácido desoxirribonucleico*
AoT	*Analytics of Things*
CE	*Comissão Europeia*
EC	*European Comission*
EUA	*Estados Unidos da América*
FTC	*Federal Trade Comission*
IEEE	*Institute of Electrical and Electronics Engineers*
IIC	*Industrial Internet Consortium*
IoT	*Internet of Things*
NLP	*Natural Language Processing*
OIC	*Open Interconnect Consortium*
PP	*Política de privacidade*
RFID	*Radio Frequency Identification*
SCA	*SAS Contextual Analysis*
TI	*Tecnologias de Informação*
WLAN	*Wireless Local Area Network*

1. Introdução

Para a DEV Tecnologia (2014), a IoT é um paradigma emergente que integra as “coisas” do mundo real no mundo tecnológico. É um conceito no qual os dispositivos e objetos do nosso dia-a-dia são equipados com sensores capazes de comunicar entre si de forma inteligente. Uma “coisa”, no contexto da IoT, é um objeto conectado que pode ser, por exemplo, uma pessoa com um monitor cardíaco, um tanque industrial com sensores de nível, um carro com sensores que avisam a pressão dos pneus, uma lâmpada de iluminação pública de uma cidade, uma tomada em casa, ou qualquer outro objeto natural ou construído pelo homem.

Segundo a Gartner (2015), 6,4 biliões de “coisas” conectadas estarão em utilização até 2016, o que significa 30% a mais que em 2015, sendo que o gasto com a IoT chegará U$235 biliões em 2016, cerca de 22% a mais que em 2015. Até 2020, serão 20,8 biliões de objetos em uso. Serão muitas as empresas fornecedoras deste *software* e *hardware* na IoT e os consumidores finais serão os maiores detentores desse tipo de tecnologia.

São muitas as vantagens e oportunidades que a IoT pode oferecer, no entanto, existe um ponto que ainda gera muitas dúvidas e preocupa tanto fornecedores, quanto consumidores: como irá ser garantida a segurança e privacidade dos dados.

Num relatório publicado pela HP (2014), 70% dos dispositivos IoT apresentam graves falhas de segurança e estão bastante suscetíveis a ataques não autorizados. Cerca de 80% dos dispositivos levantou questões ao nível da privacidade. Esta grande percentagem deve-se ao facto dos dispositivos recolherem algum tipo de informações pessoais, como o nome, morada, data de nascimento, informações de saúde e até mesmo números de cartão de crédito, sendo ainda mais preocupante por esses dispositivos estarem assentes em aplicações móveis ou em serviços *cloud*. O estudo (figura 1) analisou os dez tipos de dispositivos IoT mais comuns, incluindo televisores, *webcams*, alarmes residenciais, termostátos domésticos, entre outros, todos ligados a algum tipo de *cloud computing*, bem como a aplicações *mobile* que permitem o seu controlo remoto. Foram encontradas em média 25 vulnerabilidades em cada dispositivo, totalizando 250 vulnerabilidades. No conjunto total encontram-se falhas ao nível da privacidade, falta de encriptação de transporte de informação, *interface Web* insegura, autorização insuficiente, mecanismos de autorização de *firmware* inseguros e proteção de *software* inadequada.

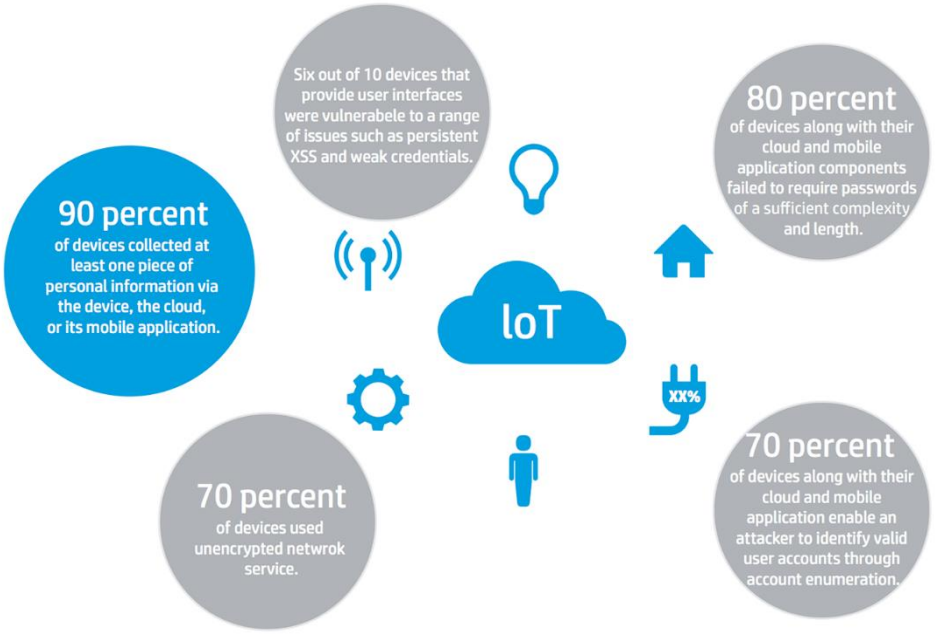

Figura 1. Resultados do estudo da HP sobre IoT
Fonte: HP (2014)

Posto isto, as organizações fornecedoras de IoT precisam de melhorar substancialmente as suas políticas e barreiras de segurança, de modo a que os consumidores sintam que os seus dados pessoais estão seguros, e que apenas tiram benefícios do uso da IoT.

Para Alecrim (2016), a indústria da IoT precisa, de definir e seguir critérios que garantam a disponibilidade dos serviços (incluindo a rápida recuperação em casos de falhas ou ataques), proteção de comunicações (que, nas aplicações corporativas, deve incluir protocolos rígidos e processos de auditoria), definição de normas para privacidade e confidencialidade de dados (ninguém pode ter acesso a dados sem a devida autorização), integridade (assegurar que os dados não serão indevidamente modificados), entre outros. Considerar todos esses aspectos está longe de ser uma tarefa trivial. Além dos desafios tecnológicos em si, a indústria precisa de tratar cada ponto levando em conta convenções globais e a legislação de cada país. Vários segmentos do mercado já lidam com tais questões, mas esse é um trabalho em constante desenvolvimento.

Diante desta realidade, a HP decidiu criar o projeto OWASP (2016) (*Open Web Application Security Project*), uma entidade sem fins lucrativos e de reconhecimento internacional, que contribui para a melhoria da segurança de *softwares* de dispositivos IoT, reunindo informações importantes que permitem avaliar riscos de segurança e combater formas de ataques através da internet.

1.1. Enquadramento

A preocupação com a segurança e privacidade é um argumento que foi, é, e sempre será válido em qualquer sociedade, área ou tecnologia. Na IoT passa-se exatamento o mesmo. Esta é vista como o futuro que irá transformar as nossas interações com os objetos e com a nossa própria vida. Onde uma grande rede de objetos conectados irá atuar de forma inteligente. Porém, com esta grande rede de dispositivos conectados e o enorme fluxo de dados que irá gerar, a segurança e privacidade dos dados na IoT vai ser um desafio fundamental.

De acordo um estudo da Gartner (2015), a preocupação com a segurança e privacidade são os maiores obstáculos à adoção da IoT. O mesmo estudo aponta, que em 2020, 60% dos orçamentos das empresas para cybersegurança serão alocados a rápidas e eficientes abordagens de deteção e resposta. Prevê ainda que, no mesmo ano, pelo menos uma organização fornecedora de produtos IoT será responsabilizada pelo seu Governo nacional por vulnerabilidades ao nível da cybersegurança dos seus produtos. Isso expõe a vulnerabilidade do sistema e a importância da segurança na IoT.

Apesar da IoT ser uma das grandes *buzzwords* do atual mercado tecnológico, 87% dos consumidores não fazem ideia do que esse termo significa, de acordo com um estudo da Altimeter (2015) sobre a utilização da IoT. No entanto, os consumidores sabem que as organizações estão a criar cada vez mais disponitivos conectados entre si, e que esses dispositivos oferecem uma grande e inquietante janela sobre os dados e informações pessoais.

De acordo com o estudo da Altimeter (2015), os consumidores estão famialirizados com as implicações dos dados dos dispositivos de controlo de *fitness* pessoal, carros conectados, ou electrodomésticos conectados. Em média (48%), um consumidor não está confortável com a ideia de partilhar os seus dados pessoais com as organizações fornecedoras de dispositivos IoT, e menos ainda lhe agrada a ideia de essas organizações venderem esses mesmos dados pessoais a outras empresas (58%).

Proteger a privacidade do consumidor torna-se cada vez mais difícil, à medida que a IoT torna-se mais prevalente. Cada vez mais dispositivos estão conectados, e este aumento da conectividade e de partilha de informação resulta numa menor capacidade de controlo, tanto de dados, como dos próprios dispositivos.

Neste cenário, a satisfação dos requisitos de segurança e privacidade desempenha um papel fundamental. Tais exigências incluem a confidencialidade dos dados e autenticação, controlo de acessos dentro da rede IoT, privacidade e confiança entre os utilizadores e as “coisas”, bem como a aplicação das políticas de segurança e privacidade. Além disso, o elevado número de dispositivos interligados potencia problemas de escalabilidade. Posto isto, é necessária uma infra-estrutura flexível, capaz de lidar com as ameaças de segurança num ambiente tão dinâmico. Esta dissertação tem como objetivo dar a entender a forma como as organizações e consumidores da IoT estão a abordar o desafio da privacidade e segurança dos dados. O objetivo é dar uma perspetiva empírica sobre esta temática, tanto da abordagem de organizações fornecedoras de produtos IoT, de consultoras na área das tecnologias de informação, bem como dos utilizadores finais destes mesmos produtos.

1.2. Formulação do Problema

A IoT é um futuro cada vez mais presente. Como consequência da conexão entre dispositivos, a IoT pode tornar a vida das pessoas mais confortável e racional. No entanto, apesar de todos os benefícios que a IoT pode trazer, esta demonstra ainda uma grande preocupação por parte dos seus utilizadores: Como irá ser garantida a segurança e privacidade dos dados? Este é provavelmente o desafio mais difícil da IoT.

De repente, tudo desde frigoríficos a portas está conectado, e enquanto estes dispositivos tornam a vida mais fácil e uma gestão de tempo por parte das pessoas muito mais eficaz, eles criam também novos vetores de ataques para *hackers*. Os aparelhos do dia-a-dia e a conexão entre eles irá tornar-se ainda mais comum do que os *Smartphones* o são nos dias de hoje, e terão acesso a dados pessoais bastante sensíveis, como cartões de crédito ou números de identificação pessoais. À medida que o nº de dispositivos IoT aumenta, também as preocupações com a privacidade e segurança dos dados aumenta proporcionalmente.

De acordo com uma pesquisa da Symantec (2015), 20% das aplicações móveis utilizadas para controlar os dispositivos IoT não possuem encriptação de dados. Além disso, nenhuma das aplicações que foram alvo de análise, possui autenticação mútua entre o cliente e o servidor, o que traz grandes riscos ao utilizador.

O relatório da Symantec (2015) fez um teste em 15 *interface*s. Dessas, 10 mostraram vulnerabilidades que poderiam, entre outras situações, permitir que um invasor desbloqueasse remotamente a casa do utilizador. Para a Symantec, os *hackers* que conseguirem acesso à rede residencial, invadindo por exemplo, uma conexão *wi-fi* com fraca criptografia, têm mais vetores de ataque à disposição.

Para Hernández (2015), muitas outras graves situações podem ocorrer devido à falta de privacidade e segurança que a IoT apresenta. Um exemplo da necessidade de segurança e privacidades dos dados na IoT acontece nas *Smart homes*, ou casas inteligentes: Uma rede de sensores de luzes domésticas, se for lida por *hackers* pode informar alguns aspetos pessoais da vida das pessoas que vivem naquela casa. Informações como com que frequência um quarto é ocupado, os horários em que há gente em casa e quando a casa está vazia. Os sensores de temperatura podem criar um idêntico mapeamento da vida pessoal ao informar o horário em que uma pessoa costuma tomar banho. A própria natureza destes dispositivos torna-os vulneráveis.

Hernandéz (2015) afirma ainda que os dispositivos IoT não contam com os recursos de segurança dos equipamentos tradicionais de tecnologias de informação (TI) (servidores, routers, etc.). O ácido desoxirribonucleico (ADN) dos atuais dispositivos IoT está ligado a um fator crítico: é essencial garantir um custo competitivo e baixo para produtos que são, afinal, para o mercado de massa. Isto é um desafio, pois a informação gerada pela IoT é essencial para trazer melhores serviços e melhor gestão dos dispositivos.

1.3. Objetivos

Na tentativa de dar resposta à problemática relacionada com a privacidade dos dados na IoT, esta dissertação tem como objetivo geral dar a entender a forma como alguns dos fornecedores, consultoras e os consumidores da IoT estão a abordar o desafio da privacidade e segurança dos dados. Visto esta temática ser um dos maiores desafios da IoT, a sua clarificação poderá ser uma mais-valia para mercado, onde se incluem consumidores e fornecedores, dando uma perspetiva sobre a forma como este desafio é abordada por ambos.

Os objectivos específicos desta dissertação são:

- Analisar a forma como algumas das organizações fornecedoras de IoT estão a abordar os temas da privacidade e barreiras de segurança nos seus dispositivos;
- Analisar a forma como a privacidade dos dados nos produtos IoT é vista por analistas da área;
- Esclarecer junto de consultoras de TI, qual o seu entendimento e visão para com a privacidade dos dados na IoT.
- Comparar a forma de abordagem dos fornecedores em relação à privacidade dos dados nos seus produtos IoT com a visão de analistas e consultoras para esse mesmo tema.

1.4. Metodologia

Segundo Freixo (2010), a metodologia é um “conjunto de métodos e das técnicas que guiam a elaboração do processo de investigação científica”, logo o que se pretende é descrever os métodos e técnicas utilizadas no desenvolvimento desta dissertação.

No campo dos estudos organizacionais, podem-se utilizar diversas abordagens metodológicas, tanto de caráter quantitativo como qualitativo. Observe-se, entretanto, que a escolha de um ou outro tipo deve estar associada ao objetivo da pesquisa e que ambos apresentam características específicas, vantagens e desvantagens. Por outro lado, muitas vezes, pode-se fazer uso de diferentes métodos de forma combinada, recorrendo-se a mais de uma fonte para recolha de dados, aliando-se o qualitativo ao quantitativo. A metodologia/ linguagem aplicada deve ser adequada ao público a quem a mesma se destina, sendo mais acessível caso se trate de público infantil ou mais especializada caso se trate de público erudito ou conhecedor da matéria (Sousa, 1998).

A definição de metodologia para a elaboração da dissertação passou por métodos de investigação, podendo estes serem classificados de diversas maneiras, porém uma das distinções mais comum é entre as metodologias de pesquisa qualitativa e quantitativa (Myers, 1997).

1.4.1. Metodologia utilizada

Visto o tema de estudo da dissertação ser um tema complexo, envolvendo sobretudo a interpretação, mas também apresentando uma tendência para a quantificação, foi dada assim uma maior maior ênfase à metodologia mista. Esta metodologia preocupa-se principalmente tanto com o sentido e entendimento, como também pela mensuração.

De uma forma mais detalhada, trata-se de um estudo de caso, visto que, para Yin (1990) o estudo de caso é considerado uma estratégia em que podem ser utilizados dados qualitativos ou quantitativos (trabalho de campo, arquivos, relatórios, entrevistas, observações, etc.), e é especialmente adequada quando procuramos compreender, explorar ou descrever acontecimentos e contextos complexos, nos quais estão simultaneamente envolvidos diversos factores.

Thousand Oaks (2003), afirma que esta abordagem se adapta à investigação em educação, quando o investigador é confrontado com situações complexas, de tal forma que dificulta a identificação das variáveis consideradas importantes, quando o investigador procura encontrar interacções entre factores relevantes próprios dessa entidade, quando o objectivo é descrever ou analisar o fenómeno, a que se acede directamente, de uma forma profunda e global, quando o investigador pretende apreender a dinâmica do fenómeno, do programa ou do processo e quando o investigador procura respostas para o “como?” e o “porquê?”, tais como “porque é que a IoT está a ter um elevado impacto global na sociedade”, ou “como as consultoras estão a olhar para a privacidade dos dados dos dispositivos IoT?”.

A análise de estudo de caso será uma forma rigorosa de fundamentar conceitos. A utilização deste método irá permitir generalizar a teoria, o que implica o fornecimento de valiosas informações para a abordagem proposta.

Assim, esta metodologia tem como objetivo ir ao encontro dos objetivos a que esta dissertação se propõe, sendo eles:

- Analisar a forma como algumas das organizações fornecedoras de IoT estão a abordar os temas da privacidade e barreiras de segurança nos seus dispositivos;
- Analisar a forma como a privacidade dos dados nos produtos IoT é vista por analistas da área;
- Esclarecer junto de consultoras de TI, qual o seu entendimento e visão para com a privacidade dos dados na IoT.
- Comparar a forma de abordagem dos fornecedores em relação à privacidade dos dados nos seus produtos IoT com a visão de analistas e consultoras para esse mesmo tema.

1.5. Estrutura da Dissertação

A dissertação está estruturada por seis capítulos, por forma a possibilitar um melhor manuseamento/ compreensão da mesma.

O **Enquadramento Teórico** surge no Capítulo 2, o qual pretende enquadrar o

enquadramento teórico acerca da temática da IoT, onde se incluem a sua história, aplicações quotidianas, a Analítica das Coisas, exemplos de tecnologias de comunicação entre os dispositivos IoT, a descrição de alianças criadas para influenciaram as normas e *standards* na IoT, e por fim, as limitações legais e sociais da IoT, onde se incluem a segurança e proteção dos dados, privacidade dos dados e legislação.

O Capítulo 3 descreve a abordagem metodológica utilizada, em particular o método **Estudo de caso**, ou seja, todas as etapas, procedimentos e estratégias efetuadas para a elaboração da dissertação, e subsequentes atividades envolvidas. Aqui incluem-se a estratégia de investigação, a concepção do questionário, e as etapas decorridas para efetuar a análises de documentos de privacidade de dados na IoT.

As **Atividades desenvolvidas** descritas no Capítulo 4**,** descreve as atividades desenvolvidas no decorrer desta dissertação. É efetuada uma análise aos resultados obtidos pela aplicação dos questionários efetuadas a organizações envolvidas no mercado da IoT, bem como uma descrição dos resultados obtidos na análise de documentos de privacidade de dados na IoT.

As **Conclusões e Perspetivas de Trabalho Futuro** surgem no Capítulo 5, onde são apresentadas as principais conclusões da análise dos resultados obtidos assim como as perspectivas de trabalho futuro que poderão dar continuidade ao estudo realizado.

2. Enquadramento Teórico

Neste capítulo é primeiro efectuada uma breve introdução à IoT, onde irão ser descritos os principais tópicos envolvidos nesta temática. Irá ser dada ênfase à IoT, onde se incluem e a sua história e as suas aplicações na vida quotidiana, dando o exemplo específico das *Smart homes*.

Segue-se uma explicação sobre a Analítica das Coisas, e a forma como ela é a grande responsável por tirar partido das potencialidades da IoT.

O ponto seguinte faz referência aos tipos de comunicação *wireless* existentes entre os dispositivos IoT, entre os quais o *Wi-fi*, *Bluetooth*, *Zigbee*, *Zigbee*, *Thread*, RFID e NFC.

De seguida, são descritas as alianças existentes no mercado da IoT para influenciarem as normas e *standards*. Nas alianças incluem-se e *AllSeen*, a *Open Interconnect Consortium* (OIC), a *Thread Group*, a *Industrial Internet Consortium* (IIC), a IEEE P2413 e a *Apple Homekit*.

Este capítulo termina com uma abordagem às limitações legais e sociais à volta da IoT, entre as quais a segurança e proteção dos dados, a privacidade dos dados, e a legislação e regulamentação na Europa e nos EUA.

2.1. Internet das Coisas

A Internet mudou definitivamente o nosso quotidiano, permitindo o acesso rápido a informações que até então não tínhamos. Mas se a Internet "das pessoas" pode ser considerada uma verdadeira revolução, a IoT pode proporcionar-nos muito mais.

A IoT é um conceito no qual os dispositivos e objetos do nosso dia-a-dia são equipados com sensores capazes de comunicar entre si de forma inteligente. Uma “coisa”, no contexto da IoT, é um objeto conectado que pode ser, por exemplo, uma pessoa com um monitor cardíaco, um tanque industrial com sensores de nível, um carro com sensores que avisam a pressão dos pneus, uma lâmpada de iluminação pública de uma cidade, uma tomada em casa, ou qualquer outro objeto natural ou construído pelo homem.

Na sua essência, a IoT significa apenas um ambiente que reúne informações de vários dispositivos (computadores, veículos, *Smartphone*s, semáforos, etc.) e de aplicações (qualquer coisa desde uma aplicação de media social como o Twitter a uma plataforma de comércio eletrónico, de um sistema de produção a um sistema de controlo de tráfego).

De acordo com uma pesquisa de Witchalls (2013) para a Unidade de Inteligência Economista, mostra que 96% dos líderes de negócios esperam que os seus negócios estejam a fazer usufruto da IoT, de uma forma ou de outra, em 2016. Além disso, 60% dos 779 líderes de negócios globais que participaram na pesquisa concorda que empresas lentas na integração de IoT ficarão para trás dos seus diretos concorrentes.

Para a Intel (2015), as cidades gastarão US$41 trilhões nos próximos 20 anos em melhorias de infraestrutura para a IoT (algumas destas melhorias são exemplificadas na Figura 2).

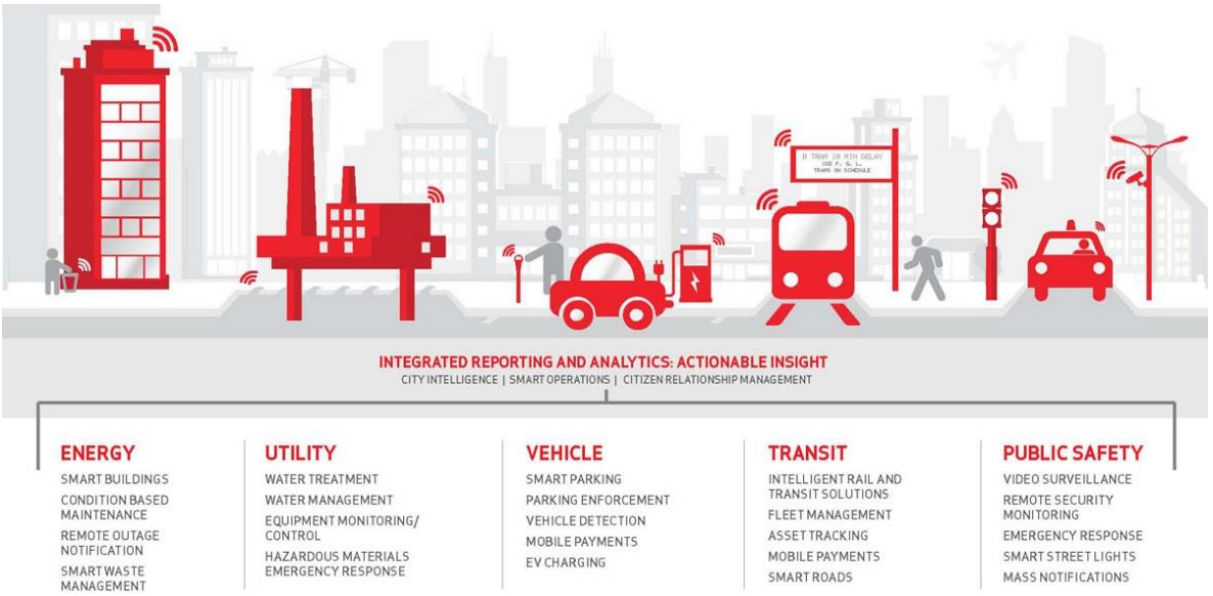

Figura 2. Cidades Inteligentes
Fonte: Verizon (2015)

Segundo a Gartner (2015), 6,4 biliões de "coisas" conectadas estarão em utilização até 2016, o que significa 30% a mais que em 2015, o gasto com a IoT chegará U$235 biliões em 2016, cerca de 22% a mais que em 2015. Até 2020, serão 20,8 biliões de objetos em uso. Serão muitas as empresas fornecedoras deste *software* e *hardware* na IoT e os consumidores finais serão os maiores detentores desse tipo de tecnologia.

A Gartner (2015) afirma também que, para além de carros conetados, a utilização por parte dos consumidores, irá continuar a ser a maior percentagem de "coisas" conectadas, ao passo que a utilização nas empresas irá obter a maior percentagem do gasto". A mesma Gartner estima que 4 biliões de coisas conectadas estarão em uso no sector consumidor em 2016, e que irão atingir os 13.5 biliões em 2020 (ver Tabela 1).

Tabela 1. *Quantidade de "coisas" conectadas por categoria (Milhões de Unidades)*

Categoria	**2014**	**2015**	**2016**	**2020**
Consumidor	2,277	3,023	4,024	13,509
Empresas: *Cross-Industry*	632	815	1,092	4,408
Empresas: *Vertical-Specific*	898	1,065	1,276	2,880
Total	**3,807**	**4,902**	**6,392**	**20,797**

Notas: Em relação às empresas, a Gartner considera duas classes de "coisas" conectadas: Cross-Industry, que são dispositivos utilizados em múltiplas indústrias, e Vertical-Specific, que são dispositivos encontrados numa indústria particular.
Fonte: Gartner (2015)

Em termos de *hardware*, a Gartner (2015) estima ainda que as aplicações para o consumidor irão rondar os $546 biliões em 2016. Em relação ao negócio, o uso de "coisas" conectadas irá atingir os $868 biliões em 2016 (Tabela 2).

Tabela 2. *Gastos com a Internet das Coisas por categoria (Biliões de Doláres)*

Categoria	**2014**	**2015**	**2016**	**2020**
Consumidor	257	416	546	1,534
Empresas: *Cross-Industry*	115	155	201	566
Empresas: *Vertical-Specific*	567	612	667	911
Total	**939**	**1,183**	**1,414**	**3,010**

Notas: Em relação às empresas, a Gartner considera duas classes de "coisas" conectadas: Cross-Industry, que são dispositivos utilizados em múltiplas indústrias, e Vertical-Specific, que são dispositivos encontrados numa indústria particular.
Fonte: Gartner (2015)

2.1.1. História da IoT

Para a Assepro (2013), o termo IoT é, de certa forma, fruto do trabalho desenvolvido pelo *MIT Auto-ID Laborator* e foi criado em 1999 por Kevin Ashton, um britânico pioneiro em tecnologia. Numa apresentação, Ashton explicou a forma como os computadores do futuro iriam estar conectados e auto-suficientes. O próprio, estava a trabalhar num projeto de otimização de cadeia de abastecimento, e queria atrair a atenção da administração da sua empresa, a Procter & Gamble, para uma nova tecnologia chamada *Radio-Frequency Identification* (RFID). Devido ao facto de a Internet ter sido a nova tendência em 1999, e porque de alguma forma faria sentido, ele deu o nome de "Internet das Coisas" IoT não cativou interesse nos 10 anos seguintes.

Segundo a IoT Analytics (2014), o conceito de IoT começou a ganhar popularidade no verão de 2010. Isto deveu-se ao facto de terem surgido informações de que o serviço *Street View* da Google não só tinha feito fotos em 360º, mas como também tinha armazenado toneladas de dados das redes *Wi-fi* das pessoas. Isso deu origem ao debate sobre se esta tinha sido o início de uma nova estratégia da Google, não só para indexar a Internet, mas para indexar todo o mundo físico. Ainda segundo a IoT Analytics (2014), no mesmo ano, o governo chinês anunciou que iria tornar a Internet das Coisa uma prioridade estratégica no seu plano a 5 anos. Em 2011, a Gartner, no seu famoso *Hype-cycle for emerging tecnologies*, uma apresentação gráfica da maturidade, *adoção* e aplicação de tecnologias específicas, incluiu uma nova tecnologia emergente, a Internet das Coisas. No seguinte, em 2012, o tema da maior conferência de Internet da Europa, a LeWeb, foi a IoT. Na mesma altura, revistas com foco em tecnologia, como a Forbes e Wired, começaram a utilizar o termo Internet das Coisas para descrever o fenómeno.

A IoT Analytics (2014), afirma ainda que o termo IoT chegou à consciência do mercado de massas, quando em Janeiro de 2014 a Google anunciou a compra da Nest por 3,2 biliões de dólares. Ao mesmo tempo, a Consumer Eletronics Show (CES), em Las Vegas, foi realizada sob o tema IoT.

2.1.2. Aplicações da IoT

A IoT transformará o modo como vivemos, trabalhamos e aprendemos. É o início de um ciclo de renovação tecnológica que auxiliará na otimização e automatização de tarefas quotidianas básicas. Além disso, poderá trazer informações importantes para o benefício público, e para empresas privadas poderem ser mais assertivas nos seus produtos e serviços prestados. A conexão virtual de dados, pessoas,

processos e coisas, promete criar um mundo de novas oportunidades económicas, entre as quais ao nível das *Smart Cities, Smart Environment, Smart Metering*, Segurança & Emergências, retalho, logística, controlo industrial, *Smart Agriculture, Smart Animal Farming*, domótica e *eHealth* (Libelium, 2015). Para Kash (2014), alguns exemplos práticos da aplicação da IoT são:

- Sistemas de estacionamento inteligente para as cidades irão fornecer visibilidade em tempo real sobre a disponibilidade de lugares de estacionamento em toda a cidade;

- O teletrabalho poderá eliminar o trajeto diário do local de trabalho, permitindo que os colaboradores trabalhem a partir de casa. Em locais remotos reduziria custos e melhoraria a produtividade para empregadores e empregados. Os impactos resultariam na redução de gastos com funcionários, manutenção e limpeza de escritório, maior retenção de funcionários, aumento de produtividade e novas oportunidades de emprego;

- Soluções de transporte inteligente aceleram fluxos de tráfego e reduzem o consumo de combustível;

- Redes elétricas inteligentes conectam de forma mais eficiente os recursos renováveis, melhoram a confiabilidade do sistema e os seus consumidores são cobrados com base na eficiência da operação;

- Através de medicina inteligente, os médicos e hospitais podem receber e organizar dados vindos de dispositivos médicos conectados, incluindo *wearables* e monitores de saúde instalados nas casas dos pacientes. Ao receber os dados em tempo real, os profissionais de medicina obtêm assim informação mais completa dos seus pacientes, melhorando o atendimento através de diagnósticos e tratamentos mais eficazes;

- Sensores de monitorização de máquinas, diagnosticam e preveem problemas pendentes de manutenção e falta de *stock*;

Um estudo da IoT Analytics (2015), mediu o que as pessoas pesquisam no Google, o que falam no Twitter, e sobre o que escrevem no Linkedin à cerca da IoT. A aplicação de IoT mais pesquisada recebeu um valor de 100%, enquanto que as restante foram avaliadas com uma percentagem que representa a sua relação à aplicação com maior percentagem. Sem margem para dúvidas, o estudo concluiu que as *Smart homes,* onde se incluem os termostátos inteligentes, luzes conectadas, frigoríficos inteligentes, e fechaduras inteligentes*,* são neste momento a aplicação de IoT mais proeminente (figura 3).

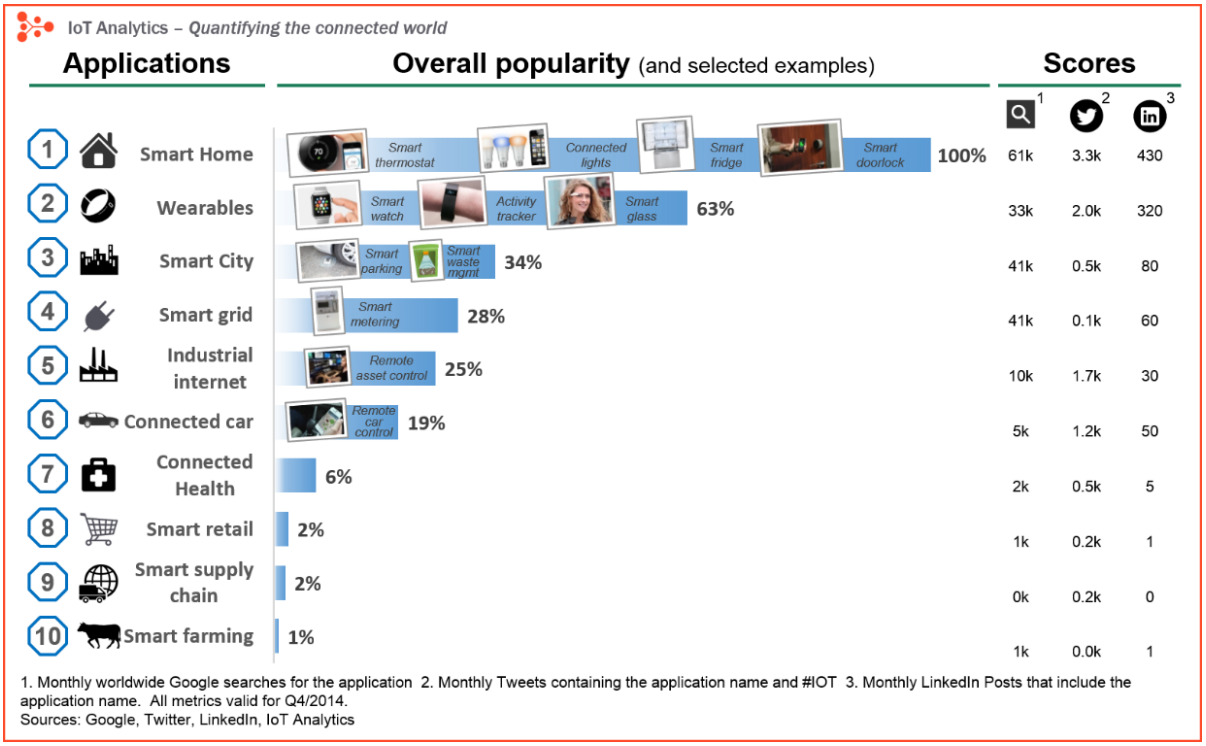

Figura 3. Estudo IoT Analytics
Fonte: IoT Analytics (2015)

De facto, segundo um estudo de Klein (2015), 68% dos americanos estão confiantes de que as *Smart homes* serão tão comuns dentro de 10 anos, como os *Smartphones o* são nos dias de hoje. O custo de possuir uma casa é a maior despesa na vida de um proprietário. Segundo este estudo, as habitações consomem a maior parte do orçamento de uma pessoa comum, chegando aos 33% das suas despesas anuais. Assim sendo, as *Smart homes* prometem economizar tempo, energia e dinheiro para os seus proprietários. Dos atuais pioneiros na utilização de *Smart homes*, 45% afirmam que conseguem poupar cerca de $1100 por ano, e 87% dizem que as suas vidas passaram a ser bastante mais facilitadas.

2.1.2.1. *Smart homes*

A Juniper Research (2014) define *Smart home* como uma casa com dispositivos inteligentes conectados entre si e projetados para oferecer ou distribuir uma série de serviços dentro e fora de casa através de uma variedade de dispositivos de rede. Embora os dispositivos não necessitem de uma ligação de alta-velocidade à Internet, para se tirar partido de todas as funcionalidades de uma *Smart home*, é necessária uma ligação à Internet de banga larga permanente.

Uma *Smart home* pode facilitar verdadeiramente a vida dos seus habitantes, podendo ter facilidades desde controlar à distância o ar condicionado, as luzes e a máquina de lavar através do *Smartphone* (figura 4). Frigorificos inteligentes podem criar inventários automáticos de todos os produtos que contem e verificar a existência de algum prazo de validade expirado, notificando desta forma o utilizador através do *Smartphone*. Uma máquina de café inteligente pode avisar quando fica sem água, ou quando necessita de uma limpeza. Termostátos inteligentes podem regular a temperatura da casa para

uma temperatura agradável mesmo antes dos seus habitantes chegarem a casa vindos de um dia de trabalho. Controlo inteligente de luzes permite agendar as horas a que determinadas luzes se acendem ou apagam, o nível de luz emitida, bem como regular a forma como as luzes reagem à deteção de movimento.

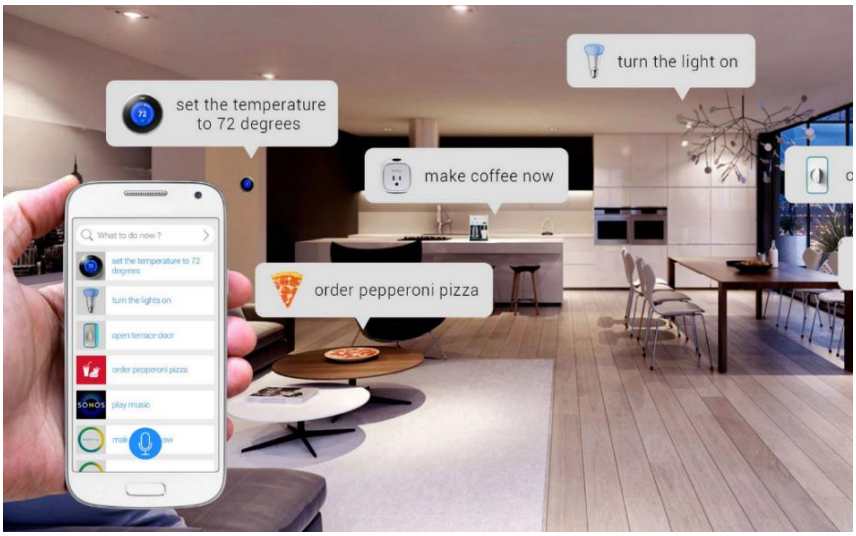

Figura 4. *Smart homes*
Fonte: Wheatley, M. (2015)

2.1.2.2. *Smart Cities*

Muitos são os conceitos dados para as Cidades Inteligentes e diversas são as características que os estudiosos entendem como necessários que tornam uma cidade "*Smart*". A *World Foundation for Smart Communities* (2012) define "uma Comunidade Inteligente é uma comunidade que faz um esforço consciente para usar a tecnologia da Informação para transformar a vida e o trabalho dentro do seu território de uma forma significativa e fundamental, em vez de seguir uma forma incremental", isto é, as cidades Inteligentes devem ser baseadas num crescimento eficiente, sóbrio e planeado por meio das TI. O tráfego e os transportes públicos podem ser muito melhor geridos com informações em tempo real sobre as condições do pavimento, congestionamentos, condições climatéricas e disponibilidade de estacionamento a serem recolhidas a partir de múltiplos sensores. Da mesma forma, a iluminação pode ser muito mais responsiva às necessidades dos habitantes das cidades, e os níveis de poluição ambiental e sonora podem ser melhor monitorizados e comunicados. Em *Smart Cities* (figura 5), há uma interação de dados de diferentes fontes em diferentes camadas. Ou seja, os dados gerados por dispositivos pessoais conectam-se a informação gerada pelos sensores de uma cidade inteligente, recebendo dados sobre, por exemplo, horários de transportes públicos, ou estradas com menor tráfego automóvel.

Figura 5. *Smart* City
Fonte: IoT Philipphines. (2015)

2.1.2.3. *Wearables* e *Portables*

Alguns dos *icons* atuais da IoT são os *wearables* e os *portables*, onde se incluem as pulseiras, óculos ou relógios inteligentes (figura 6). Podem acompanhar e registar a atividade física, como o exercício, comer, dormir, ou outras atividades, como a leitura, etc. Os *wearables* têm sido altamente utilizados como uma tecnologia inovadora na área da saúde, pela sua capacidade em registar continuamente as estatísticas vitais e observações em tempo real como a pressão arterial remotamente. Eles podem monitorizar as condições de um paciente e notificar familiares, prestadores de cuidados médicos ou serviços de emergência conectados ao sistema de incidentes de riscos potenciais, como quedas, mudanças de dieta, ou mudanças de temperatura.

Figura 6*.* Wearables (*Smart* Watch, *Smart* Glasses, Fitness Tracker)
Fonte: Harris, R. (2015)

2.1.3. Analitica das Coisas

Com o advento da IoT, todo o tipo de “coisas” – desde termostátos, carros, até roupa – consegue comunicar entre si e gerar dados, informação e ações que prometem transformar uma grande variedade de produtos e serviços.

De forma a capitalizar esta era, é crucial perceber a Analítica das Coisas, ou *Analytics of Things* (AoT), em inglês, e como juntar *Machine Intelligence* e *Human-decision-making*. O termo *AoT* aponta assim que os dispositivos de IoT geram um grande volume de dados, e que esses mesmos dados precisam de ser analizados para se tornarem úteis (figura 7).

IoT e *Big Data* são basicamente dois lados da mesma moeda. Gerir e extrair valor dos dados provenientes da IoT é o maior desafio que as empresas enfrentam. As organizações devem estabelecer uma adequada plataforma de análise/infraestrutura para analisar os dados provenientes dos sensores. Há que ter em conta também, que nem todos os dados são relevantes.

Um dispositivo de IoT gera fluxos contínuos de dados numa forma escalável, por isso as organizações devem saber lidar com esses fluxos e excetuar ações sobre eles. Essas ações podem ser, por exemplo, correlação de eventos, cálculos de métricas, estatísticas e previsões descritivas.

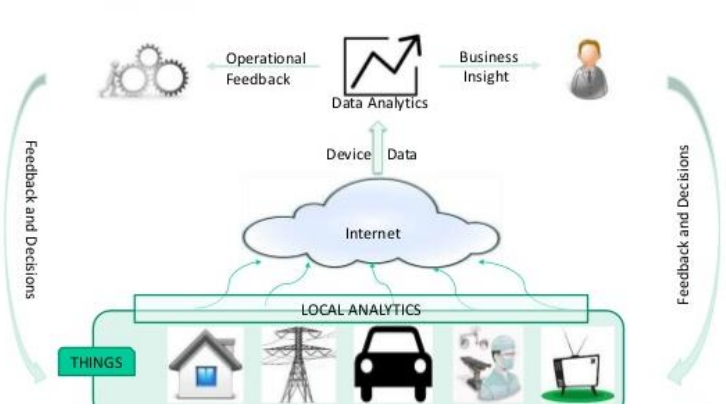

Figura 7. Arquitetura da *AoT*
Fonte: Awasthi, G. (2015)

2.1.3.1. Valor e propósito da Analítica das Coisas

A analítica e análise da IoT surge para um vasto conjunto de propósitos. A virtude primária da analítica em dispositivos conectados é a possibilidade de agregar dados de vários dispositivos e fazer comparações temporais, levando a uma melhor tomada de decisão por parte dos utilizadores.

A comparação no uso de um recurso tão importante como a energia, é, por exemplo, uma abordagem analítica chave para dados conectados. Para Davenport (2015), a AoT pode ser utilizada para vários propósitos, entre os quais:

- **Analítica descritiva -** recolher introspeções sobre o desempenho passado e olha para as razões do sucesso ou fracasso, de modo a desenvolver modelos estatísticos que expliquem as variações;

- **Deteção de anomalias –** identificar situações fora do normal, tal como temperatura demasiado alta, ou uma imagem de uma pessoa numa área que deverá estar desabitada;

- **Analítica preditiva –** utilizar analítica preditiva para detetar possíveis problemas em dispositivos, antes mesmo de estes ocorrerem;

- **Otimização –** utilizar dados e análises de sensores para otimizar um processo;

- **Analítica prescritiva –** utilizar sensores e outros tipos de dados para dizer aos trabalhadores o que fazer, como por exemplo, a utilização de sensores de temperatura e solo para plantação prescritiva por parte dos agricultores.

- **Consciência situacional –** Juntar eventos aparentemente desconectados, de modo a formar uma explicação lógica, como quando uma série de leituras de temperatura do óleo de um carro, combinada com a queda de eficiência do combustível, indicam que uma mudança de óleo poderá ser eventualmente necessária.

2.2. Comunicação entre os dispositivos IoT

A IoT englobará todos os aspectos de nossa vida quotidiana, pois ela literalmente possibilita que biliões de coisas fiquem conectadas a qualquer momento, em qualquer lugar, a qualquer coisa ou pessoa. As suas aplicações são muitas, tais como casas inteligentes, carros conectados, sistemas de energia, agricultura, transportes, saúde, etc. Uma única tecnologia não consegue efetivamente atender a todas as necessidades das inúmeras aplicações da IoT. Portanto, embora alguns objetos utilizem conexões cabladas como a *Ethernet*, as tecnologias de comunicação Wireless desempenham um papel crucial para possibilitar a conectividade da IoT. Uma rede de comunicação IoT ideal será uma mistura entre os 2 tipos, cabeada e *Wireless* (Strickland, 2014).

Além das tecnologias emergentes, tais como o Zigbee, Z-Wave. *Thread*, RFID e NFC, muitas das tecnologias de comunicação *Wireless* são bem conhecidas por parte do público em geral, tais como o *Wi-fi* e *Bluetooth*. Dependendo da aplicação, a escolha da tecnologia a utilizar vai depender de fatores como o alcance, requisitos de dados, exigências de segurança, potência de vida da bateria, etc.

2.2.1. *Wi-fi*

Figura 8. *Wi-fi*
Fonte: Malik, A. (2014)

A rede *Wi-fi (*figura 8*)* é uma rede local sem fios (*WLAN*) que transmite via ondas de rádio padronizadas segundo a norma IEEE 802.11[1], através de um alcance máximo de 50metros e uma velocidade de conexão de 2,4GHz ou 5GHz de ultra-frequência. Esta tecnologia é ótima para efetuar transferências de grandes quantidades de dados entre os dispositivos. No entanto, esta requer uma grande quantidade de energia para operar, ao passo que muitos dispositivos IoT requerem uma taxa de transferência de dados muito menor do que a usada pelo *Wi-fi*. Isto significa que as baterias dos dispositivos têm de ser mudadas numa base regular.

2.2.2. *Bluetooth*

Introduzido pela Ericsson na década de 1990, a tecnologia *Bluetooth* é um pilar da comunicação de curto alcance. Transmite dados numa frequência de banda entre os 2,4 e os 2,485GHz. Opera em distâncias menores do que o *Wi-fi* e requer menos energia para operar. O novo *Bluetooth* v4.0, ou *Smart Bluetooth* (figura 9), é um protocolo importante para a IoT, visto oferecer uma range de alcance similiar ao *Bluetooth*, mas projetado para um consumo de energia significativamente reduzido. No entanto, o *Smart Bluetooth* não é realmente concebido para transferência de arquivos e é mais adequado para pequenos blocos de dados.

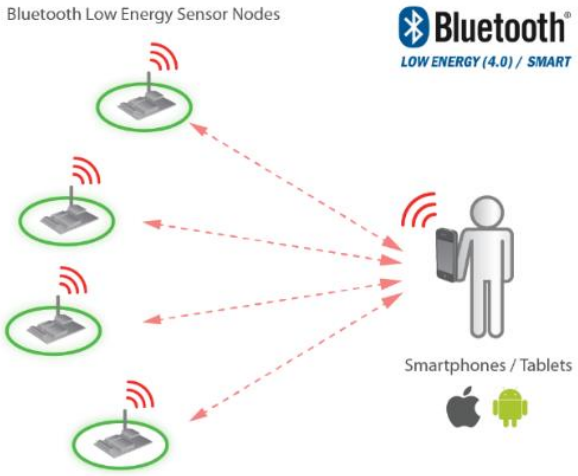

Figura 9. *Bluetooth*
Fonte: Libelium (2014)

[1] O padrão 802.11 foi desenvolvido pelo IEEE (Institute of Electrical and Electronics Engineers) para redes locais sem fio (WLANs). O propósito desta norma é desenvolver um padrão para prover um "Medium Access Control" (MAC) e uma Camada Física específica para conexões sem fio com estações de trabalho fixas ou móveis dentro de uma rede local. Este padrão define os tipos de protocolos necessários para que haja uma interoperabilidade entre equipamentos para rede sem fio de fabricantes diferentes.

2.2.3. Zigbee

A tecnologia *Zigbee* permite a dispostivos de baixa potência de operação, baixa taxa de transmissão de dados e baixo custo de implementação enviarem dados na rede, com cada dispositivo capaz de retransmitir os dados em direção ao seu destino pretendido (figura 10). Resumidamente, é um chip que, por ser mais barato e gastar menos energia, tem vindo a ganhar adeptos no mercado. Para Strickland (2014), a única desvantagem é o facto de o *standard Zigbee* existir em vários formatos, não sendo por isso um verdadeiro *standard*.

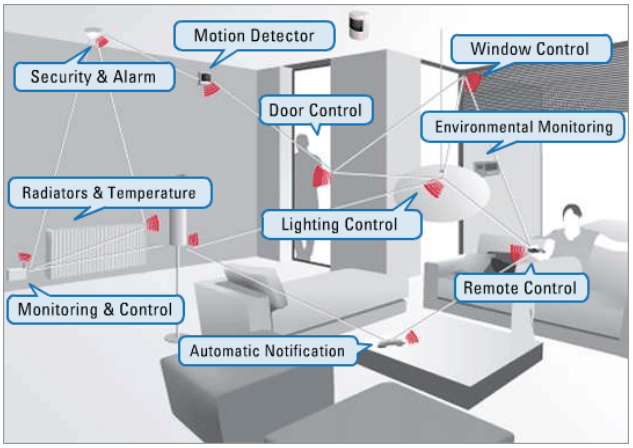

Figura 10 *Zigbee*
Fonte: Biswas, S. (2011)

2.2.4. *Z-Wave*

É uma tecnologia de baixo consumo, primariamente projetada para automação de residências, ou seja, para produtos como controladores de lâmpadas e sensores, entre outros (figura 11). Otimizada para comunicação confiável e de baixa latência de pequenos pacotes de dados, com taxas de transferência entre os 100kbit/s, opera na faixa de sub-1GHz, não interferindo na largura de banda 2,4GHz, como o *Bluetooth* ou o *Z-Wave*. O *Z-Wave* utiliza um protocolo mais simples do que as outras tecnologias, que podem permitir um desenvolvimento mais rápido e simples, no entanto a única fabricante destes *chips* é a Sigma *Design*s, sendo uma desvantagem para as outras tecnologias *wireless* que apresentam múltiplos fabricantes (RS, 2015).

Figura 11. *Z-Wave*
Fonte: Z-Wave Alliance (2014)

2.2.5. *Thread*

O *Thread* visa solucionar as necessidades da IoT. Com base nas especificações atuais, o *Thread* é capaz de suportar uma rede de até 250 dispositivos. Cada casa pode ter a sua própria rede, ou seja, uma rede pode ter até 250 aparelhos que interagem com os seus habitantes numa base diária. Tal como acontece no *Zigbee*, tem uma topologia mesh, ou seja, todos esses dispositivos são capaz de retransmitir dados. Esta tecnologia procura evitar o problema de vários *standards* como acontece com o *Zigbee*, exigindo um programa de certificação para todos os que desejem incorporar esta tecnologia nos seus produtos, não permitindo a variação de *standards*.

Segundo Strickland (2014), se a *Thread* comprovar a sua utilidade, será uma plataforma sólida para a IoT. Mas para isso, os executivos da *Thread* vão necessitar de convencer tanto os utilizadores, como os fabricantes, de que irão resolver um problema, e não apenas adicionar o seu nome à lista de tecnologias em alternativa.

2.2.6. RFID

A tecnologia de RFID (*radio frequency identification* – identificação por radiofrequência) é o termo dado às tecnologias que utilizam a frequência de rádio para captura de dados. Para isso existem diversos métodos de identificação, sendo que o mais utilizado é armazenar um número de série que identifique uma informação, num *microchip*. Tal tecnologia permite a captura automática de dados, para identificação de objetos com dispositivos eletrónicos, conhecidos como etiquetas eletrónicas, *tags* ou RF *tags*, que emitem sinais de radiofrequência para leitores que recolhem estas informações (figura 12). Esta tecnologia existe desde a década de 40 e complementa a tecnologia do código de barras, já ela bastante difundida. Segundo a RFID Center of Excellence (2013), esta tecnologia pode ter várias aplicações: segurança e controlo de acessos, controlo de tráfego de veículos, identificação pessoal, rastreio animal, identificação de objetos, etc.

Figura 12. Sistema RFID
Fonte: Amplio (2014)

As suas áreas de aplicação são igualmente as mais variadas: setor público (controlo de passaportes, identificação de ativos em bibliotecas (figura 13), farmacêutico (autenticidade de produtos), automotivo (imobilizador eletrónico de motor), aéreo (identificação e movimentação de bagagens em aeroportos), médico-hospitalar (identificação de pacientes, controlo da administração de medicamentos).

Figura 13. Sistema RFID em Livrarias
Fonte: Booktec (2014)

Barbin,M. (2015) afirma que a RFID uma das mais promissoras, visto as etiquetas para identificação de objetos serem baratas, e diferentemente do código de barras, têm processamento e memória, fornecendo alguma inteligência.

2.2.7. NFC

O NFC (*Near Field Communication*) é uma tecnologia que permite a transferência de dados numa comunicação sem fios de curta distância (figura 14), sendo apenas este fator de distância, a única diferença entre o NFC e o RFID. O NFC surgiu a partir do RFID, por isso muitos dos benefícios observados no ponto anterior são compartilhados por ambas as tecnologias. Tal como acontece no RFID, a comunicação é feita de maneira simples e intuitiva, bastando apenas aproximar dois aparelhos, ou o aparelho e uma *tag* passiva, a uma curta distância. A velocidade da taxa de transferência do NFC é de 424 kbits/s e opera na frequência de 13.56 Mhz.

Figura 14. NFC
Fonte: Contactless Intelligence (2015)

Na Tabela 3, segue um quadro-resumo das tecnologias de comunicação *wireless* disponíveis na IoT:

	Wi-fi	*Z-Wave*	*Zigbee*	*Thread*	*Bluetooth*	NFC
Primeiro ano no mercado	1997	2003	2003	2015	2010	2006
***Standard* PHY/MAC**	IEEE 802.11.1	ITU-T G.9959	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.15.1	IEEE 802.15.1
Largura de banda	2.4 GHz	900MHz	2.4GHz	2.4GHz	2.4GHz	13.56 MHz
Alcance	100 m	30–100 m	10–100 m	10–100 m	30 m	20 cm
Velocidade de transferência de dados	54 Mbit/s	40-100 Kbit/s	250 Kbit/s	250 Kbit/s	1 Mbit/s	424 kbit/s
Topologia	Star	Mesh	Mesh	Mesh	Scatternet	Star
Power usage	Alto	Baixo	Baixo	Baixo	Baixo	Baixo

Tabela 3*.* Tecnologias de comunicação *Wireless* na IoT
Fonte: Elaborado pelo autor

2.3. Normas e *standards* na IoT

Os *standards* e normas na IoT começaram a ser falados por meados do início de 2013. A indústria tecnológica, tipicamente, não espera que os *standards* sejam desenvolvidos, muitas batalhas tecnológicas são ganhas ou perdidas antes das normas estarem sequer perto de concluídas.

A IoT envolve a conexão entre dispositivos que na maior parte dos casos nunca se pensou conectarem-se. Envolve também a gestão desses objetos e desenvolver aplicações para que eles façam coisas juntos que nunca fariam sozinhos. Visto isto, os produtos de diferentes fabricantes terão eventualmente, em algum nível, de "falar a mesma língua". Caso contrário, para Lawson (2015), os produtos para casas conectadas, cidades e fábricas não serão tão vendidos como o esperado, especialmente se os preços dos produtos começarem a cair a pique, tal como aconteceu com os PCs, *smartphone*s e outros produtos, ao longo dos anos. Isto é especialmente importante para os utilizadores da IoT, onde o custo é um fator primordial. Posto isto, os fornecedores não pretendem esperar por *standards* formais, estando já eles próprios a formar alianças para influenciar as normas e *standards*. Estas alianças estão a ser criadas para administrar quatro áreas principais: a conectividade, interoperabilidade, privacidade e segurança.

2.3.1. Aliança *AllSeen*

O primeiro grupo de normas IoT, a *AllSeen*, foi lançada em Dezembro de 2013, e conta com dezenas de empresas envolvidas, incluindo nomes como a Microsoft, Qualcomm, LG, Cisco e Panasonic.

A framework de *software open-source*, *AllJoyn*, é baseada numa tecnologia criada pela Qualcomm. O objetivo da aliança é proporcionar aos dispositivos para *Smart homes*, que utilizam diferentes sistemas operativos e diferentes protocolos de rede, uma forma para comunicarem uns com os outros. A Aliança prevê a conectividade através de camadas de transporte, tais como *WiFi*, *WiFi-Direct*, *Ethernet*, *Bluetooth LE*, *Zigbee*, e *Zigbee*. A interoperabilidade é também um foco, com plataformas suportadas, incluindo Android, iOS, Linux, OpenWRT, Windows e OS X. A AllJoyn (figura 15) prevê ainda

garantir a segurança e privacidade dos dados. Segundo Matias (2015) uma extensão da *framework*, o *AllJoyn gateway Agent* (figura 15) usa criptografia *end-to-end* para manter comunicações seguras. O *Gateway Agent* também usa controlos de privacidade que permitem aos utilizadores decidir quais os dispositivos e quais as aplicações que têm acesso e quais os serviços da *cloud*.

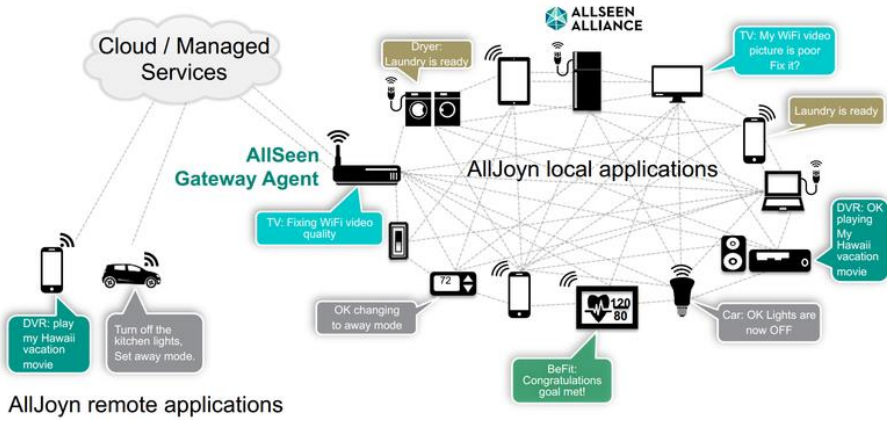

Figura 15. *AllSeen* - AllJoyn *Gateway* Agent
Fonte: Nichols, S. (2015)

2.3.2. *Open Interconnect Consortium* (OIC)

A Open Interconnect Consortium (OIC), composta por organizações como a Dell, Atmel, Intel, Samsung, Broadcom e Wind River, tem como objetivo criar uma especificação e desenvolver um projeto *open-source*, capaz de fazer com que todos os dispositivos IoT sejam capazes de comunicar entre si, independentemente do seu sistema operativo, fornecedor, ou protocolos. A sua especificação é simples de ser implementada e é fácil de utilização para o *developers*. Existe já uma implementação *open-source* da especificação, a IoTivity (figura 16), uma estrutura de código aberto baseado no modelo de licenciamento do Apache 2.0. Esta aliança pretende assim, garantir a interoperabilidade dos dispositivos IoT para consumidores, negócios e industrias.

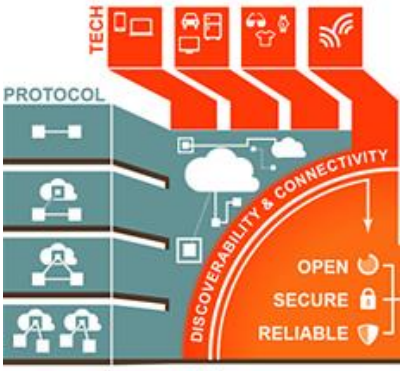

Figura 16. *OIC* – IoT*ivity*
Fonte: Zemlin, J. (2014)

2.3.3. *Thread Group*

Fundada por organizações a Samsung, ARM Holdings, Silicon Labs e a Nest Labs (empresa de termostátos e alarmes de fumo adquirida pela Google), pretende criar um protocolo de rede *mesh* para conectar e controlar os dispositivos de habitações. O objetivo do grupo é incentivar os fabricantes de dispositivos *Smart home* a utilizar o protocolo *Thread* (ver ponto 2.1.4.5) para comunicações entre dispositivos através de uma rede. Este protocolo baseia-se num protocolo de rádio de baixa potência, conhecido como *IPv6 over Low power Wireless Personal Area Networks* (6LoWPAN) (figura 17). Assim sendo, todos os dispositivos IoT certificados pela *Thread* irão ganhar um endereço IPv6. Segundo Peter (2014), a filosofia da IoT tem como objetivo conectar todos os dispositivos à Internet, e por isso é importância vital os dispositivos terem um endereço IPv6, visto os endereços IPv4 começam a ficar esgotados.

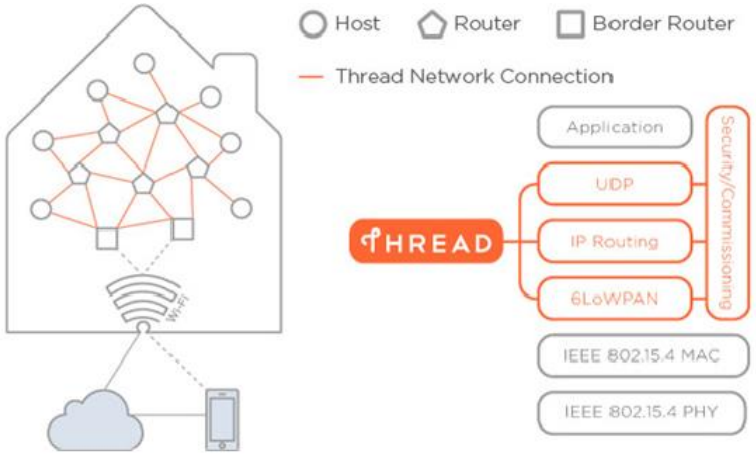

Figura 17. Protocolo *Thread*
Fonte: Peter (2014)

O grupo *Thread* vê este protocolo como interligações com as camadas de aplicação fornecidos pelas outras alianças. Esta aliança teve início em Julho de 2014 e começou a fazer certificações em 2015.

Null (2014), vice-presidente da segurança e estratégia da *Cloud* na CipherCloud afirma que o protocolo *Thread* tem muito potencial. Segundo ele, este protocolo de rede mesh baseado em IP apresenta um grande conceito e está no bom caminho para ser bem adotado nas redes IoT.

Duas das grandes componentes de peso das *Smart homes*, o *standard Zigbee* e a aliança *Thread*, fizeram uma parceria em 2015, de forma a permitir aos produtos que utilizam o *standard* de comunicação *Zigbee* (ver ponto 2.1.4.3), utilizarem o protocolo *Thread* e um programa de certificação, de forma a garantir a interoperabilidade. A *Zigbee* começou já a desenvolver uma solução combinada que vai permitir agilizar o desenvolvimento dos produtos IoT, melhorar a interoperabilidade e ultimar a experiência do consumidor com os seus dispositivos IoT para *Smart home* (*Zigbee*, 2016).

2.3.4. *Industrial Internet Consortium* (IIC)

Fundada em Março de 2014 pela Intel, Cisco, AT & T, GE e IBM, o IIC, tal como o nome indica está a trabalhar em diretrizes relacionadas com as aplicações industriais. Os membros do grupo estão a colaborar para desenvolver padrões de conectividade, tendo o *Industrial Internet Consortium* (IIC) assinado um acordo estratégico com a OIC para partilhar informações de forma a agilizar a interoperabilidade de dispositivos com IoT.

A IIC (2014), afirma que o grupo não vai definir normas, mas em vez disso irá trabalhar com os organismos de *standardarização* de forma a garantir as tecnologias trabalham em conjunto em todos os setores de negócio. Afirma ainda que está a reunir as organizações (figura 18) e as tecnologias necessárias de forma a acelerar a *adoção* da IoT ao definir os padrões, através da identificação e promoção das melhores práticas.

Segundo Matias (2014), o IIC assinou uma parceria com fornecedores de plataformas de segurança CyberX e SAP para definirem as normas de segurança e privacidade. Estas empresas vão entregar à IIC casos de uso, arquitectura e *frameworks* de referência e de segurança para aplicações da IoT.

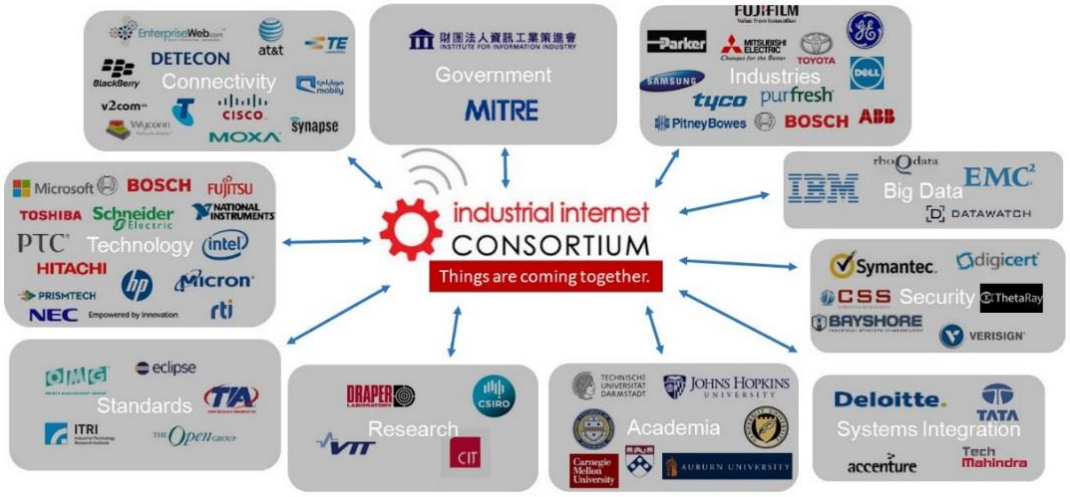

Figura 18. Organizações Aliança IIC
Fonte: Soley, R. (2015)

2.3.5. IEEE P2413

Segundo Lawson (2014), o IEEE formou um grupo de trabalho para trazer alguma ordem à matriz de especificações e *standards* desenvolvidos pelas alianças do setor da IoT. Entre outras coisas, pretende transformar a informação das diferentes plataformas IoT em objetos de dados normalmente entendidos. O grupo realizou a sua primeira reunião em Julho de 2014 com 23 fornecedores e organizações envolvidas na IoT e pretende terminar o seu trabalho sobre a futura norma em 2016. A IEEE (2014) afirma que após conclusão, o *Standard* irá fornecer uma *framework* de arquitetura robusta para a IoT, reduzindo a fragmentação do mercado, melhorando a interoperabilidade e servindo como um catalisador para o crescimento da IoT.

2.3.6. *Apple Homekit*

A Apple não poderia ficar de fora dos *standards* para IoT, tendo vindo dar a aprovação a fabricantes de aparelhos no âmbito do processo de certificação “Made for iPhone” já utilizado para os acessórios iOS. A *Homekit* (figura 19) fornecerá *kits* de ferramentas para os developers para que possam fazer a integração de *Smart home*s com os seus consumidores. A API *Homekit* apresenta uma linguagem projetada para ser interoperável com dispositivos não-HomeKit que usam protocolos como o *Zigbee* ou *Zigbee*. Este *standard* inclui também camadas de segurança e privacidade, como criptografia end-to-end entre dispositivos iOS e dispositivos inteligentes (Matias, 2015).

Naturalmente, a *Homekit* da Apple não poderá ser considerado propriamente um s*tandard* comum, visto apresentar o método base proprietário muito conhecido da Apple.

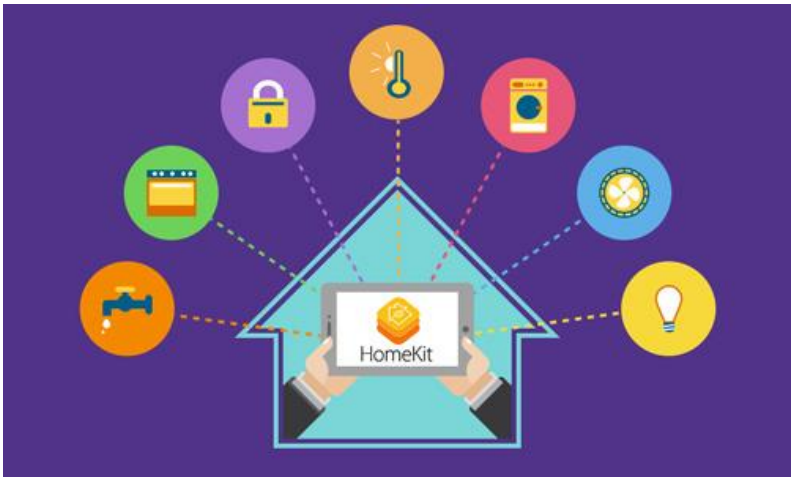

Figura 19. *Apple Homekit*
Fonte: Feierman, A. (2015)

2.4. Limitações legais e sociais

Segundo a Mckinsey (2015), em 2025 a IoT irá ter um impacto económico potencial total entre $3.9 triliões a $11.1 triliões. Esse valor poderá equivaler a 11% da economia global.

Grande parte dos fabricantes tecnológicos já se juntou a este paradigma emergente, mas tal como qualquer mudança disruptiva, ainda vai demorar algum tempo até as *frameworks* regulatórias estarem bem definidas.

Com o aparecimento desta indústria, são muitas as questões legais e sociais que surgem. As principais áreas de legislação a serem afetadas pela IoT são a segurança, privacidade e a competição legal. Em relação à segurança, os reguladores terão de introduzir protocolos de forma a garantir de segurança do utilizador. A importância da privacidade também aumenta exponencialmente, uma vez que a quantidade de informação sobre a vida de uma pessoa vai aumentar à medida que a quantidade de dispositivos conectados à IoT também aumenta. Os consumidores desses produtos irão exigir um maior controlo sobre as suas informações privadas, enquanto as empresas vão querer armazenar essas

informações para fins de marketing e comercial. A concorrência é também um desafio, visto os grandes *players* do mercado tecnológico tentarem criar *standards* e controlarem as *frameworks* que conectam estes dispositivos, patatenteando essas tecnologias e procurarem acordos comerciais exclusivos.

2.4.1. Segurança e proteção dos dados

Um dos desafios mais preocupantes da IoT é a forma como a segurança dos dados e dos próprios consumidores irá ser garantida.

Como já acontece com os equipamentos de medição inteligente e automóveis cada vez mais autónomos, haverá um vasto volume de dados fornecendo informações sobre o uso pessoal dos aparelhos que, caso não forem seguros, poderão abrir caminho para violações de privacidade. Isto é um desafio, pois o volume de informação gerada pela IoT é essencial para trazer melhores serviços e comudidades aos consumidores.

Dreibi (2014), da Cisco, afirma que para a IoT se tornar uma realidade não basta apenas conectar as coisas, é preciso controlar e ter visibilidade de toda a rede. A segurança não é opcional. O segundo ponto, para Dreibi, é o controlo dos dispositivos, o que eles podem aceder na rede. Para o mesmo, o terceiro ponto é a segurança tradicional, ou seja, colocar barreiras para evitar que toda a infraestrutura seja prejudicada em caso de um ataque.

Um relatório sobre o crime organizado e a Internet, publicado pela Europol (2014), adverte que os dispositivos inteligentes dependem na maioria das vezes de programas/aplicações que podem ser facilmente pirateados e que são muitas vezes concebidos sem qualquer medida de segurança. O relatório acrescenta que com a multiplicação dos objetos ligados à Internet, devemos esperar um número crescente de ataques contra as infraestruturas existentes e emergentes, incluindo novas formas de chantagem e de extorsão – como o *ransomware*, uma forma de chantagem que utiliza os dados pessoais roubados por *hackers*. Entre os riscos conta-se não apenas o roubo de dados como também “ferimentos físicos ou até mesmo mortes, conclui o estudo da Europol (2014).

2.4.2. Privacidade dos dados

O glossário de segurança da Internet[2] define a privacidade como “o direito de um entidade (geralmente uma pessoa), agindo em seu próprio nome, determinar o grau ao qual ela irá interagir com o seu ambiente, incluindo o grau à qual a entidade está disposta a compartilhar informação sua com os outros”.

Tipicamente na IoT, o ambiente é formado por uma rede de dispositivos conectados com sensores. Esses dispositivos transmitem então a informação recolhida e eventos específicos a um servidor. Essa transmissão é feita através de uma comunicação fixa ou móvel. A privacidade deve então ser protegida ao nível do dispositivo, durante a comunicação com o servidor, no armazenamento no

[2] Glossário que providencia um consistente e complementar conjunto de abreviações, definições, explicações e recomendações sobre a terminologia relacionada com a segurança dos sistemas de informação. https://www.ietf.org/rfc/rfc2828.txt

servidor e no processamento.

No primeiro caso, ao nível do dispositivo, a informação sensível pode ser roubada em caso de manipulação do *hardware* ou do *software* do próprio dispositivo. Por exemplo, um *hacker* pode entrar no sistema de luzes inteligentes de uma casa e analisar os hábitos de uma família, agregando a informação e encontrando padrões de quando a casa está inabitada, ou quando uma certa divisão está vazia. Durante a comunicação com o servidor, a abordagem mais utilizada é a encriptação. Apesar de ser a mais utilizada, pode não ser a mais segura, pois a encriptação geralmente dispõe os dados em pacotes que deixam vestígios, tais como o seu número de sequência, etc. Em relação à privacidade no armazenamento que é feito no servidor, deve ser feita uma filtragem desta, armazenando o mínimo de informação possível, ou então apenas aquilo que o consumidor consinta. Por fim, o fornecedor de cada dispositivo pode utilizar a informação recolhida desses mesmos dispositivos para diversos propósitos, entre os quais: análise ou comercialização. O utilizador deve assim poder saber que uso é dado aos seus dados, e consentir ou não, que estes sejam utilizados para um propósito diferente do inicial e consentido.

A WP29 (2014), um órgão europeu consultor em privacidade e proteção de dados, instituído pelo artigo 29 da diretiva 95/46 CE, decidiu emitir um parecer específico sobre a consideração de que a IoT representa um grande número de desafios ao nível da privacidade e proteção de dados, alguns novos e outros tradicionais, que irão aumentar em simultâneo com o aumento exponencial de processamento de dados, decorrendo da evolução contínua da IoT.

Os desafios de privacidade e proteção de dados na IoT que a WP29 (2014) identifica são:

1. **Falta de controlo e assimetria da informação**: A interação entre objetos que comunicam automaticamente, e entre os objetos e sistemas de *back-end* irá resultar na geração de fluxos de dados que dificilmente podem ser controlados com as ferramentas tradicionais utilizadas para garantir a devida proteção dos interesses e direitos das pessoas em causa. Esta questão de falta de controlo, diz respeito também a áreas como a *cloud computing* ou *big data*, e é ainda mais desafiadora quando se pensa que diferentes tecnologias emergentes podem ser utilizadas em combinação;

2. **Qualidade do consentimento do utilizador**: Em muitos casos, o utilizador pode não estar ciente do tratamento de dados efetuado por certos dispositivos. A possibilidade de rejeitar determinados serviços não é uma alternativa viável na IoT, e os mecanismos clássicos usados para obter consentimento são difíceis de aplicar. Portanto, novas formas de obtenção de consentimento por parte do utilizador dos aparelhos conectados devem ser consideradas pelos seus fabricantes.

3. **Redefinição do processamento original dos dados**: O aumento da quantidade de dados gerada pela IoT, em combinação com técnicas modernas de análise de dados e *cross-matching* podem dar origem a usos secundários desses mesmos dados, relacionados ou não com a finalidade de processamento atribuídos inicialmente aos dispositivos. Ou seja, dados aparentemente insignificantes recolhidos de dispositivos podem ser utilizados para inferir informações com um propósito totalmente diferente do

inicial (por exemplo, hábitos de condução).

4. **Identificação de padrões e relações:** Apesar de cada aparelho gerar fluxos de dados isoladamente, a sua recolha e posterior análise pode facilmente revelar padrões, comportamento, preferências e hábitos específicos de um individuo. Como visto no ponto acima (3. Redefinição do processamento original dos dados), conhecimento pode ser gerado a partir de informação trivial, através de capacidade de profiling aos dados dos sensores.

5. **Limitações sobre a possibilidade de manter o anonimato ao utilizar serviços:** o pleno desenvolvimento das capacidades da IoT pode colocar pressão sobre as possibilidades atuais de utilização anónima de serviços e limitam a possibilidade de se manter anónimo.

Tal como referenciado no ponto 2.1.2.3, os *wearables* e *portables* são alguns dos *icons* da IoT atual. Estes produtos recolhem, naturalmente, informação sensível do utilizador para o seu funcionamento, tal como no caso dos *fitness trackers*, recolhem informação de batimentos cardíacos, temperatura corporal, calorias gastos, número de passos dados, etc. Esta informação é posteriormente armazenada nos servidores dos fornecedores dos dispositivos (segundo os padrões das suas políticas de privacidade dos produtos), é enviada a *apps* próprias dos produtos, a prestadores de serviços de saúde ou seguradores de saúde, e pode também ser enviada para redes sociais. Essa informação, apesar de sensível e confidencial, é partilhada, tal como mostra a figura 20 com uma série de canais, pondo em causa vários fatores de risco.

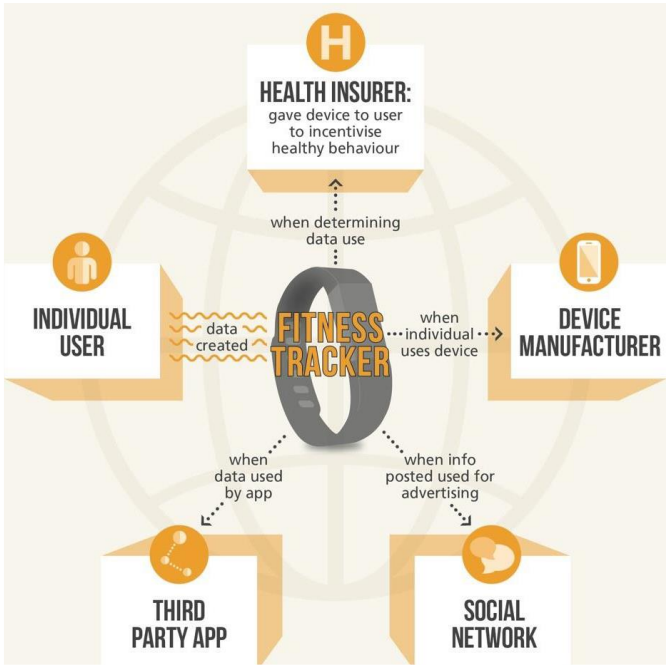

Figura 20. Canais de partilha de dados por parte de um Fitness Tracker
Fonte: Consumers International. (2016)

Tal como referenciado pelo Escritório do Comissário de Privacidade do Canada (2016), à medida que a IoT vai evoluindo, cada vez mais serão as pessoas que terão as suas atividades e comportamentos registados e analizados, havendo por isso uma necessidade crescente para que os fornecedores do mercado informem os seus consumidores sobre quem armazena os dados dos seus dispositivos pessoais, como são armazenados, como são utilizados e a quem são divulgados. Os princípios de privacidade exigem que as pessoas devam manter o controlo dos seus dados, bem como de serem capazes de optar por sair do ambiente "inteligente" sem incorrer em consequências negativas.

O impacto total da IoT para a nossa privacidade pode tornar-se mais evidente quando as suas capacidades são combinadas com outras inovações que moldam o nosso mundo atual e futuro, e que controlam não só as nossas atividades, comportamentos e preferências, mas também as nossas emoções e pensamentos.

2.5. Legislação

Por todo o mundo, governos, reguladores e outras instituições já se começaram a focar na IoT e na sua importância. Na Europa, encontra-se em fase de negociações um regulamento que cobre os aspetos relacionados com a proteção e dados por todos os 28 estados membros da União Europeia. Já nos EUA, a regulamentação ainda não é uma realidade, pois segundo eles, a IoT está ainda numa fase muito prematura para ser desde já legislada.

2.5.1. Na Europa

Em relação à Europa, a Comissão Europeia publicou um relatório em 2013, onde fornece uma visão geral dos seus resultados de consulta pública sobre a gestão da IoT. Segundo a CE (2013), a IoT tem o potencial de melhorar consideravelmente a vida dos cidadãos da União Europeia, abordando muitos dos desafios da sociedade de hoje, nomeadamente na área da saúde, transportes, ambiente, energia, etc. Ao mesmo tempo, contempla também riscos para as pessoas, em áreas como a privacidade e segurança. Através de uma consulta pública, a comissão procurou obter pontos de vista sobre uma política adequada que promova um desenvolvimento dinâmico no mercado digital, garantindo simultaneamente a proteção adequada aos cidadãos da União Europeia. A consulta pública foi efetuada com base num questionário online, com cerca de 600 responstas, desde cidadãos interessados no assunto, a alunos, e fabricantes na indústria da IoT.

Como resultado do questionário, não houve um consenso sobre a necessidade e o âmbito de intervenção pública no campo da IoT. A maior parte dos intervientes questionou a legitimidade da intervenção pública num setor que ainda está na sua infância e afirmaram que as tecnologias e aplicações da IoT devem continuar a desenvolver-se antes de as apropriadas medidas políticas serem impostas. Segundo eles, os trabalhos de normalização em curso sobre identificação, arquitetura e segurança irão promover um desenvolvimento competitivo e seguro da IoT. Ressaltaram também que as inadequadas políticas podem levantar barreiras ao investimento e à inovação. Então, uma futura intervenção política deve ser flexível e reconhecer a diversidade inerente à IoT. Por outro lado, alguns intervientes

responderam que a intervenção e regularização política é necessário o quanto antes, sendo as considerações económicas um tema secundário, quando os direitos à privacidade, segurança e outras questões éticas estão em jogo.

Em modo de conclusão, o relatório da Comissão Europeia recomenda que desde o ínicio, a IoT deva ser concebida para atender aos requisitos fundamentais que sustentam o direito ao esquecimento, portabilidade de dados, privacidade e os princípios da proteção de dados.

Atualmente, as Instituições Europeias, entre as quais a Comissão Europeia, o Concelho Europeu e o Parlamento Europeu estão a negociar um Regulamento Geral de Proteção de Dados[3] (GPDR 2012/0011 que irá substituir a atual diretiva 95/46/EC) (figura 21), proporcionando uma *framework* harmonizada por todos os 28 estados membros da União Europeia. Em caso de aprovação pelo conselho, a nova regulação pode entrar em vigor em 2017.

O regulamento introduz algumas disposições que são relevantes para lidar com o ecossistema IoT, e os seus desafios de proteção de dados, entre os quais, a portabilidade de dados, privacidade de dados, *profiling*, direito ao esquecimento, e o consentimento por parte do utilizador, aplicando graves multas às empresas ou indivíduos que não cumprirem essa regulamentação.

Resta saber se estas regulamentações serão ou não as adequadas para a nova era inteligente e conectada.

Figura 21. EU Data Protection Reform
Fonte: Hawkins, A. (2016)

2.5.2. Nos EUA

Em Novembro de 2013, a *Federal Trade Comission*, FTC (2013), uma agência independente do governo dos EUA (Estados Unidos da América) que se dedica à promoção da proteção dos consumidores, organizou um *workshop* público com o intuito de explorar questões de privacidade e segurança dos consumidores, tanto em casa (onde se incluem a automação residencial, eletrodomésticos inteligentes, etc.) como na rua (incluindo dispositivos de fitness, carros autónomos, etc.), colocadas pela crescente

[3] Este projeto de regulamento atualiza e moderniza os princípios estabelecidos na diretiva de 1995 relativa à proteção de dados. Nomeadamente, define os direitos das pessoas singulares e estabelece as obrigações dos que efetuam o tratamento dos dados e dos responsáveis por esse tratamento. Estabelece ainda os métodos que garantem a conformidade e o âmbito das sanções aplicáveis aos infratores. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

conectividade de dispositivos. Neste *workshop*, estiveram presentes alunos, representantes da indústria e grupos de defesa do consumidor. Este serviu para informar a Comissão sobre os desenvolvimentos nesta área.

Após este *workshop*, em Janeiro de 2015, a FTC (2013) divulgou um relatório de 71 páginas, onde descreve as melhores práticas para a IoT, de forma a ir ao encontro da proteção do consumidor, e ainda permitindo que todos os benefícios da IoT sejam plenamente realizados.

Segundo Whaley (2015), a FTC recomenda que os fabricantes dos dispositivos tomem medidas concretas para proteger a segurança das informações recolhidas através desses mesmos aparelhos.

Estas medidas incluem:

- Pensar na segurança do dispositivo desde o ínicio da sua construção, e não apenas uma reflexão tardia;
- Formar os colaboradores da organização sobre a natureza crítica da informação, e garantir que este é gerida a um nível elevado dentre da própria organização;
- Garantir que, quando estão envolvidos fornecedores ou consultores de serviços externos à organização, que estes são capazes de manter as medidas de segurança adequadas, bem como uma correta supervisão;
- Monitorização os dispositivos conectados durante todo o seu ciclo de vida, e fornecer *patches* de segurança de forma a cobrir os riscos conhecidos.

Ainda segundo Whaley (2015), o relatório incentiva também os fornecedores a considerarem uma "minimização de dados", limitando a recolha de dados dos consumidores em primeiro lugar, e retê-los apenas por um determinado período de tempo, ao invés de os guardarem indefinidamente. Isto reduz o risco de uma empresa com grandes volumes de dados de consumo, de se tornar um alvo bastante atraente para os *hackers*, bem como o risco de os dados dos consumidores serem utilizados de uma forma não consentida pelos mesmos. De acordo com as recomendações de minimização de dados, a FTC pretende ser flexível, e as organizações podem escolher entre três opções: não armazenar nenhuns dados; apenas armazenar dados limitados às áreas necessárias para prestar o serviço oferecido pelo dispositivo; ou fazerem uma filtragem aos dados recolhidos.

A FTC recomenda ainda que os fornecedores informem os consumidores sobre a recolha e o uso que dão aos seus dados, bem como fornecer escolhas aos consumidores sobre a forma como as suas informações serão usadas, particularmente quando o volume de dados recolhidos é maior do que o utilizador pode razoavelmente esperar.

O relatório conclui que qualquer legislação específica sobre IoT é ainda muito prematura, dada a rápida evolução da tecnologia.

2.6. Síntese

Através da leitura do enquadramento teórico é possível entender os conceitos associados ao tema principal da dissertação, a privacidade dos dados na IoT, e subsequentemente às atividades desenvolvidas, que têm com o objetivo de dar a entender a forma como os fornecedores, consultoras e

os consumidores da IoT estão a abordar o desafio da privacidade e segurança dos dados.

A primeira parte do enquadramento referencia a temática da IoT, onde se incluem exemplos da sua utilização e o seu propósito. De seguida, a explicação dos tipos de comunicação existentes entre os dispositivos IoT é feita, com o objetivo de dar a entender a forma como estes objetos comunicam e "falam" entre si, com as suas vantagens e perigos de segurança e privacidade adjacentes. A revisão das normas e *standards* atualmente existentes evidencia a forma como as organizações fornecedores de produtos IoT se estão a posicionar no mercado face às suas estratégias de negócio e da concorrência. De seguida, as limitações legais e sociais dão a entender as duas principais barreiras para uma maior adoção da IoT por parte dos consumidores, que são a segurança e privacidade dos seus dados, sendo estas também os maiores desafios para os fornecedores. Por último, a legislação em vigor na Europa e nos EUA permite dar uma noção sobre a forma como a temática da IoT está a ser abordada pelos governos Europeus e Norte Americanos.

3. Estratégia Metodológica

Este capítulo tem como objetivo fazer uma referência às estratégias metodológicas existentes, e a qual o tipo de estratégia utilizada para a elaboração da dissertação.

A estratégia metodologia deve ser encarada como um conjunto de métodos ou regras que têm como objetivo delinear um determinado caminho que conduza a um fim, num processo de transmissão de conhecimentos, dirigido ao público-alvo e entendido pelos destinatários, aplicando processos de investigação específicos de modo a conduzir a resultados adequados e credíveis. (Sousa, 1998).

3.1. Metodologia qualitativa

A pesquisa qualitativa, utilizada para interpretar fenómenos, ocorre por meio da interação constante entre a observação e a formulação conceitual, entre a pesquisa empírica e o desenvolvimento teórico, entre a perceção e a explicação (Bulmer, 1977). O método qualitativo é útil e necessário para identificar e explorar os significados dos fenómenos estudados e as interações que estabelecem, assim possibilitando estimular o desenvolvimento de novas compreensões sobre a variedade e a profundidade dos fenómenos sociais (Bartunek; Seo, 2002).

Também Bogdan e Bilken (1994) utilizam a expressão investigação qualitativa como termo genérico para agrupar diversas estratégias de investigação que partilham determinadas características. Nesta investigação, os dados recolhidos são *design*ados por qualitativos, o que significa ricos em fenómenos descritivos relativamente a pessoas, locais e conversas, e de complexo tratamento estatístico (Bogdan e Bilken, 1994, p.16). As questões a investigar não se estabelecem mediante a operacionalização de variáveis mas são, antes, formuladas com o objectivo de estudar fenómenos com toda a sua complexidade em contexto natural.

Os métodos qualitativos sugerem que o investigador esteja no trabalho de campo, faça observação, emita juízos de valor e que analise. Na investigação qualitativa, é essencial que a capacidade interpretativa do investigador nunca perca o contacto com o desenvolvimento do acontecimento. Outro aspecto característico (Stake, 1999) da investigação qualitativa é que direcciona os aspectos da investigação para casos ou fenómenos em que as condições contextuais não se conhecem ou não se controlam.

Alguns exemplos dos métodos a utilizar nesta dissertação são as ações de investigação, estudos de caso, entre outros, sendo que a sua fonte de evidências inclui a observação, entrevistas, documentos e textos.

3.2. Metodologia quantitativa

A investigação quantitativa caracteriza-se pela atuação nos níveis de realidade e apresenta como objetivos a identificação e apresentação de dados, indicadores e tendências observáveis. Este tipo de investigação mostra-se geralmente apropriado quando existe a possibilidade de recolha

de medidas quantificáveis de variáveis e inferências a partir de amostras de uma população. Esta investigação utiliza medidas numéricas para testar hipóteses, mediante uma rigorosa recolha de dados, ou procura padrões numéricos relacionados com conceitos quotidianos. Numa fase posterior, os dados são sujeitos a análise estatística, através de modelos matemáticos (ou *software* próprio), no sentido de testar as hipódissertaçãos levantadas. Como tal, a sua utilização está geralmente ligada à investigação experimental ou quasi-experimental.

Nos estudos organizacionais, a pesquisa quantitativa permite a mensuração de opiniões, reações, hábitos e atitudes num universo, por meio de uma amostra que o represente estatisticamente. Pode-se afirmar que se estabelece então uma relação causa-efeito e se procede a uma previsão dos fenómenos.

Stake (1999) assinala que nos modelos quantitativos habituais o investigador exerce um esforço para limitar a sua função de interpretação pessoal, desde que se inicia o desenho da investigação até que se analisam estatisticamente os dados. Trata-se de um período que se deve pautar pela ausência de valores. Na investigação quantitativa, as perguntas procuram a relação entre um pequeno número de variáveis. O esforço vai para a operacionalização dessas variáveis e para reduzir ao mínimo o efeito da interpretação, até que os dados estejam analisados. Aqui é importante que a interpretação não mude o rumo da investigação.

Os principais métodos de pesquisa quantitativa são a survey (levantamento), a correlacional, a causal-comparativa e a experimental. Reconhecem-se como principais formas de abordagem qualitativa a pesquisa ação, a pesquisa histórica, o estudo de caso, o *focus group*, a etnografia e a *grounded theory*.

3.3. Estratégia de Investigação

Conforme mencionado na secção 1.4. Metodologia, em que se abordou as questões subjacentes às metodologias, foi considerado que o método de Estudo de Caso seria o mais indicado para a condução do estudo em causa.

A característica mais central da investigação qualitativa, em contraste com a quantitativa, é que aquela põe a ênfase na perspectiva individual do que está a ser estudado. Descrevendo a complexidade do problema, pode-se contribuir para o processo de mudança, possibilitando o entendimento de variadas particularidades.

Verifica-se que o Estudo de Caso constitui um método de investigação que pode ser aplicada quer à abordagem quantitativa quer à abordagem qualitativa. Isto porque, esta é a metodologia que se deve utilizar para “compreender, explorar ou descrever acontecimentos e contextos complexos” (Araújo et al, 2008).

Yin (2003) afirma que esta estratégia é utilizada em situações complexas, quando o investigador procura respostas para “como?” e “porquê”, quando o investigador pretende relacionar fatores de uma determinada entidade, quando o investigador pretende analisar, descrever, ou conhecer a dinâmica do fenómeno, do programa ou do processo em estudo (as cited Araújo et al, 2008). Assim, a seleção deste método pode justificar-se com os fundamentos de Yin (2003): “os casos de estudo são preferíveis quando

as questões propostas são “como” ou “porquê”, quando o investigador tem pouco controlo sobre os eventos e quando a questão se centra num fenómeno contemporâneo com contexto real”.

Três princípios concorrem para uma boa recolha de dados segundo Yin (1990): (i) Usar múltiplas fontes de evidências; (ii) construir, ao longo do estudo, uma base de dados; (iii) formar uma cadeia de evidências.

Partindo destas premissas, a questão de investigação colocada “Na IoT, de que forma os fornecedores e consumidores de produtos abordam a privacidade dos dados?” é uma questão explicativa que pretende explorar o tema da privacidade dos dados na IoT. Este objetivo pressupõe a recolha de informação variada, no entanto, é importante salientar que o investigador não tem qualquer influência sobre os dados procedendo apenas à sua recolha e análise.

É através da revisão da literatura que se pretende compreender e explorar os artigos já existentes bem como definir alguns conceitos que ajudarão a uma melhor compreensão da dissertação.

A definição do conceito de IoT, a contextualização das suas aplicações no mercado, as questões envolventes às limitações legais e sociais, bem como a exploração da comunicação entre dispositivos e das normas e *standards* existentes, permitem uma contextualização mais abrangente face aos objetivos a que esta dissertação se propõe.

Esta dissertação tem como objetivo entender a forma como as organizações fornecedoras, consultoras, e utilizadores finais da IoT estão a abordar o desafio da privacidade e segurança dos dados. Tuckman (2000: 516) refere que as fontes de obtenção de dados que se podem utilizar num estudo de caso são normalmente de três tipos: (1) Inquéritos (Questionários e entrevistas), (2) documentos vários e (3) através da observação.

Tendo em conta esta premissa, a metodologia de estudo baseou-se, numa primeira fase, na investigação da temática por questionários dirigidos a fornecedores de produtos e tecnologias IoT.

Numa segunda fase, através da ferramenta SAS Contextual Analysis, procedeu-se à identificação de padrões, relações e tendências em informação obtida de documentos da área.

3.4. Concepção e análise do questionário

A utilização de modelos qualitativos sugerem que o investigador esteja no trabalho de campo, faça observação, emita juízos de valor e que analise. Na investigação qualitativa, é essencial que a capacidade interpretativa do investigador nunca perca o contacto com o desenvolvimento do acontecimento.

3.4.1. Âmbito de investigação

A primeira preocupação operacional relativa ao preenchimento do questionário dirigiu-se para a concepção e fiabilidade das questões, na confirmação de uma correcta abordagem ao tema e ao enquadramento nacional.

Assim, a escolha criteriosa das questões teve com base os seguintes critérios:

- Enquadramento com a área de atividade das organizações, no domínio da IoT

a) Porque é que a IoT está a ter um elevado impacto global na sociedade;
b) De que forma se está a dar o comportamento das organizações na IoT.

- Enquadramento com o panorama nacional
  a) Como está a correr o desenvolvimento da IoT em Portugal.
- Enquadramento com o tema principal da dissertação, a privacidade dos dados
  a) Qual a visão das organizações para a privacidade dos dados;
  b) Como está a decorrer o processo de adequar a privacidade dos dados dos utilizadores aquando do desenvolvimento dos produtos IoT por parte das organizações.

Tendo em consideração o facto de as perguntas do questionário serem de resposta aberta, será da responsabilidade do investigador analisá-las e tirar conclusões sobre elas.

3.4.2. Participantes na investigação

A escolha das empresas a realizar o questionário teve como critérios, em primeiro lugar, à escolha de organizações fornecedoras de tecnologias IoT com bastante pegada no mercado e presentes no famoso *Internet of Things Landescape (figura 22)*: IBM, Microsoft e HP.

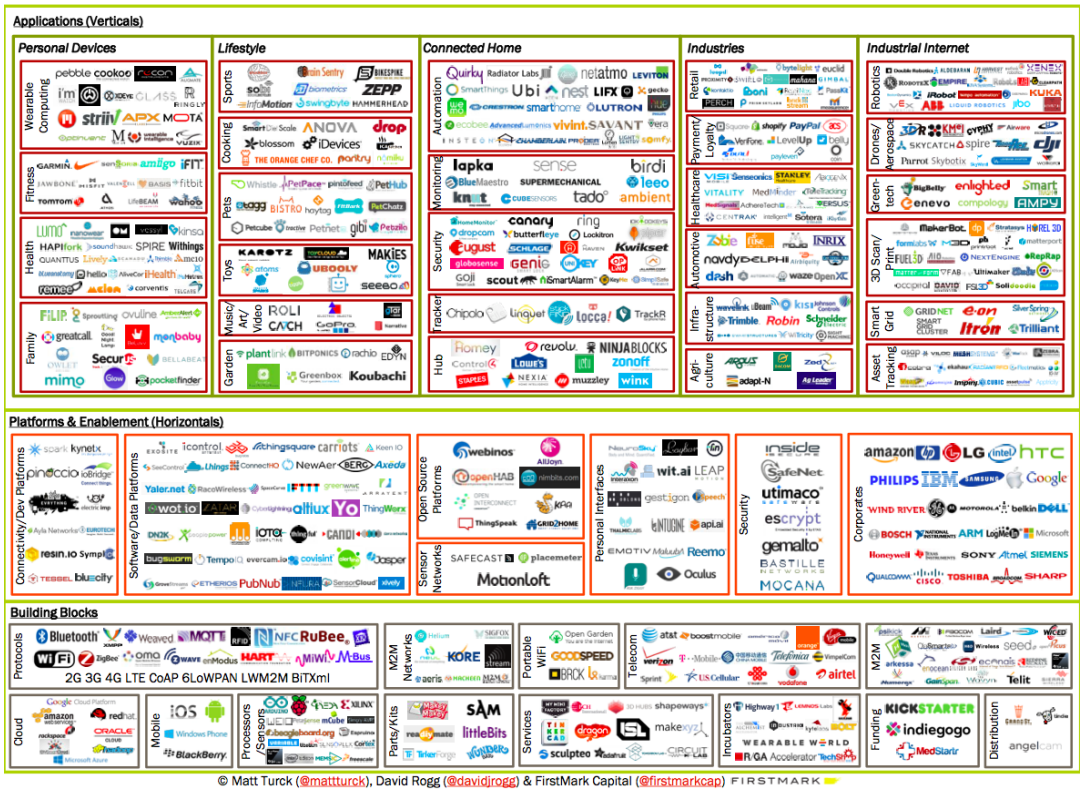

Figura 22. *Internet of Things Landescape*
Fonte: Turck, M. (2014)

A escolha das restantes organizações teve como critério o facto de, apesar de não estarem presentes no *Internet of Things Landescape*, terem uma grande reputação no mercado tecnológico, e com área de atuação no processamento de dados da IoT: SAS e Oracle.

O questionário foi direcionado aos elementos responsáveis pela IoT de cada empresa, sendo que:

- 3 foram feitos de modo presencial (nas instalações das organizações) – SAS, Oracle e Microsoft;
- 2 que apesar de não poderem preencher o questionário, devido a questões de natureza interna das organizações, enviaram documentação oficial de suporte às questões, de modo a que o investigador a analise e posteriormente preencha as respostas do questionário conforme a sua capacidade de análise à documentação – HP e IBM.

Das organizações, os elementos contactados para a realização dos questionários foram pessoas com responsabilidades na área da IoT. As equipas de cada organização tentaram sempre transmitir a mensagem corporativa de cada empresa, e não a sua opinião pessoal às perguntas do questionário.

3.5. Análise de documentos de privacidade dos dados na IoT

Posteriomente à análise dos questionários, dar-se-à a análise de documentos de privacidade dos dados na IoT, através da leitura automática de documentos, e posterior geração e análise dos seus resultados através da ferramenta SAS Contextual Analysis, com o objetivo de entender a forma como os produtos das organizações na área da IoT estão a garantir a privacidade dos dados dos seus consumidores. Estes resultados serão comparados com os resultados de documentos de análise a estes mesmos produtos. Além disso, foi também analisada a visão das principais consultoras da área da IoT para este tema. A figura 23 dá uma visão macro das comparações e análises que foram efetuadas. A escolha dos documentos a serem analisados teve como base os seguintes fatores:

- As políticas de privacidade dos fornecedores IoT são os documentos oficiais das empresas, e que estão disponíveis nos seus *websites*;
- Os documentos de análise à privacidade dos dados dos produtos de alguns dos fornecedores, são documentos elaborados por analistas da área e são referentes a apenas alguns dos fornecedores analisados acima;
- As análises efetuadas pelas consultoras dizem respeito a análises ao estado atual da IoT e da privacidade dos dados, e foram extraidas dos *websites* dessas mesmas consultoras.

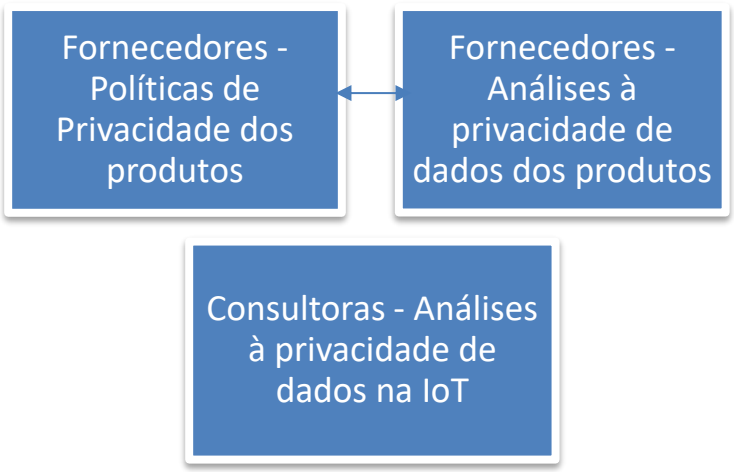

Figura 23. Tipos de análises efetuadas a documentos de privacidade de dados na IoT
Fonte: Elaborado pelo autor

3.5.1. Escolha da ferramenta a utilizar para efetuar as análises aos documentos

A ferramenta escolhida pelo aluno para efetuar as análises aos documentos de privacidade de dados na IoT referenciados no ponto anterior, foi o SAS Contextual Analysis. A escolha desta ferramenta de análise linguística de texto não-estuturado deveu-se ao facto de esta ser uma ferramenta bastante prática, *user-friendly*, perfeitamente enquadrada com as análises pretendidas, tendo sido solicitada e autorizada, junto do SAS, o licenciamento e utilização durante o periodo de trabalho da dissertação.

3.5.2. SAS Contextual Analysis

A ferramenta SAS Contextual Analysis (SCA) é uma solução linguística avançada que permite retirar insights de texto não-estruturado. Utiliza uma combinação de *machine learning* com apuramento do utilizador de forma a descobrir tendências, padrões e temas nos dados (figura 24).

O SAS Contextual Analysis elimina a necessidade de rever documentos e desenvolver taxonomia manualmente. Uma vez que a informação é registado no *software*, mecanismos de NLP (*Natural Language Processing*[4]) são realizados automaticamente, incluindo contagem de frequência de termos, deteção de sinónimos e erros de escrita, entre outros. Uma combinação de *machine learning*[5] *e* estatística, com uma ampla gama de operadores linguísticos e definições de entidades pré-construídos, o analista tem o poder de personalizar os resultados descobertos de forma automática.

[4] *NLP* (*Natural Language Processing*) é a capacidade que um programa computacional tem para entender a fala humana tal como ela é falada. É, por isso, uma componente de inteligência artificial (Rouse, 2011).
[5] *Machine Learning* é um método de análise de dados que automatiza a construção de modelos analíticos. Utilizando algoritmos, permite que computadores encontrem padrões ocultos sem serem explicitamente programados para onde investigar (SAS, 2014).

A partir de uma área de trabalho prática, o SCA é um *software* que utiliza técnicas de *text mining*[6], categorização, extração de contexto e análise de sentimentos – permitindo aos analistas aplicarem a sua análise apropriada de modo a irem ao encontro das suas necessidades, sem terem que utilizar múltiplas ferramentas.

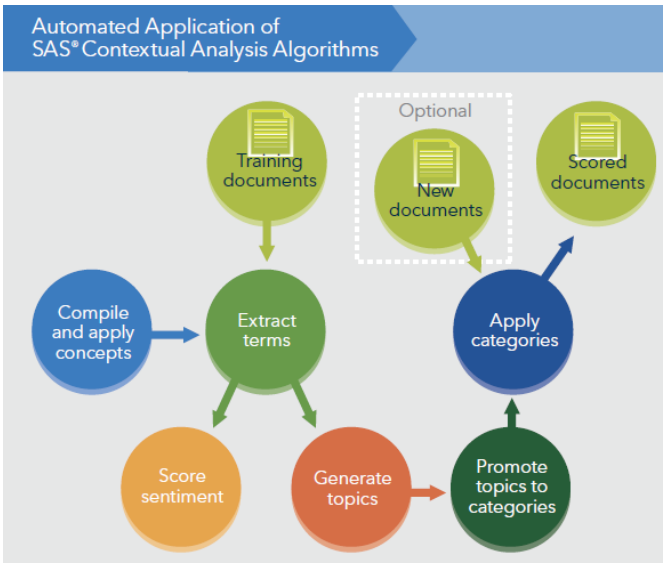

Figura 24. SAS Contextual Analysis
Fonte: SAS (2015)

O *software* providencia o seguinte (figura 25):

- Abordagem híbrida para categorização;
- Termos automáticos e descoberta de tópicos (através de procedimentos de *text mining*);
- Identificação de sentimento ao nível do documento;
- Geração automática de regras, bem como regras/taxonomia customizáveis;
- Conceitos pré-definidos e customizáveis.

[6] *Text mining* é um processo de análise de textos, geralmente utilizando técnicas estatísticas, para encontrar informações ou conhecimentos implícitos em textos (Loh, 2008)

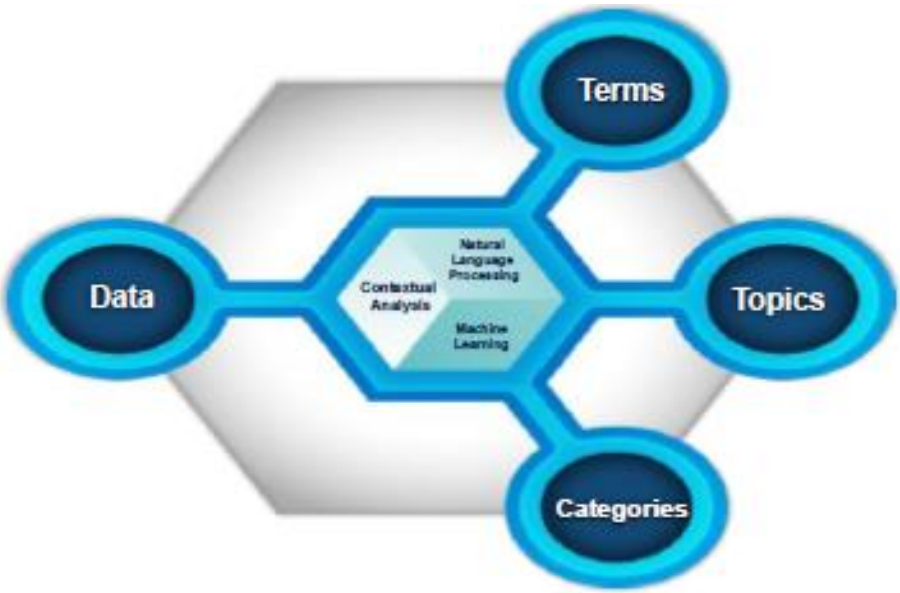

Figura 25. Funcionalidades SCA
Fonte: SAS (2015)

3.5.2.1. Identificação de termos

Examinação automática de texto com as capacidades de NLP (figura 26), incluindo:

- Deteção de sinónimos;
- Verificação ortográfica;
- Contagem de frequência de termos;
- Relação entre os termos através de term maps;
- Integração de uma *Stop*/*Start List*;
- Análise de sentimento (Positivo, negativo ou neutro) por documento de cada termo, através das capacidades analíticas do SAS.

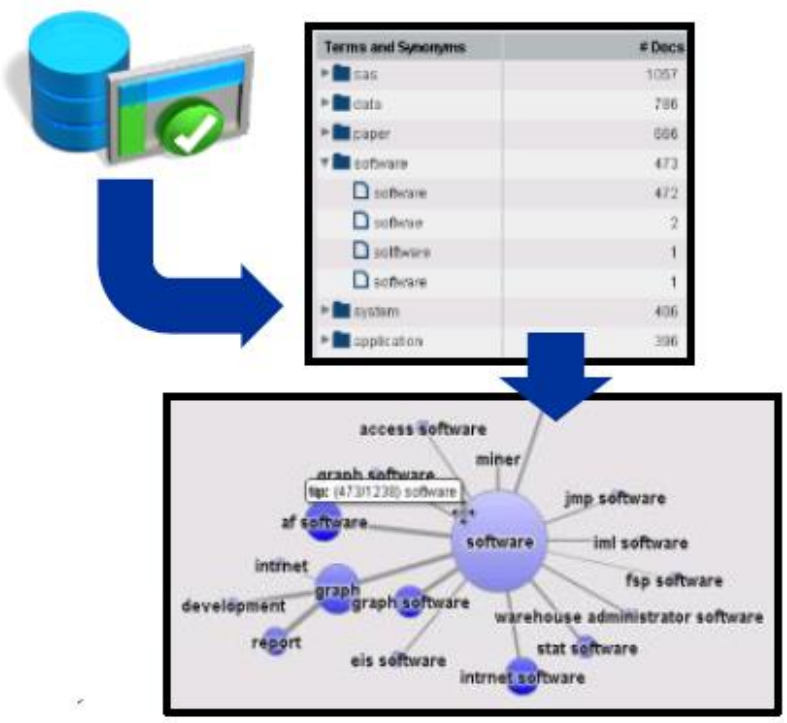

Figura 26. Identificação de termos – SCA
Fonte: SAS (2015)

3.5.2.2. Deteção automática de tópicos

Descoberta automática de tópicos escondidos:

- Descoberta automática de tópicos centrais (temas) (figura 27);
- Ranking de documentos mais relevantes por tópico;
- Visualização através de *term clouds* e mapas (figura 28);
- Possibilidade de juntar tópicos

Figura 27. Deteção de tópicos – SCA
Fonte: SAS (2015)

3.5.2.3. Deteção automática de categorias

Categorização de geração de regras:

- Definição de regras fáceis de entender;
- Teste de precisão de categorização e especificidade;
- Personalização pelo analista de forma a alcançar os resultados desejados.

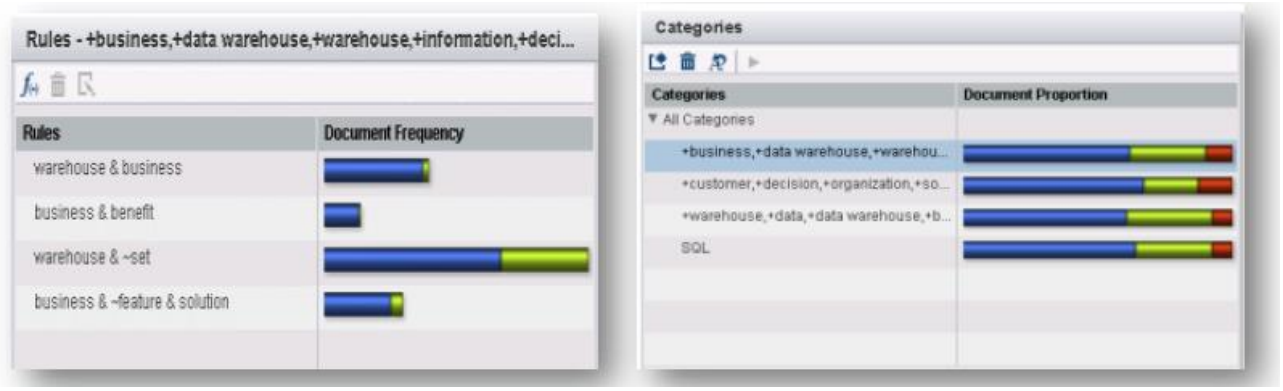

Figura 28. Identificação de categorias - SCA
Fonte: SAS (2015)

3.5.3. Âmbito de investigação

Através do *software* SAS Contextual Analysis, irá ser possível, através da leitura automática de vários documentos em formato *pdf*, criar conceitos customizados (como por exemplo o conceito Privacidade, onde se incluem os seus sub-tópicos, tais como “autorização”, “confidencialidade”, etc.) e saber o sentimento que cada documento atribui a este conceito (positivo, negativo, ou neutro), permitindo também ter uma visão macro de cada conceito.

Após a análise de conceitos, o *software* permite ter uma visão dos termos (englobando os seus sinónimos) mais utilizados em todos os documentos, bem como uma análise de sentimento a cada um dos termos, e uma árvore de termos (permitindo analisar de que forma os termos se relacionam entre si).

Por último, a ferramenta diz-nos quais os tópicos mais frequentes do conjunto de documentos. O nome *default* do tópico será o *top* cinco dos termos que mais aparecem em cada tópico. Cada tópico tem também a sua árvore de termos, dando assim uma noção dos termos englobados em cada tópico. Além disso, cada tópico tem a sua *Word Cloud,* que analisa os termos com mais ou menos peso.

Os documentos utilizados nas análises irão contemplar:

- Documentos de políticas de privacidade dos fornecedores de produtos IoT;
- Documentos de análise à privacidade dos produtos acima descritos, elaborados por analistas e utilizadores finais;
- Documentos de análise à privacidade na IoT por parte de consultoras líderes mundiais na área das TI;
- Documentos de análise à privacidade na IoT por parte do mercado em geral.

3.5.4. Participantes na investigação

Tal como na escolha das organizações a colocar o questionário, a escolha das organizações a serem analisadas pela ferramenta SAS Contextual Analysis teve como base vários critérios, entre os quais:

- Escolha de organizações fornecedoras de tecnologias IoT com bastante pegada no mercado e presentes em várias áreas do *Internet of Things Landescape (*figura 22*):*
  - **Corporates:** Apple, Atmel, Bosch, Dell, IBM, Intel, Microsoft, Oracle, SAP, Toshiba, Wind River;
  - **Personal Devices (Fitness)**: Fitbit, Garmin, Nike, Wahoo;
  - **Personal Devices (Health):** Lively, Withings;
  - **Personal Devices (Wearable Computing):** Pebble, Ringly;
  - **Personal Devices (Family):** Ovuline;
  - **Conneced Home (Automation):** Nest, Nestatmo, SmartThings.
- Escolha de consultoras presentes no ranking de 2015 da Vault[7] das consultoras de TI mais prestigiadas a nível global:
  - Accenture, Capgemini, Deloitte, Ernst & Young, KPMG, McKinsey & Company, PricewaterhouseCoopers Advisory Services LLC.
- Na reflexão às análises da privacidade dos dados nos produtos IoT, os analistas e análises escolhidas não obedeceram a um critério definido, tendo como único critério, o facto da análise estar relacionada com os produtos dos fornecedores IoT acima referenciado, sendo eles a Apple, Fitbit, Garmin, Nest, Netatmo, Nike, Pebble e a Samsung Smartthings.

[7] Ranking das melhores empresas consultoras nas mais diversas áreas. http://www.vault.com/company-rankings/consulting/best-firms-in-each-practice-area?sRankID=396

4. Atividades desenvolvidas

Este capítulo descreve todas as atividades desenvolvidas para a elaboração da dissertação, onde se incluem a análise aos resultados obtidos nos questionários submetidos a várias organizações presentes no mercado da IoT, bem como a descrição dos resultados obtidos pela análise a documento de privacidade dos dados na IoT.

4.1. Resultados obtidos – Questionários

A primeira etapa das atividades desenvolvidas na dissertação baseou-se na elaboração e apresentação de questionários com questões sobre a IoT e a respetiva privacidade dos dados, a várias organizações fornecedoras da área.

Wolcott (citado por Vale, 2004) revela três momentos fundamentais durante a fase de análise de dados: descrição, análise e interpretação. A descrição corresponde à escrita de textos resultantes dos dados originais registados pelo investigador. A análise é um processo de organização de dados, onde se devem salientar os aspectos essenciais e identificar factores chave. Por último, a interpretação diz respeito ao processo de obtenção de significados e ilações a partir dos dados obtidos.

Na mesma ordem de ideias, Miles e Huberman (citados por Vale, 2004) propõem um modelo de análise na investigação qualitativa que consiste em três momentos: a redução dos dados, a apzresentação dos dados e as conclusões e verificação. A redução dos dados diz respeito ao processo de seleccionar, simplificar e organizar todos os dados obtidos, durante a investigação. A apresentação dos dados refere-se ao momento em que a informação é organizada e compactada para assim o investigador poder ver rápida e eficazmente o que se passa no estudo. O terceiro e último momento corresponde à extracção de conclusões de toda a informação recolhida, organizada e compactada, que está dependente da quantidade de notas tiradas, dos métodos usados e, principalmente, da experiência do investigador neste campo.

Tomando como referência os três momentos referidos por Wolcott (2004) e, adequando-os ao presente estudo de investigação, pode-se referir que:

- A primeira fase, de redução dos dados, diz respeito à simplificação e organização de cada resposta do questionário, no caso das empresas que entregaram o questionário preenchido, de simplificação e organização da informação referentes à documentação fornecedia pelas restantes empresas;
- A segunda fase, de apresentação dos dados, refere-se à compactação e sumarização das respostas dos questionários, bem como à sumarização da documentação recebida e preenchimento dos questionários referentes às empresas que não o poderam preencher;
- A última fase, de extração de conclusões, diz respeito à análise das respostas dos questionários, por parte do investigador, de forma a retirar conclusões e padrões sobre elas.

4.1.1. Simplificação e organização das respostas dos questionários

Tal como referenciado no ponto 3.4.1., a escolha criteriosa das questões teve com base os seguintes critérios:

- Enquadramento com a área de atividade das organizações, no domínio da IoT
    a) Porque é que a IoT está a ter um elevado impacto global na sociedade;
    b) De que forma se está a dar o comportamento das organizações na IoT.
- Enquadramento com o panorama nacional
    c) Como está a correr o desenvolvimento da IoT em Portugal.
- Enquadramento com o tema principal da dissertação, a privacidade dos dados
    d) Qual a visão das organizações para a privacidade dos dados;
    e) Como está a decorrer o processo de adequar a privacidade dos dados dos utilizadores aquando do desenvolvimento dos produtos IoT por parte das organizações.

Com base nos critérios acima referidos, elaborou-se o questionário presente no Anexo 1:

- A Questão nº1 (Segundo dados divulgados pelo Gartner, 6,4 biliões de "coisas" conectadas estarão em uso até 2016, o que significa 30% a mais que em 2015. De que forma o(a) (nome da organização) está a ver este crescimento exponencial da Internet das Coisas? Já previam este boom da conectividade entre dispositivos) é uma questão genérica sobre a IoT, e portanto diz respeito ao critério **a)**;
- A questão nº2 (Na vossa opinião, Portugal está a fazer uma boa aposta na IoT? Se sim, quanto tempo acham que vai demorar até as Smart Cities serem uma realidade em Portugal?) é uma questão sobre o desenvolvimento da IoT em Portugal, estando enquadrada no critério **c)**;
- A questão nº 3 (De que forma o(a) (nome da organização) se está a posicionar em relação à IoT?) está enquadrada no critério **b)**, sobre o comportamento das organizações na IoT;
- A questão nº4 (De que forma os serviços e produtos de IoT do(a) (nome da organização) estão construidos de forma a garantir a privacidade do consumidor e a segurança dos seus dados?) está enquadrada com o critério **e)**, ou seja, com a forma como os produtos IoT da organização em questão garante a privacidade dos dados dos seus utilizadores.
- A questão nº5 (Quais são, no entendimento do(a) (nome da organização), os maiores desafios que os fornecedores de produtos IoT podem ter de forma a assegurar a privacidade e segurança dos dados dos seus clientes?) refere-se à visão da organização para a forma como estas vêm esta temática de implementação de medidas de segurança e privacidade no mundo fornecedor de produtos IoT, ou seja, ao critério **e)**.
- A questão nº6 (Testes realizados pela HP encontraram, em média, 25 vulnerabilidades em cada dispositivo IoT examinado. Os testes indicam que os dispositivos IoT examinados apresentaram ameaças como o *heartbleed* (divulgação dos dados do utilizador),

vulnerabilidade a ataques e grandes falhas nos processos de autorização de acesso, encriptação e construção de *interface*s. Acham que este irá ser um problema presente e futuro das IoT, ou apenas se deve ao facto de ser uma realidade recente, e por isso a segurança dos dispositivos ainda está por evoluir?) é uma questão sobre a realidade atual e futura da privacidade dos dados na IoT, dizendo então respeito ao critério **d)**.

- A questão nº7 (A principal questão sobre a privacidade na Internet das Coisas estará ainda por responder: quem atuará como fiscal sobre esse mercado?) diz respeito à visão da organização sobre a legislação da privacidade dos dados na IoT, ou seja, ao critério **d)**.

A primeira preocupação operacional relativa ao preenchimento do questionário dirigiu-se para a concepção e fiabilidade das questões, na confirmação de uma correcta abordagem do tema em ambiente organizacional. Seguiu-se-lhe o tempo de leitura e resposta para cada pergunta.

Em relação às empresas a quem o questionário foi direcionado, este foi realizado da seguinte forma:

- 3 foram feitos de modo presencial (nas instalações das organizações) – SAS, Oracle e Microsoft – O aluno reuniu-se com o responsável da área de IoT de cada uma destas empresas e apresentou o respetivo questionário (Ver anexos). Nos três casos, as respostas foram dadas de forma oral, tendo o aluno preenchido o questionário ao mesmo tempo que as respostas eram dadas. No caso do questionário ao responsável do SAS, a reunião foi gravada com autorização do mesmo;
- 2 que apesar de não preencherem o questionário por questões internas da própria organização, enviaram documentação oficial de suporte às questões, de modo a que o investigador a analise e posteriormente preencha as respostas do questionário conforme a sua capacidade de análise à documentação – HP e IBM.

4.1.2. Compactação e sumarização das respostas

Visto o foco desta dissertação ser a privacidade dos dados na IoT, optou-se por dar foco às respostas referentes às perguntas dos critérios d) e e), visto estas serem as questões referentes à privacidade dos dados, ou seja, as questões nº4, 5, 6 e 7.

As respostas às perguntas nº1, 2 e 3 (critério a), b) e c)) também serão analisadas, mas com um menor foco do que em relação às restantes questões.

- Referentemente ás questões do critério **a)** Questões genéricas sobre o impacto global da IoT, temos a questão nº1:

  Questão nº 1: Segundo dados divulgados pelo Gartner, 6,4 biliões de “coisas” conectadas estarão em uso até 2016, o que significa 30% a mais que em 2015. De que forma o(a) (nome da organização) está a ver este crescimento exponencial da Internet das Coisas? Já previam este boom da conectividade entre dispositivos?

O objetivo desta questão seria de enquadrar a organização com o tópico global da dissertação, que é a IoT.

Apenas o SAS, Microsoft e IBM responderam a estão questão, tendo como base de resposta os seus produtos IoT, e a forma como estes têm acompanhado passo a passo esta tendência, "transformadora", segundo o SAS.

- Referentemente ás questões do critério **b)** Questões sobre o comportamento das organizações na IoT, temos a questão nº3:
  Questão nº 3: De que forma o(a) (nome da organização) se está a posicionar em relação à IoT?

Com esta questão de resposta aberta, tal como todas as questões presentes no questionário, pretendia obter.

- Cada um dos fornecedores tem posicionado os seus produtos na IoT nas suas principais áreas de domínio. O SAS está posicionar os seus produtos IoT principalmente na vertente analítica, onde têm grande parte da quota de mercado. A Microsoft, por sua vez, além do Azure (software que recolhe informações de dispositivos), tem feito uma grande aposta na sua especidalidade, um sistema operativo que corre nos dispositivos IoT. A Oracle está a posicionar-se sobretudo no mundo *cloud*, "oferecendo a capacidade de analisar altos volumes de informações relacionadas à IoT, em tempo real, usando dispositivos conectados". Também a IBM está a fazer uma grande aposta nesta área da *cloud,* com o *Watson Internet of Things*, uma "parceria entre a IBM e a Cisco, que resultou numa solução de grandes capacidades de business analytics na *Cloud*". Por outro lado, dos fornecedores analisados, a HP é aquele que "oferece um dos portfólios mais abrangentes de soluções de computação da IoT".

- Referentemente ás questões do critério **c)** Questões sobre o desenvolvimento da IoT em Portugal, temos a questão nº2:
  Questão nº 2: Na vossa opinião, Portugal está a fazer uma boa aposta na IoT? Se sim, quanto tempo acham que vai demorar até as Smart Cities serem uma realidade em Portugal?

Esta questão tinha como objetivo obter a visão dos fornecedores sobre o posicionamento de Portugal em relação à temática da IoT.

Apenas se obteve resposta do SAS, Microsoft e IBM a esta questão. Em relação ao SAS, afirma que "Portugal tem feito alguns esforços e desenvolvido projetos nesta área mas de forma comparativa com outros países europeus está longe de estar a fazer uma boa aposta".

Já a Microsoft afirma que "as empresas em Portugal, estão a fazer um bom trabalho na implementação da realidade IoT no país". No seu caso, não se limitam apenas a fornecer produtos para utilizadores finais, mas também produtos corporativos.

Em relação à IBM, afirma que o seu "trabalho pioneiro na área de Smarter Planet e de Smarter

Cities baseava-se já nas aplicações práticas da IoT e levou ao desenvolvimento de soluções que ajudassem a reduzir a criminalidade, a minimizar o risco no trabalho diário dos bombeiros ou a monitorizar a qualidade da água".

- Em relação às questões do critério **d)** "Questões acerca da visão das organizações para a privacidade dos dados", temos a questão nº6 que a seguir se transcreve:
  Questão nº 6: Testes realizados pela HP encontraram, em média, 25 vulnerabilidades em cada dispositivo IoT examinado. Os testes indicam que os dispositivos IoT examinados apresentaram ameaças como o heartbleed (divulgação dos dados do utilizador), vulnerabilidade a ataques e grandes falhas nos processos de autorização de acesso, encriptação e construção de *interface*s. Acham que este irá ser um problema presente e futuro das IoT, ou apenas se deve ao facto de ser uma realidade recente, e por isso a segurança dos dispositivos ainda está por evoluir?

Com esta questão de resposta aberta, tal como todas as questões presentes no questionário, pretendia obter-se a visão das organizações fornecedoras sobre o panorama atual e futuro da privacidade dos dados na IoT, e sobre a possibilidade de evolução contínua dos mecanismos de proteção da segurança e privacidade dos consumidores.

Das cinco organizações de estudo, três delas responderam a esta questão, tendo sido o SAS, Microsoft e IBM. Da análise à resposta de cada organização a esta questão, pode-se concluir que abordam dois pontos em comum: 1) Atualmente os consumidores dão mais importância ao preço e qualidade de um produto IoT do que propriamente à segurança e privacidade dos dados desse mesmo produto. 2) À medida que o preço da segurança e da privacidade for diminuindo, e a facilidade em garantir esses mesmos fatores, os produtos IoT irão ter um paralelismo entre o preço/qualidade/segurança

- Outra das questões do critério **d)** "Questões acerca da visão das organizações para a privacidade dos dados" é a questão nº7 que a seguir se transcreve:
  Questão nº 7: A principal questão sobre a privacidade na Internet das Coisas penso que ainda estará por responder: quem atuará como fiscal sobre esse mercado?

Com esta questão pretendia-se obter a visão da organização sobre a legislação da privacidade dos dados na IoT, e se a legislação irá tornar os consumidores mais seguros e com mais confiança nos produtos IoT, visto a legislação, por norma, implicar multas a quem não as cumprir.

Apenas duas organizações responderam a esta questão, tendo sido o SAS e a Microsoft, duas das empresas cujo questionário foi efetuado de forma presencial. Isto significa que, segundo a documentação oficial enviada pela IBM e HP, esta preocupação com a legislação poderá não ser ainda, uma realidade. O SAS e a Microsoft têm respostas um pouco dispâras, tendo o SAS uma opinião mais elaborada. Na sua opinião, quem "legislará deverá ser sempre a autoridade máxima de regulação do ambiente onde os dados estão a ser tratados e ou utilizados, no nosso caso a União Europeia, e quem cuidará da aplicabilidade dessa regulamentação serão os diferentes organismos locais, no nosso caso a

CNPD, ANACOM etc.", ou seja, tal como vimos no ponto 2.5.1., o Conselho Europeu prepara-se para aprovar um regulamento geral de proteção de dados que entrará em vigor em 2017. Na opinião do SAS a garantia da aplicabilidade desta regulamentação será feita por organismos de regulamentação portugueses, tais como a Comissão Nacional de Proteção de dados (CNPD) e a Autoridade Nacional de Comunicações (ANACOM).

Já a Microsoft tem uma opinião mais vaga em relação a este assunto, não abordando entidades reguladoras, mas sim dando o exemplo da regulação na Internet "Quem atua como fiscal na Internet? A resposta a esta pergunta passa muito por aí".

- Em relação às questões do critério **e)** "Questões sobre a atenção dada à privacidade dos dados dos utilizadores aquando do desenvolvimento dos produtos IoT por parte das organizações" é a questão nº4 que a seguir se transcreve:
  Questão nº 4: De que forma os serviços e produtos de IoT do(a) (nome da organização) estão construidos de forma a garantir a privacidade do consumidor e a segurança dos seus dados?

Esta é uma questão pertinente por se enquadrar perfeitamente no tema central da dissertação, e questiona às organizações se os seus produtos IoT realmente estão concebidos de origem para garantir a privacidade dos dados dos seus consumidores.

A esta questão, tal como aconteceu na questão nº7, só se obteve resposta das organizações cujo questionário foi efetuado de forma presencial. Desta vez tanto o SAS, como a Microsoft, como a Oracle responderam a esta questão.

O SAS garante ter dado "uma preocupação particular a todos os aspetos associados à encriptação" tal como a garantia de que os ambientes SAS garantem a segurança dos dados e acessos dos seus utilizadores. Em relação à Microsoft, esta assenta em quatro grandes pilares de valores para com os seus clientes: Segurança (ao nível do dispositivo, em trânsito e em repouso), Privacidade, Compliance (certificação nas mais diversas normas de compliance tais como a ISO 27001, EUMC, HIPAA), Transparência (dos serviços prestados). Já a Oracle, controla a segurança e privacidade de "todo o ciclo de vida de todos os pontos finais e dispositivos conectados" através do Oracle IoT Cloud Service. Também garante mecanismos exclusivos de autenticação, além de todas as mensagens serem encriptadas usando HTTPS.

- Outra das questões do critério **e)** "Questões sobre a atenção dada à privacidade dos dados dos utilizadores aquando do desenvolvimento dos produtos IoT por parte das organizações" é a questão nº5 que a seguir se transcreve:
  Questão nº 5: Quais são, no entendimento do(a) (nome da organização), os maiores desafios que os fornecedores de produtos IoT podem ter de forma a assegurar a privacidade e segurança dos dados dos seus clientes?

Esta é outra questão que pretende esclarecer a forma como a privacidade dos dados é garantida pelos fornecedores na conceção dos seus produtos, mas neste caso sobre os desafios e dificuldades que estes possam ter a garantia completa da privacidade dos dados dos consumidores.

Em relação à opinião do SAS a esta temática, fazem questão de esclarecer que a correta e eficiente normalização e legislação do mercado IoT é um dos maiores desafios do mercado. Já a Microsoft é da opinião que a encriptação é o maior desafio para os fornecedores de produtos IoT. Já a IBM vê este tema de uma forma mais genérica, realçando que "a segurança e privacidade dos dados dos consumidores devem ter em atenção duas perspetivas: a dos fabricantes das coisas – o *design* e construção de produtos e sistemas IoT seguros; dos operadores das coisas – a utilização correta e segura dos produtos ou sistemas IoT implementados", ou seja, vêm sobre essas duas perspetivas os maiores desafios dos fornecedores de produtos IoT. A HP, tal como a IBM vê os principais desafios da IoT sobre os prismas consumidor e fabricante. Em relação ao consumidor, a HP afirma que os mesmos "devem ser cuidadosos em relação à adoção de medidas que parecem simples e práticas". Já no prisma fabricante, a HP realça que "os fabricantes dos dispositivos devem assumir a responsabilidade de integrar a segurança dos seus produtos, de forma a evitar expor os seus clientes a sérias ameaças.

4.1.3. Análise das respostas

Com base nas respostas obtidas às perguntas dos questionários, obteve-se as seguintes conclusões:

- Pela análise às respostas da Questão nº6, podemos concluir que atualmente os consumidores dão mais importância ao preço do produto IoT do que propriamente à qualidade da segurança e privacidade que este apresente, e que à medida que o preço da segurança e da privacidade for diminuindo, os produtos IoT irão ter um paralelismo entre o preço, qualidade e segurança;
- Segundo as respostas à Questão nº7, ainda não existe uma preocupação relativamente assente em relação à legislação em vigor, por parte das organizações. Visto as empresas analisadas estarem sediadas nos EUA, neste país a legislação na IoT ainda não é uma preocupação, pois segundo eles, a IoT ainda está numa fase muito prematura para ser legislada;
- Todas as organizações assumem que os seus produtos garantem que a segurança e privacidade dos dados dos consumidores foi uma preocupação garantida desde o zero, ou seja, desde a fase inicial da concepção de cada produto IoT. É a conclusão que se obteve através da análise às respostas da Questão nº4;
- Em relação à Questão nº5, que aborda aos maiores desafios que as organizações fornecedoras de produtos IoT têm neste momento, as organizações analisadas apresentam perspetivas distintas. Umas sentem que o maior desafio é a encriptação, outras a legislação, e outras vêm sobre dois prismas de desafios: "Consumidor e fornecedor".

4.2. Resultados obtidos – Análise de documentos de privacidade de dados na IoT

A segunda etapa das atividades desenvolvidas baseou-se na análise de documentos de privacidade de dados na IoT, através do software *SAS Contextual Analyis*.

De acordo com a metodologia detalhada no ponto 3.5, foram quatro as análises efetuadas isoladamente, sendo elas:

1. Fornecedores de produtos IoT – Análise às políticas de privacidade dos produtos;
2. Fornecedores de produtos IoT – Análise à privacidade de dados dos produtos através de análises de analistas e utilizadores desses mesmos produtos;
3. Consultoras de TI – Análises á privacidade de dados na IoT por parte das consultoras de TI com maior prestígio;
4. Público geral – Análises à privacidade de dados na IoT por parte do mercado e público geral.

4.2.1. Descrição detalhada das etapas seguidas para a construção das análises

Para a construção das análises acima descritas foram seguidas as seguintes etapas:

1. Recolha dos documentos pdf através do motor de busca *www.google.pt,* e disposição dos mesmos em pastas diferentes, consoante o tipo de análise a que lhes irão ser atribuídos (figura 23). Caso seja um documento de política de privacidade de um produto de um fornecedores é atribuído a pasta “SCA – Fornecedores IoT”, caso seja um documento de análise à privacidade dos produtos dos fornecedores é atribuído a pasta “SCA – Fornecedores IoT – Análise”, caso seja um documento de análise das consultoras à privacidade dos dados na IoT é atribuído a pasta “SCA – Consultoras”, e caso seja um documento de análise do público geral à privacidade dos dados na IoT é atribuído a pasta “SCA – Geral” (figura 29).

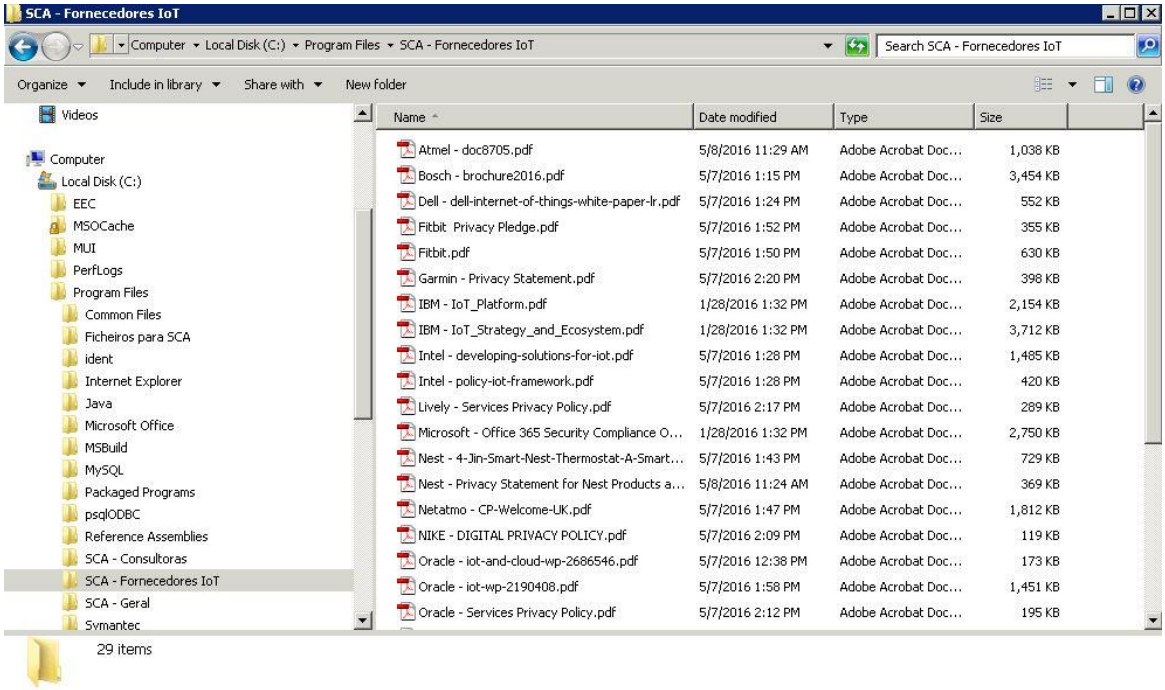

Figura 29. Organização de documentos para análises no SCA
Fonte: Elaborado pelo autor

2. Na solução SAS Contextual Analysis é criado um novo projeto consoante a análise que se pretende. No caso da figura 30, pretendeu-se analisar as políticas de privacidade dos fornecedores IoT, escolhendo a linguagem dos documentos (inglês) e aplicando um *Sentimental Model default* (modelo estatístico que atribui um sentimento (positivo, negativo ou neutro) a uma determinada expressão).

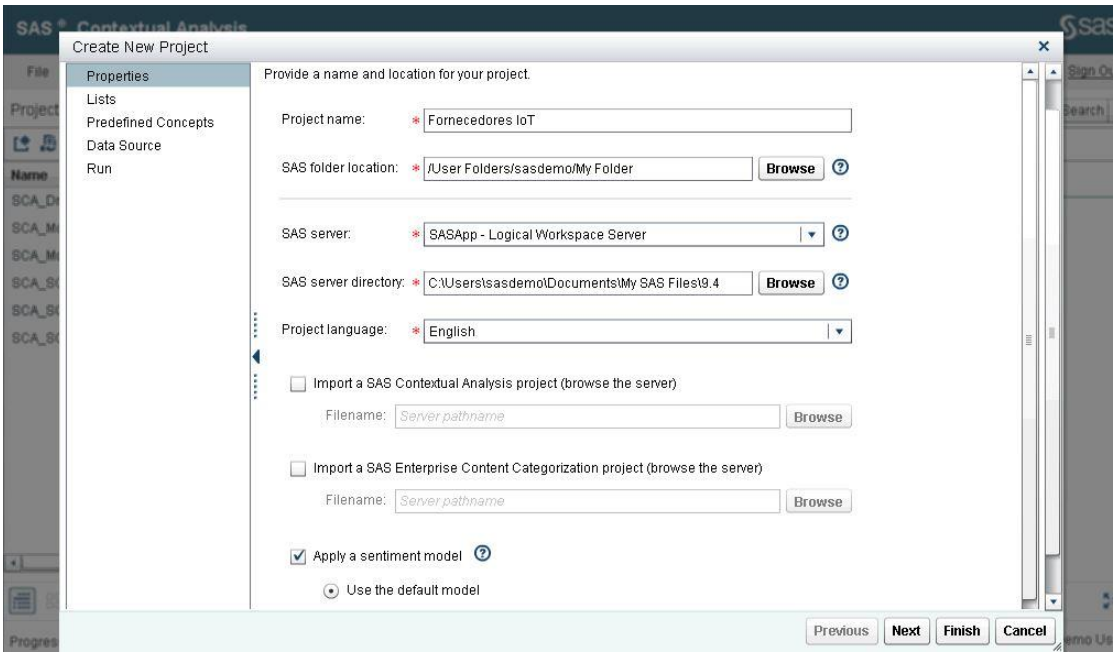

Figura 30. Criação de um novo projeto no SCA
Fonte: Elaborado pelo autor

3. De seguida, é definida uma *Stop List* para o projeto (uma tabela que contêm um conjunto de palavras a remover das análises (figura 31).

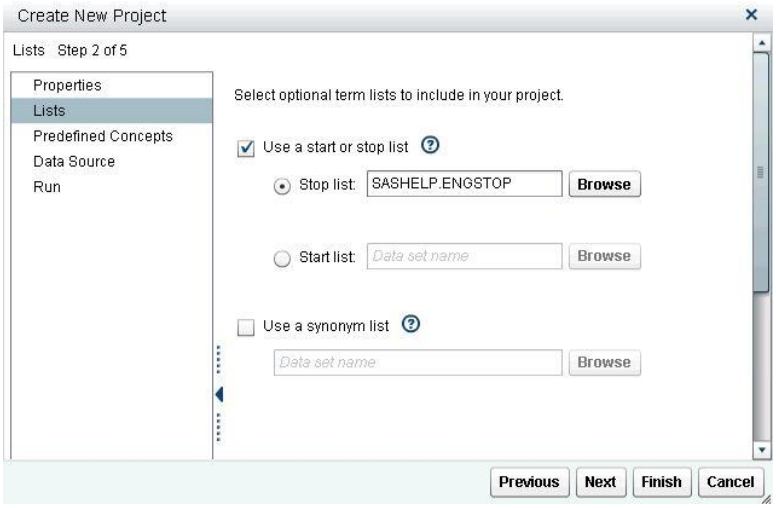

Figura 31. Criação de um novo projeto no SCA – Listas
Fonte: Elaborado pelo autor

4. Após isso, são incluídos um conjunto de conceitos predefinidos (figura 32), sendo eles: “Address”, “Company”, “Currency”, “Date”, “Internet”, “Location”, “Measure”, “Organization”, “Percent”, “Person”, “Phone”, “Prop_misc”, “Ssn” e “Time_Period”.

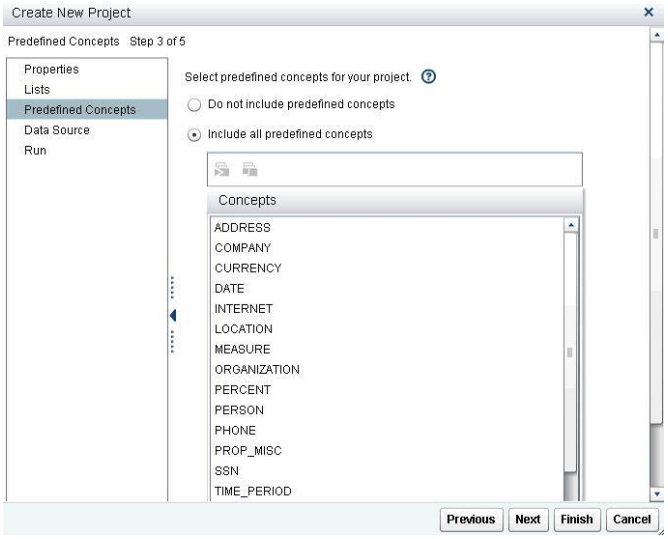

Figura 32. Criação de um novo projeto no SCA - Conceitos predefinidos
Fonte: Elaborado pelo autor

5. É escolhida a diretoria que contêm os ficheiros a analisar no projeto. Tal como falado no ponto 1., os documentos estão divididos em várias pastas, consoante o grupo a que pertencem. Neste caso específico, como se quer analisar as políticas de privacidade dos produtos dos fornecedores IoT, a direitoria escolhida é a “SCA – Fornecedores IoT” (figura 33).

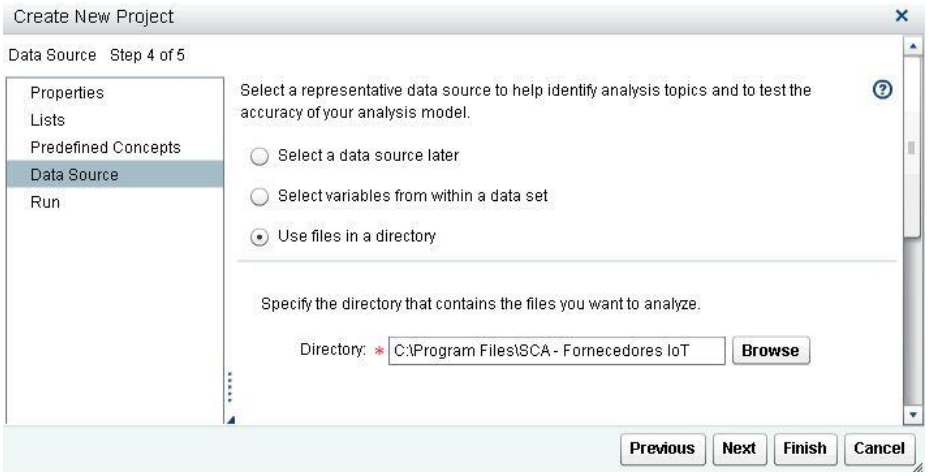

Figura 33. Criação de um novo projeto no SCA - Data Source
Fonte: Elaborado pelo autor

6. Por último, o SAS Contextual Analysis corre o projeto e analisa os ficheiros (figura 34):

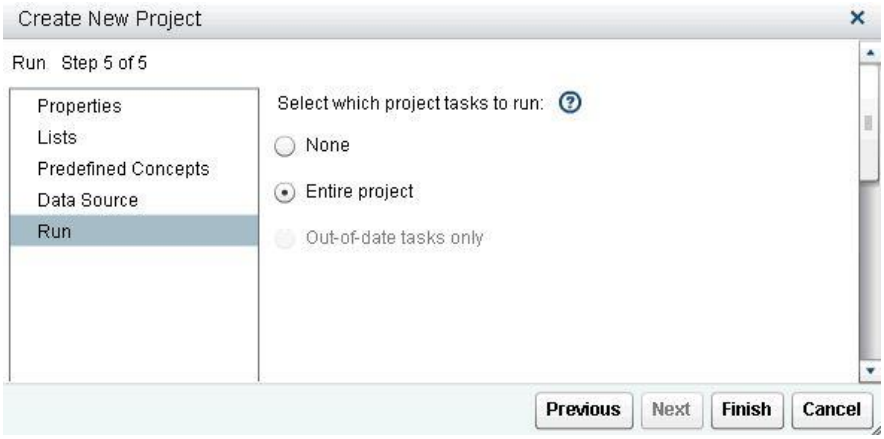

Figura 34. Criação de um novo projeto no SCA - Run
Fonte: Elaborado pelo autor

4.2.2. Fornecedores IoT – Análise às políticas de privacidade dos produtos IoT

A primeira análise efetuada diz respeito à análise das políticas de privacidade dos produtos de fornecedores IoT. Tal como referenciado no ponto 3.5.4., foram vários os participantes na investigação escolhidos, entre os quais organizações de renome no mercado das TI, que fizeram grandes investimentos na IoT, mas também *start-ups* que se dedicam a um nicho específico do mercado IoT.

Da recolha das políticas de privacidade destas organizações, surgiram 25 documentos. Como detalhado na figura 35, foram encontrados 8765 termos e 4 tópicos nesse conjunto de documentos.

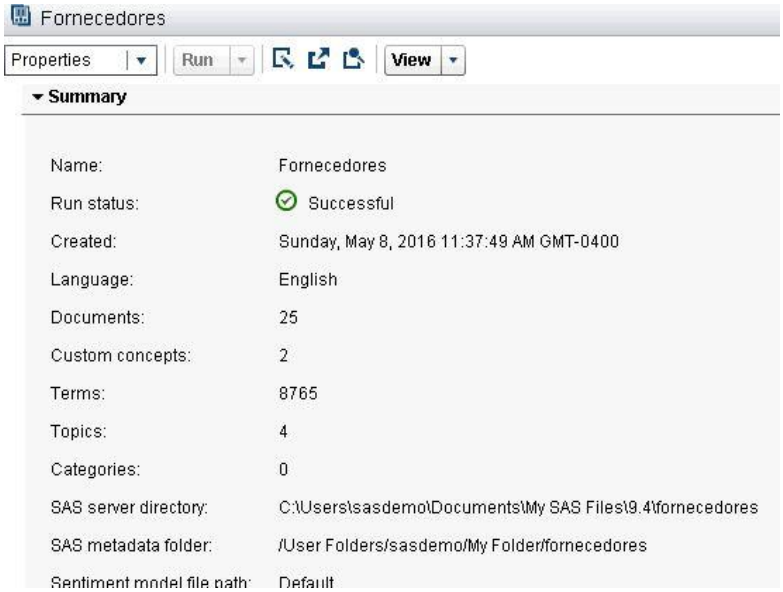

Figura 35. Análise às Políticas de Privacidade dos fornecedores - Propriedades
Fonte: Elaborado pelo autor

4.2.2.1. Análise de conceitos

Em relação à análise de conceitos, para além dos conceitos predefinidos pelo *software (*"Address", "Company", "Currency", "Date", "Internet", "Location", "Measure", "Organization", "Percent", "Person", "Phone", "Prop_misc", "Ssn" e "Time_Period"), e referenciados no ponto 4.2.1., foram criado dois conceitos customizados (figura 36 e 37), sendo eles:

1. O conceito de "IoT", que abrange as expressões "IoT" e "Internet of Things" (visto todos os documentos estarem em inglês) (figura 36). A escolha deste conceito deve-se ao facto da IoT ser o ponto central da dissertação.
2. O conceito de "Privacidade", que abrange as expressões "Consent" (consentimento em português), "User Control" (controlo por parte do utilizador), "Anonymous" (anónimo), "Freedom of Choice" (liberdade de escolha), "User Consent Acquisition" (aquisição do consentimento do utilizador), "Anonymity (anonimato), "Identity Privacy Protection" (proteção da privacidade da entidade), "Confidentiality" (confidencialidade), "Data Privacy" (privacidade dos dados), "Authorization" (autorização) e "Personal Information" (Informação pessoal) (figura 37). A escolha do conceito "Privacidade" deveu-se ao facto – tanto facto de este, tal como o conceito "IoT", ser o principal tema de estudo de toda a dissertação. A escoha das suas expressões subsequentes deveu-se ao facto de estas serem algumas das expressões e termos mais utilizados quando se fala de privacidade na IoT, tal como foi possível veriricar através de uma breve leitura dos documentos a serem analisados mais à frente pelo *software*, tal como foi possível verificar no ponto 2., do enquadramento teórico, e tal como será possível verificar na análise de termos efetuada mais à frente (pontos 4.3.1.2., 4.3.2.2., 4.3.3.2.).

Ou seja, sempre que o *software* encontrar as expressões acima referenciadas, vai associar aos respetivos conceitos customizados. Por exemplo, quando o *software* encontrar a expressão “Data Privacy” vai associar ao conceito “Privacidade”.

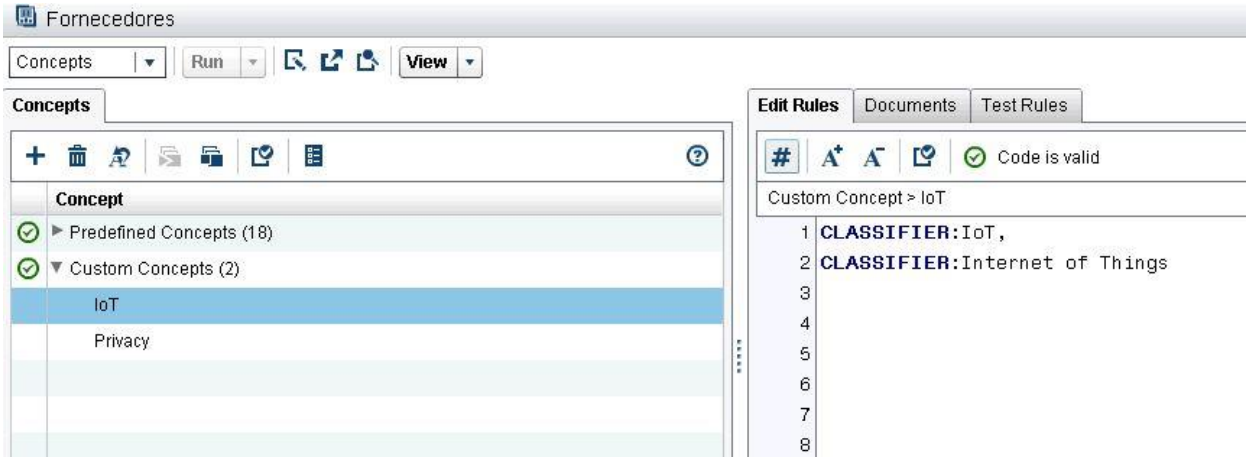

Figura 36. Análise às Políticas de Privacidade dos fornecedores - Conceitos customizados – IoT
Fonte: Elaborado pelo autor

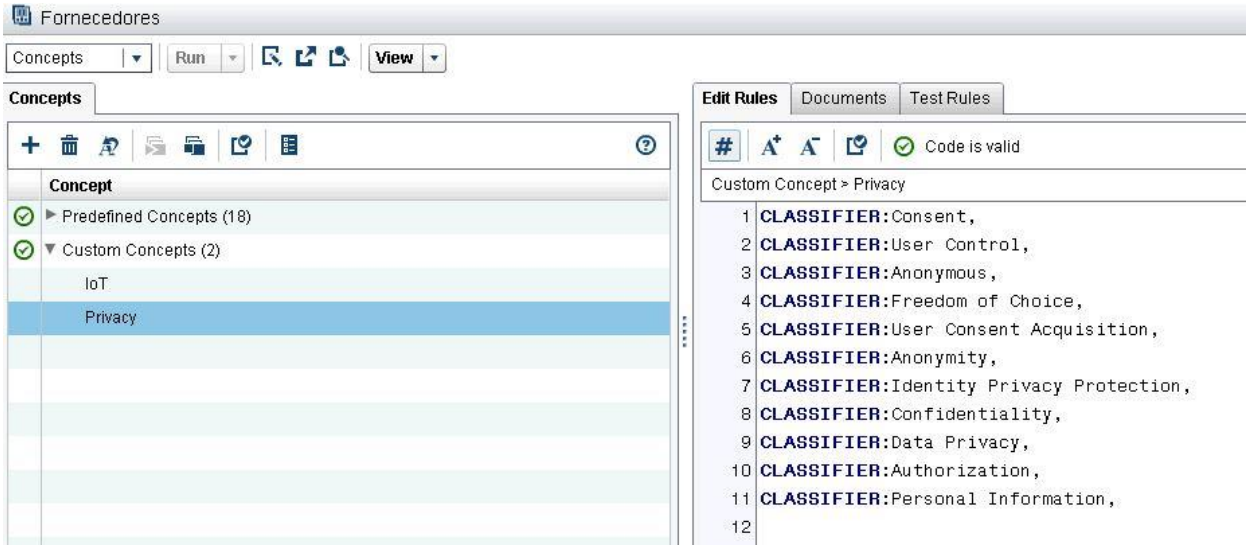

Figura 37. Análise às Políticas de Privacidade dos fornecedores - Conceitos Customizados – Privacy
Fonte: Elaborado pelo autor

De seguida, o *software* procurou em todos os documentos por cada expressão dos conceitos acima explicados, e atribuiu um sentimento (conotação) positivo, negativo ou neutro, dependendo do contexto onde a expressão é referenciada.

Tal como ilustrado na figura 38, as expressões referentes ao termo “IoT” foram encontradas em 3 documentos, sempre com um sentimento positivo, obtendo um pontuação de 100% positivo. Isto significa que nas suas políticas de privacidade de produtos IoT, os fornecedores encaram com positivismo a Internet das Coisas.

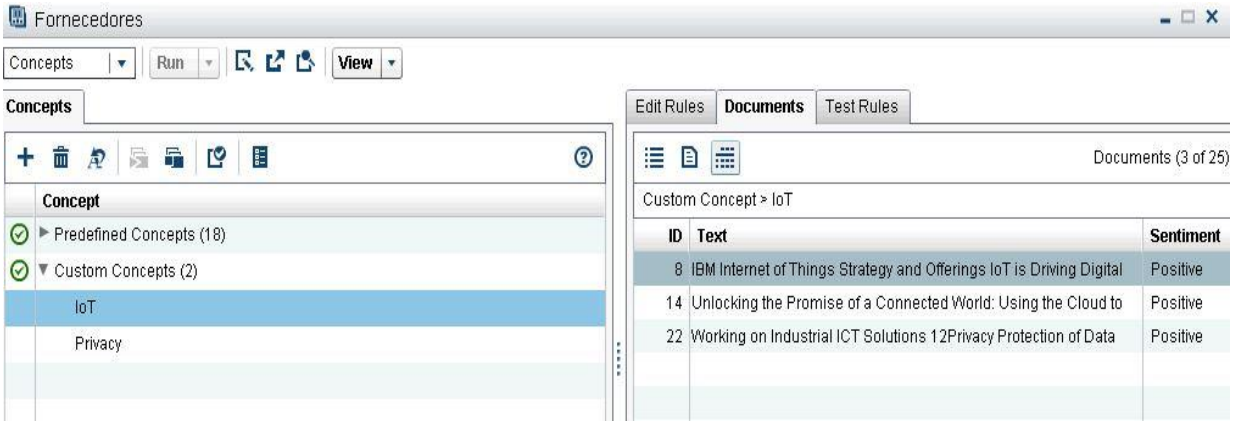

Figura 38. Análise às Políticas de Privacidade dos fornecedores – Conceitos customizados - Análise de sentimentos IoT
Fonte: Elaborado pelo autor

Em relação ao conceito "Privacy", como mostram as figuras 39 e 40, as suas expressões foram encontradas em 21 dos 25 documentos, e obtiveram 15 sentimentos positivos (71%), 4 sentimentos negativos (19%) e 2 sentimentos neutros (10%). Visto existir uma grande diferença entre os sentimentos positivos e negativos, isto significa que os fornecedores vêm com muito positivismo e segurança a privacidade dos dados nos seus produtos IoT, passando essa imagem aos utilizadores desses mesmos produtos.

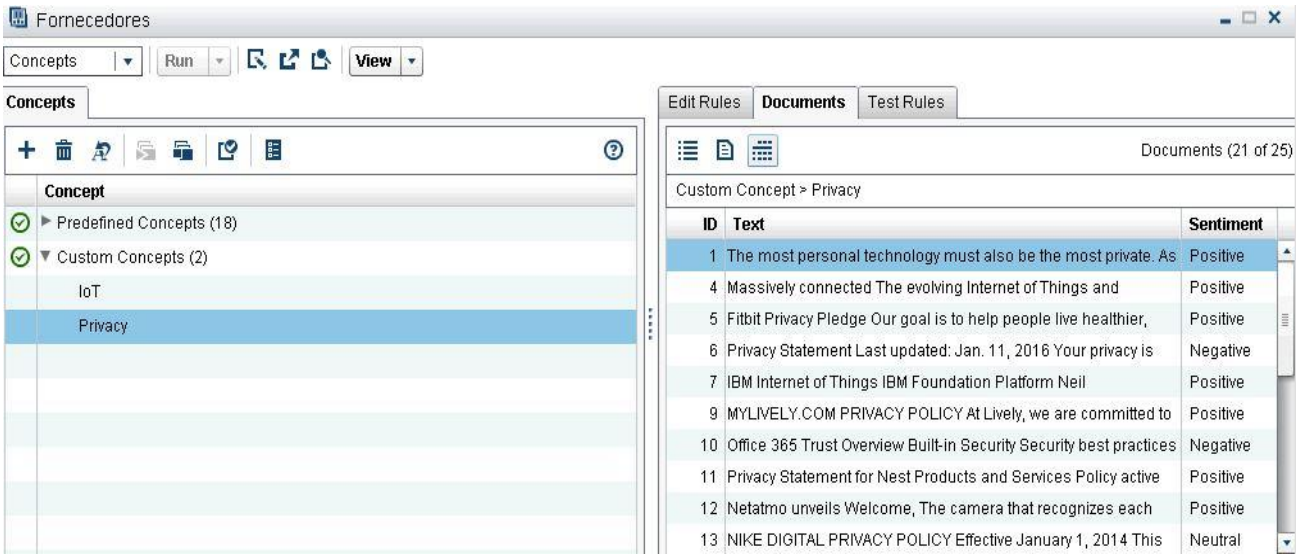

Figura 39. Análise às Políticas de Privacidade dos fornecedores – Conceitos customizados - Análise de sentimentos Privacy
Fonte: Elaborado pelo autor

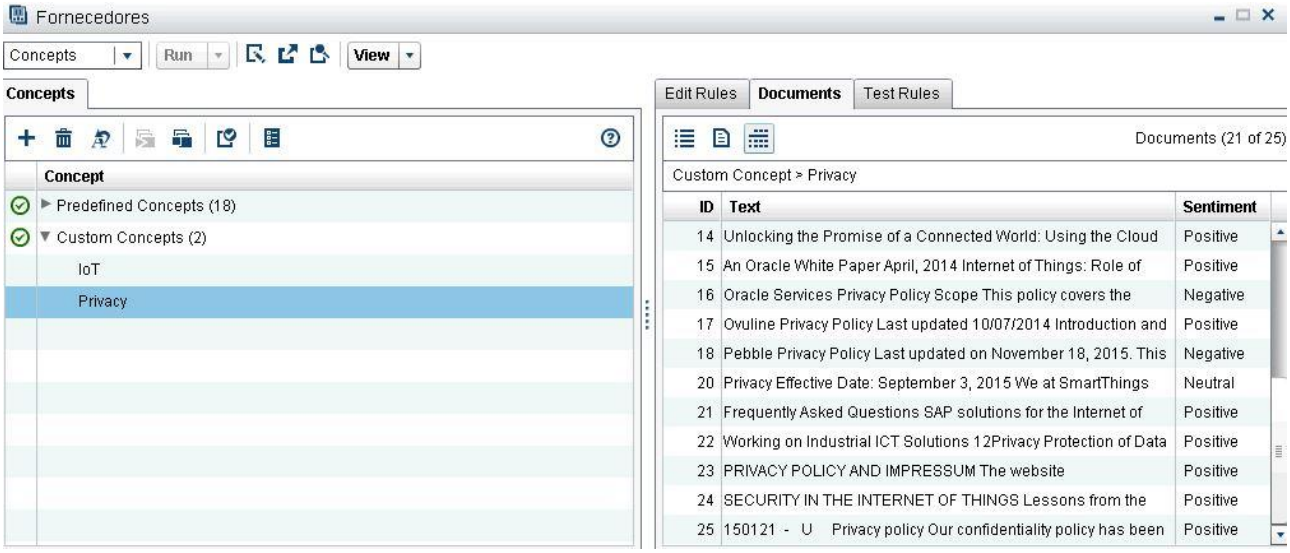

Figura 40. Análise às Políticas de Privacidade dos fornecedores – Conceitos customizados - Análise de sentimentos Privacy
Fonte: Elaborado pelo autor

A tabela 4 e o gráfico 1 mostra um resumo dos resultados obtidos pela análise dos conceitos.

Conceitos – Políticas de privacidade de dados de fornecedores IoT		
	IoT	**Privacy**
Sentimentos positivos	3	15
Sentimentos negativos	0	4
Sentimentos neutros	0	2
%Sentimentos positivos	100%	71%
%Sentimentos negativos	0%	19%
%Sentimentos neutros	0%	10%

Tabela 4. Análise às Políticas de Privacidade dos fornecedores - Conceitos customizados - Análise de sentimentos - Tabela
Fonte: Elaborado pelo autor

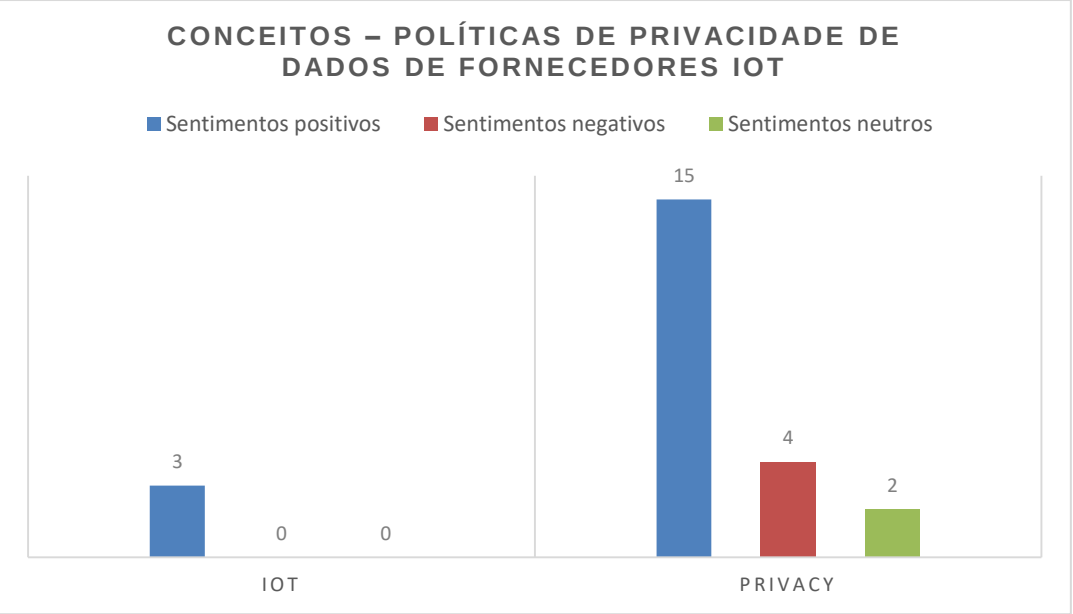

Gráfico 1. Análise às Políticas de Privacidade dos fornecedores - Conceitos customizados - Análise de sentimentos - Gráfico
Fonte: Elaborado pelo autor

Visto a pontuação dos sentimentos positivos do conceito "IoT" ser de 100%, significa que nas suas políticas de privacidade de produtos IoT, os fornecedores encaram com positivismo a Internet das Coisas. Em relação ao conceito "Privacy", visto existir uma grande diferença entre os sentimentos positivos e negativos, isto significa que os fornecedores vêm com muito positivismo e segurança a privacidade dos dados nos seus produtos IoT, passando essa imagem aos utilizadores desses mesmos produtos.

4.2.2.2. Análise de termos

Tal como vimos no ponto 4.2.2., o *software* encontrou 8765 termos. A figura 41 ilustra quais os termos que aparecem mais vezes no conjunto dos 25 documentos.

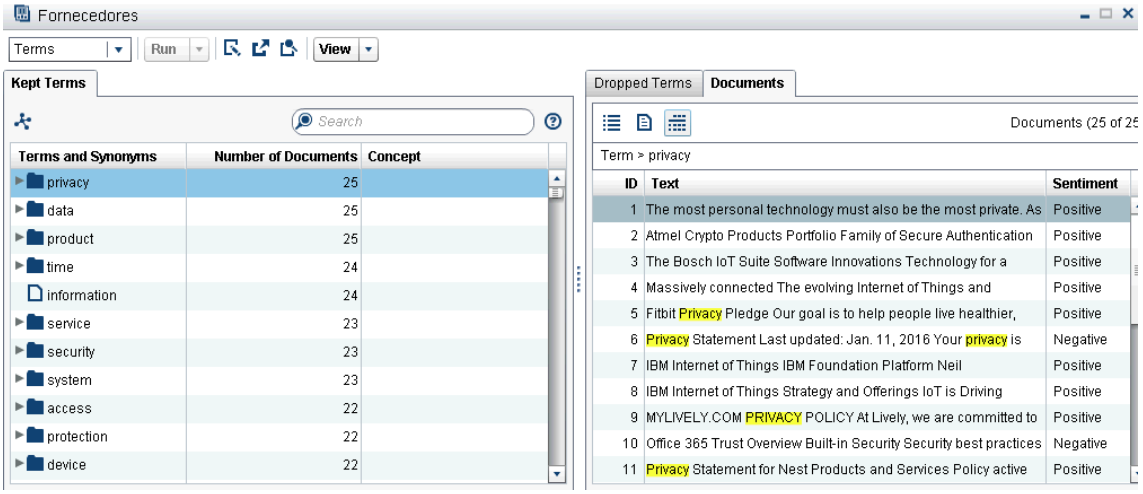

Figura 41. Análise às Políticas de Privacidade dos fornecedores – Termos
Fonte: Elaborado pelo autor

A tabela 5 e o gráfico 2 resumem a análise de sentimento dos 10 termos mais repetidos (“Privacy”, “Data”, “Product”, “Information”, “Service”, “Security”, “System”, “Access”, “Protection”, “Device”), onde foi descartado o termo “time” visto não ser um termo enquadrado com o tema de estudo da dissertação:

Termos – Políticas de privacidade de dados de fornecedores IoT										
	Privacy	**Data**	**Product**	**Information**	**Service**	**Security**	**System**	**Access**	**Protection**	**Device**
Sentimentos positivos	18	18	22	18	20	16	17	15	16	17
Sentimentos negativos	5	5	2	4	2	6	4	5	4	3
Sentimentos neutros	2	2	1	2	1	1	2	2	2	2
Total	25	25	25	24	23	23	23	22	22	22
%Sentimentos positivos	72%	72%	88%	75%	87%	70%	74%	68%	78%	77%
%Sentimentos negativos	20%	20%	8%	17	9%	22%	17%	23%	18%	14%
%Sentimentos neutros	8%	8%	4%	8	4%	9%	9%	9%	9%	9%

Tabela 5. Análise às Políticas de Privacidade dos fornecedores – Termos – Top 10 - Tabela
Fonte: Elaborado pelo autor

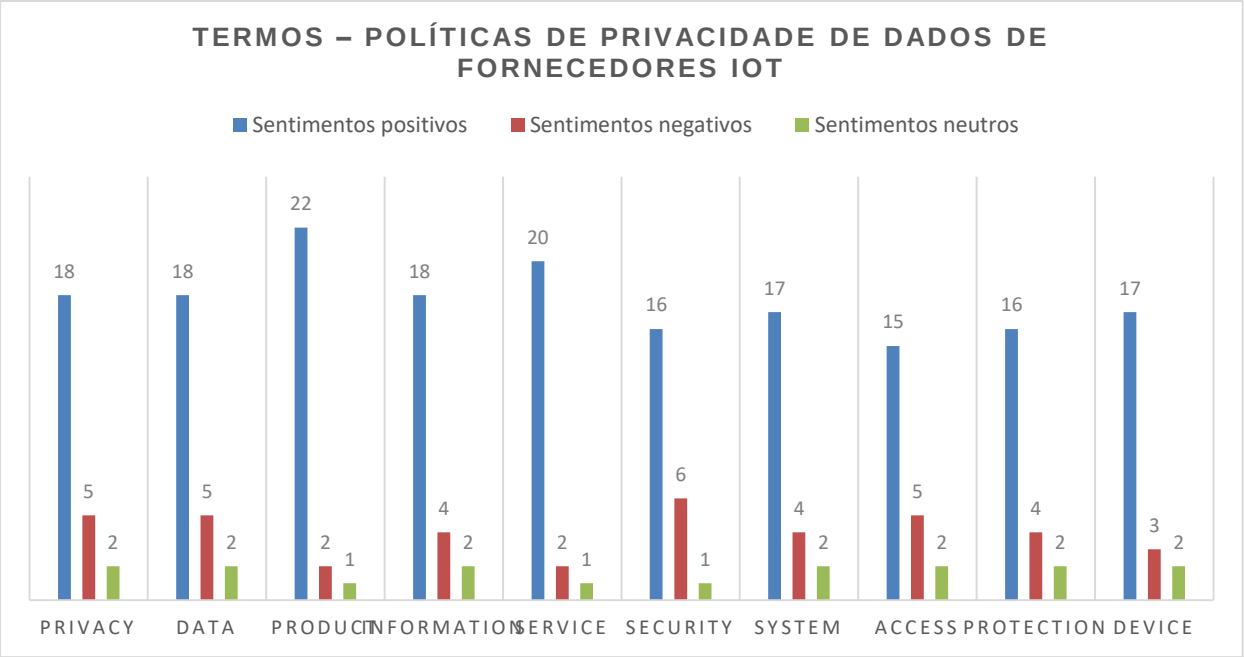

Gráfico 2. Análise às Políticas de Privacidade dos fornecedores – Termos – Top 10 – Gráfico
Fonte: Elaborado pelo autor

Pela análise da tabela 5 e do gráfico 2, conclui-se que todos os termos têm um cariz maioritariamente positivo, tendo o termo “Product” sido aquele que teve a maior percentagem de sentimentos positivos e a menor percentagem de sentimentos negativos. O termo central desta dissertação, “Privacy”, tal como no ponto 4.2.2.1., em que se analisou o conceito “Privacy” e as suas expressões associadas, obteve uma grande percentagem de sentimentos positivos (72%) e uma baixa percentagem de sentimentos negativos (20%), percentagens estas bastante idênticas às verificadas na análise do conceito customizado “Privacy” no ponto anterior.

Com isto podemos concluir que, nas suas políticas de privacidade, os fornecedores de produtos IoT atribuem um elevado grau de privacidade (72% positivo), segurança (70% positivo) e proteção (78% positivo) dos dados (72% positivo) dos seus utilizadores, garantindo também um acesso (68% positivo) relativamente seguro.

O *software* permite-nos também ter uma noção de quais os termos que têm relação com os termos principais, ou seja, quando esses termos aparecem, há uma forte probabilidade de os termos principais aparecerem também. A figura abaixo (figura 42) mostra a árvore de termos do tema principal “Privacy”. O tamanho da bola representa o grau de relação desse termo com o termo “Privacy”.

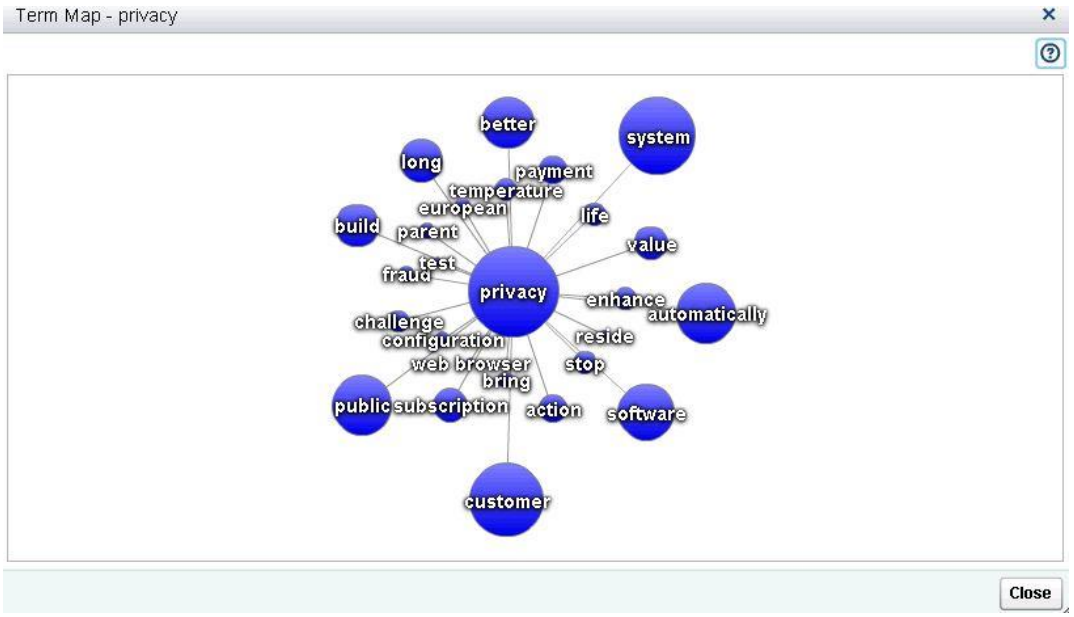

Figura 42. Análise às Políticas de Privacidade dos fornecedores – Termos – *Term map*
Fonte: Elaborado pelo autor

Da análise da árvore, podemos concluir que os termos mais correlacionados com o termo “Privacy” são “System”, “*Software*”, “Public”, “Customer” e “Automatically”. Ou seja, quando estas palavras aparecem no texto, há uma forte probabilidade de o termo “Privacy” aparecer também.

4.2.2.3. Análise de tópicos

Por último, na análise de tópicos. Os tópicos são gerados automaticamente e têm como finalidade

indicar quais os principais assuntos encontrados na coleção de documentos analisada. Cada tópico é identificado pelos seus 5 termos mais importantes e comuns (figura 43).

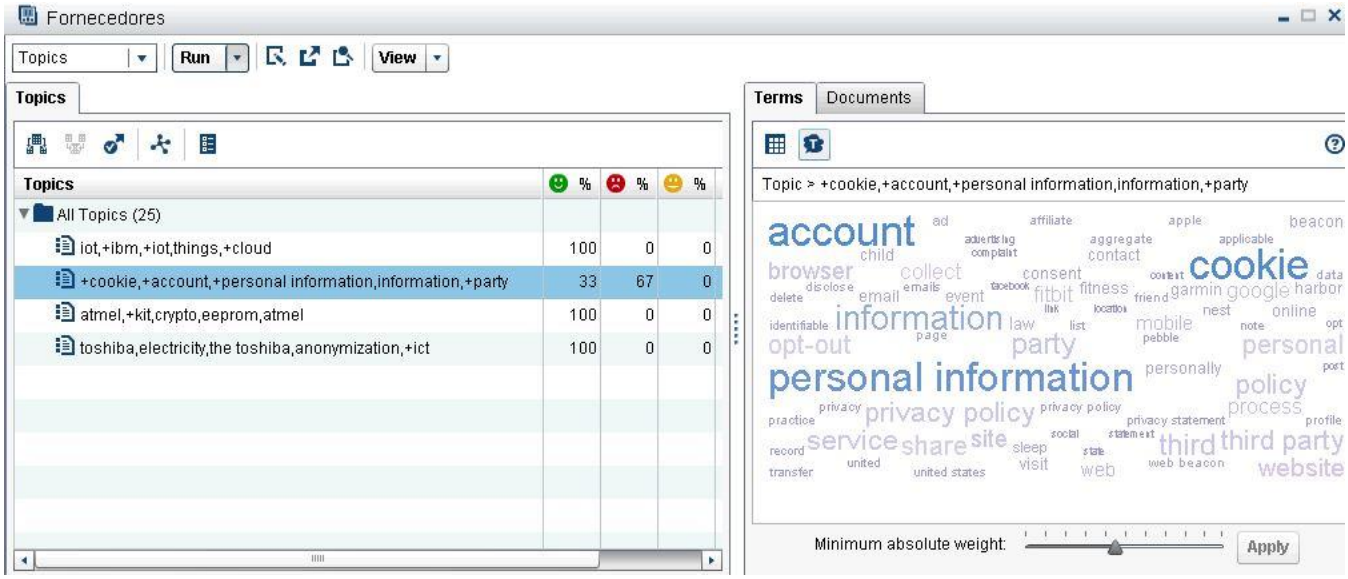

Figura 43. Análise às Políticas de Privacidade dos fornecedores – Tópicos
Fonte: Elaborado pelo autor

Através da análise da figura 43, podemos concluir que foram encontrados 4 tópicos principais em toda a coleção de documentos analisada. Dos 4 tópicos encontrados, 3 deles têm uma conotação 100% positiva, ao contrário do restante, o tópico formado pelos termos “cookie”, “account”, “personal information”, “information” e “party”. Este tópico apresentou 33% de conotação positiva e 67% de conotação negativa.

4.2.3. Fornecedores IoT – Análise a documento de análise da privacidade de dados de produtos IoT efetuadas por analistas

Relativamento à segunda análise, esta diz respeito às análises à privacidade de dados de produtos IoT efetuadas por analistas. Cada análise diz respeito a um produto de um fornecedor analisado no ponto anterior (4.2.2.).

Esta análise tem como objetivo fazer uma comparação com os resultados obtidos na análise às políticas de privacidade dos fornecedores IoT (4.2.2.). Podemos assim comparar se as práticas e suposições de privacidade que os fornecedores descrevem nas suas políticas de privacidade são realmente uma realidade. Tal como referenciado no ponto 3.5.4., foram vários os participantes escolhidos para a investigação, tendo os analistas e análises escolhidas não obedecido a um critério definido, tendo como único critério, o facto da análise estar relacionada com os produtos dos fornecedores IoT acima referenciados.

Da recolha das análises da privacidade dos produtos dos fornecedores, surgiram 8 documentos (o que corresponde a 8 dos fornecedores referenciados nos pontos 3.5.4. e 4.2.2, sendo eles a Apple, Fitbit, Garmin, Nest, Netatmo, Nike, Pebble e a Samsung Smartthings). Como descrito na figura 44, foram

encontrados 2532 termos e nenhum tópico nesse conjunto de documentos, visto não ter encontrado qualquer relação de tópicos entre os documentos.

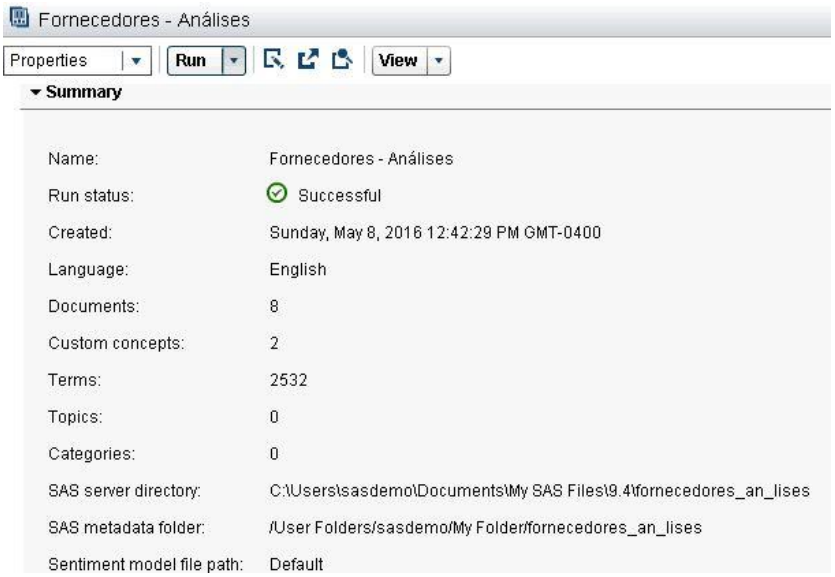

Figura 44. Análise a documentos de análise de produtos IoT – Propriedades
Fonte: Elaborado pelo autor

4.2.3.1. Análise de conceitos

Na análise de conceitos, os conceitos customizados (e as respetivas expressões) utilizados foram os mesmos que no ponto 4.2.2.1., ou seja os termos “IoT” e “Privacy”.

Assim, o *software* procurou em todos os documentos por cada expressão dos conceitos acima explicados, e atribuiu um sentimento positivo, negativo ou neutro, dependendo do contexto onde a expressão é referenciada.

Tal como ilustrado na figura 45, as expressões referentes ao termo “IoT” não foram encontradas por nenhuma vez em nenhum dos 8 documentos analisados. Isto significa que nas análises efetuadas, os analistas referem-se sempre ao produto e à utilidade em si, e nunca ao mercado em que ele está inserido, ou seja à IoT.

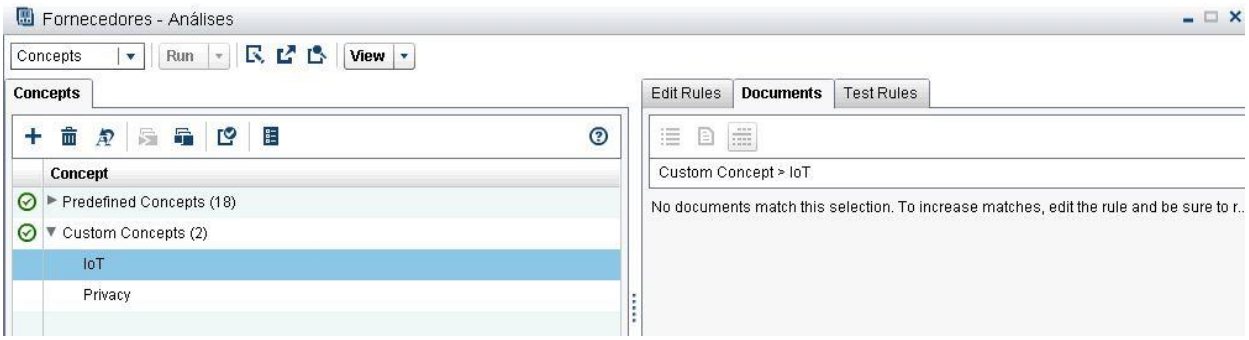

Figura 45. Análise a documentos de análise de produtos IoT - Conceitos customizados – Análise de sentimentos IoT
Fonte: Elaborado pelo autor

Em relação ao conceito “Privacy”, como mostra a figura 46, as suas expressões foram encontradas em todos os 8 documentos, e obtiveram apenas 1 sentimento positivo (13%), 6 sentimentos negativos (74%) e 1 sentimento neutro (13%). Visto existir uma grande diferença entre os sentimentos negativos e positivos, isto significa que os analistas vêm com muito negativismo a privacidade dos dados dos produtos IoT analisados, tendo encontrado diversas lacunas e defeitos nos produtos no que a este tema diz respeito.

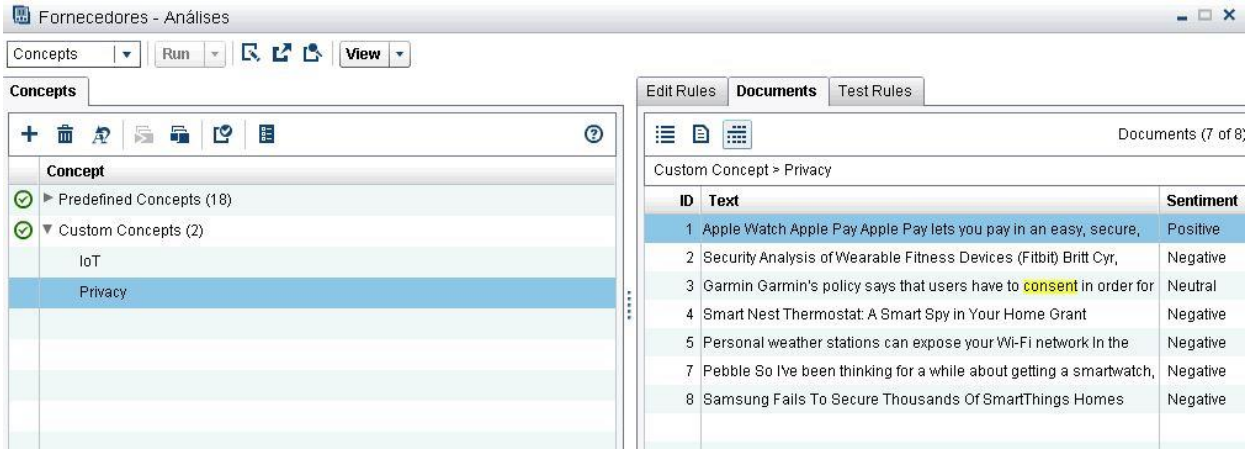

Figura 46. Análise a documentos de análise de produtos IoT - Conceitos customizados – Análise de sentimentos Privacy
Fonte: Elaborado pelo autor

A tabela 6 e o gráfico 3 mostram um resumo dos resultados obtidos pela análise dos conceitos.

Conceitos – Documentos de análise à privacidade de dados de produtos IoT		
	IoT	**Privacy**
Sentimentos positivos	0	1
Sentimentos negativos	0	6
Sentimentos neutros	0	1
%Sentimentos positivos	0%	13%
%Sentimentos negativos	0%	74%
%Sentimentos neutros	0%	13%

Tabela 6. Análise a documentos de análise de produtos IoT - Análise de sentimentos - Tabela
Fonte: Elaborado pelo autor

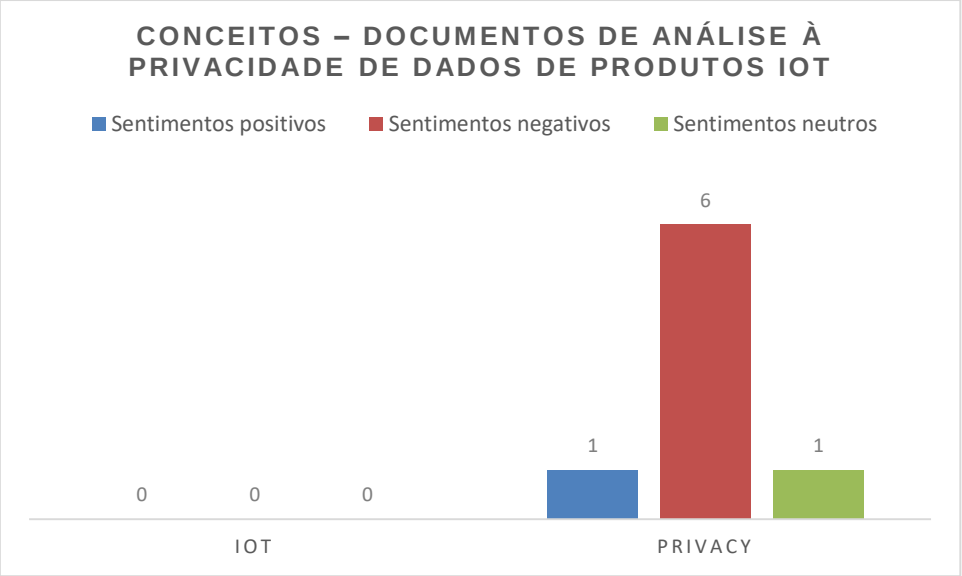

Gráfico 3. Análise a documentos de análise de produtos IoT - Análise de sentimentos – Gráfico
Fonte: Elaborado pelo autor

Tendo em conta que as expressões referentes ao conceito "IoT" não foram encontradas por nenhuma vez em nenhum dos 8 documentos analisados, significa que nas análises efetuadas, os analistas referem-se sempre ao produto e à utilidade em si, e nunca ao mercado em que ele está inserido, ou seja à IoT. Em relação ao conceito "Privacy", visto existir uma grande diferença entre os sentimentos negativos e positivos, isto significa que os analistas vêm com muito negativismo a privacidade dos dados dos produtos IoT analisados, tendo encontrado diversas lacunas e defeitos nos produtos no que a este tema diz respeito.

4.2.3.2. Análise de termos

Tal como descrito no ponto 4.2.3., o *software* encontrou 2532 termos. A figura 47 ilustra quais os termos que aparecem mais vezes no conjunto dos 8 documentos.

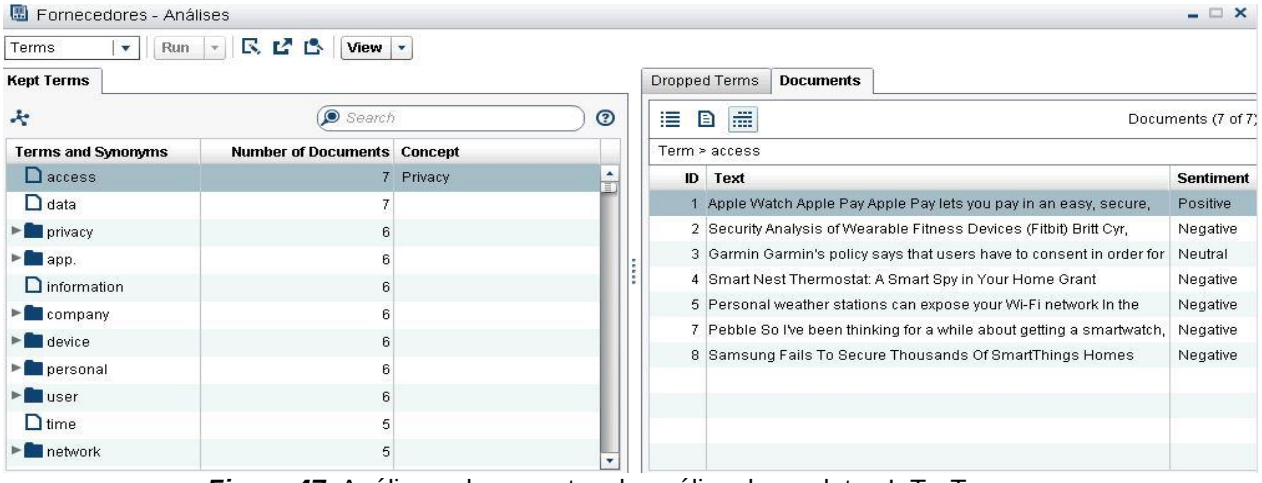

Figura 47. Análise a documentos de análise de produtos IoT - Termos
Fonte: Elaborado pelo autor

A tabela 7 e o gráfico 4 resume a análise de sentimento dos 10 termos mais repetidos (“Access”, “Data”, “Privacy”, “App”, “Information”, “Company”, “Device”, “Personal”, “User”, “Network”), onde foi descartado o termo “time” visto não ser um termo enquadrado com o tema de estudo da dissertação:

Termos – Documentos de análise à privacidade de dados de produtos IoT										
	Access	**Data**	**Privacy**	**App**	**Information**	**Company**	**Device**	**Personal**	**User**	**Network**
Sentimentos positivos	1	1	1	1	1	1	1	1	0	0
Sentimentos negativos	5	4	3	4	3	3	5	3	5	4
Sentimentos neutros	1	2	2	1	2	2	0	2	1	1
Total	7	7	6	6	6	6	6	6	6	5
%Sentimentos positivos	14%	14%	17%	17%	17%	17%	17%	17%	0%	0%
%Sentimentos negativos	72%	57%	50%	66%	50%	50%	83%	50%	83%	80%
%Sentimentos neutros	14%	29%	33%	17%	33%	33%	0%	33%	17%	20%

Tabela 7. Análise a documentos de análise de produtos IoT - Termos - Top 10 - Tabela
Fonte: Elaborado pelo autor

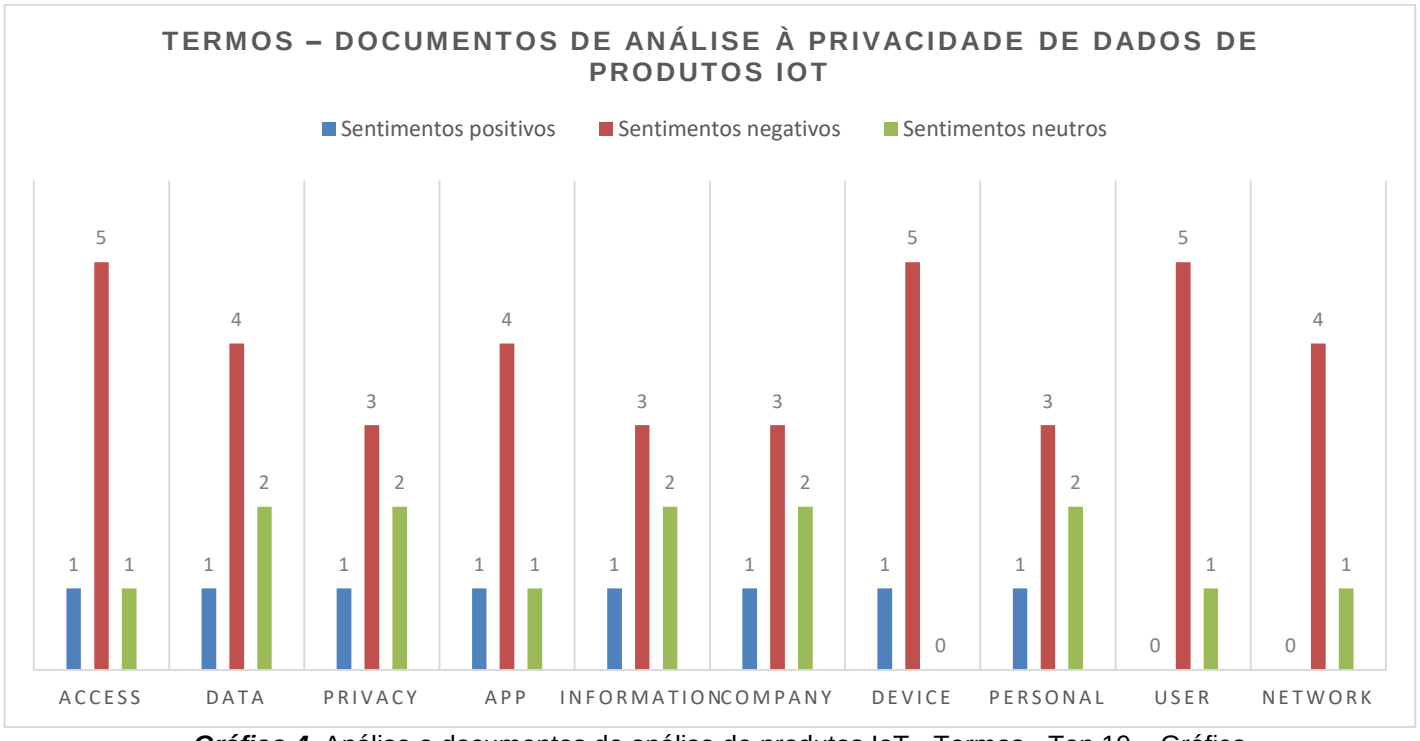

Gráfico 4. Análise a documentos de análise de produtos IoT - Termos - Top 10 – Gráfico
Fonte: Elaborado pelo autor

Pela análise da tabela 7 e do gráfico 4 conclui-se que todos os termos assumem um cariz maioritariamente negativo, tendo os termos “Device” e “User” sido aqueles que obtiveram a maior percentagem de sentimentos negativo, tendo mesmo o termo “User” não obtido qualquer sentimento positivo na análise de todos os documentos. O termo central desta dissertação, “Privacy”, tal como no ponto 4.2.3.1., em que se analisou o conceito “Privacy” e as suas expressões associadas, obteve tal como os restantes, um cariz negativo (50%) e um baixo cariz positivo (apenas 17%).

Através desta análise, podemos concluir que, nos documentos de análise à privacidade de dados dos produtos IoT, os analistas atribuem um baixo grau de privacidade (50% negativo) e acesso (72% negativo) aos dados dos utilizadores dos produtos dos seus utilizadores, bem como uma rede pouco segura (0% positivo e 80% negativo), tal como as *Apps* dos produtos (66% negativo).

4.2.4. Consultoras de TI – Análise à privacidade dos dados na IoT

A última análise diz respeito às análises à privacidade de dados dos produtos IoT efetuadas por algumas das consultoras mais prestigiadas na área das TI.

Esta análise tem como objetivo fazer uma comparação com os resultados obtidos na análise às políticas de privacidade dos fornecedores IoT (4.2.2.), e com os resultados obtidos na análise aos documentos de análise à privacidade dos dados dos produtos IoT por parte de analistas (4.2.3.). Podemos assim comparar se as práticas e suposições de privacidade que os fornecedores descrevem nas suas políticas de privacidade são realmente uma realidade, pelo menos em comparação com a opinião de analistas e consultoras de TI. Tal como referenciado no ponto 3.5.4., foram vários os participantes escolhidos para a investigações, tendo sido escolhidas as consultoras mais prestigiadas do mercado das TI, tendo sido elas a Accenture, Capgemini, Deloitte, Ernst & Young, KPMG, McKinsey & Company, PricewaterhouseCoopers Advisory Services LLC.

Da recolha das análises da privacidade dos dados na IoT por parte das consultoras, surgiram 6 documentos, correspondendo cada documento a uma consultora referenciada no ponto 3.5.4. Como descrito na figura 48, foram encontrados 13546 termos e nenhum tópico nesse conjunto de documentos.

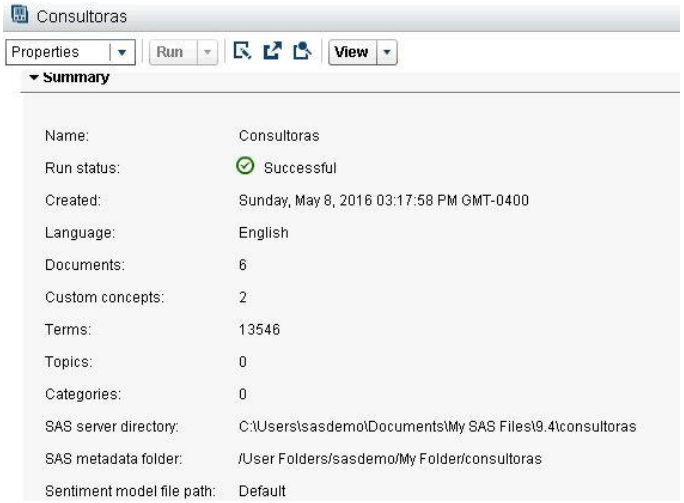

Figura 48. Análise de consultoras à privacidade dos dados na IoT - Propriedades
Fonte: Elaborado pelo autor

4.2.4.1. Análise de conceitos

Na análise de conceitos, os conceitos customizados (e as respetivas expressões) utilizados foram os mesmos que no ponto 4.2.2.1 e 4.2.3.1., ou seja os termos “IoT” e “Privacy”.

Assim, o *software* procurou em todos os documentos por cada expressão dos conceitos acima explicados, e atribuiu um sentimento positivo, negativo ou neutro, dependendo do contexto onde a expressão é referenciada.

Tal como mostra a figura 49, as expressões referentes ao termo “IoT” foram em 3 dos 8 documentos analisados, obtendo em 2 deles um sentimento positivo (67%) e um sentimento neutro no documento restante (33%), não obtendo assim este termo nenhum sentimento de cariz negativo. Isto significa que as consultoras de TI têm uma boa imagem da IoT e das suas potencialidades futuras e presentes.

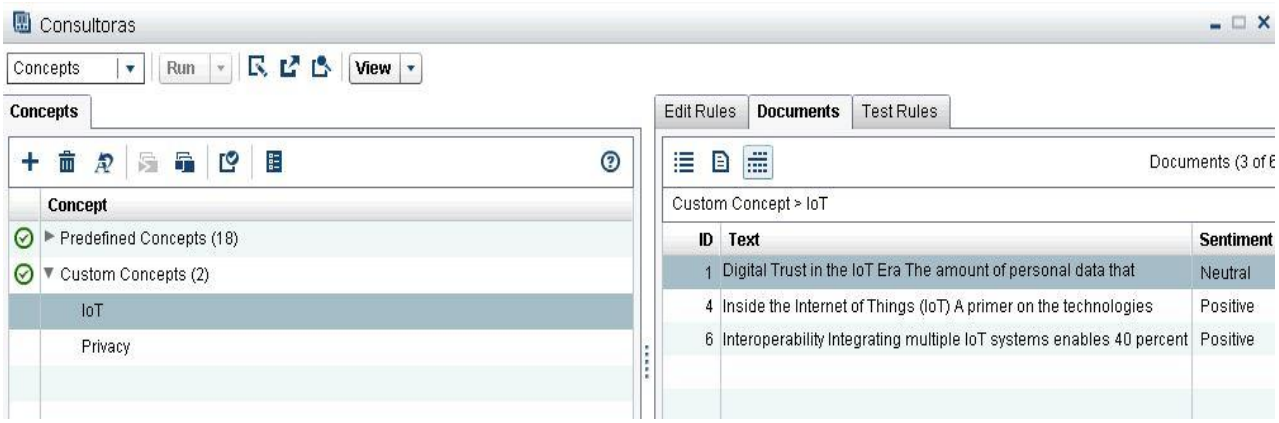

Figura 49. - Análise de consultoras à privacidade dos dados na IoT - Conceitos customizados – Análise de sentimentos IoT

Fonte: Elaborado pelo autor

Em relação ao conceito “Privacy”, tal como mostra a figura 50, as suas expressões foram encontradas em todos os 6 documentos, e obtiveram apenas 2 sentimentos positivos (33%), 3 sentimentos negativos (50%) e 1 sentimento neutro (17%). Apesar da diferença entre os sentimentos positivos e negativos não ser muito grande, a percentagem maior recai sobre o sentimento negativo, significando assim que as consultoras enquadram com um cariz negativo a privacidade dos dados na IoT, pelo menos à data de hoje, visto este ser um tema ainda em “erupção” e a emergir na vida das organizações e dos consumidores.

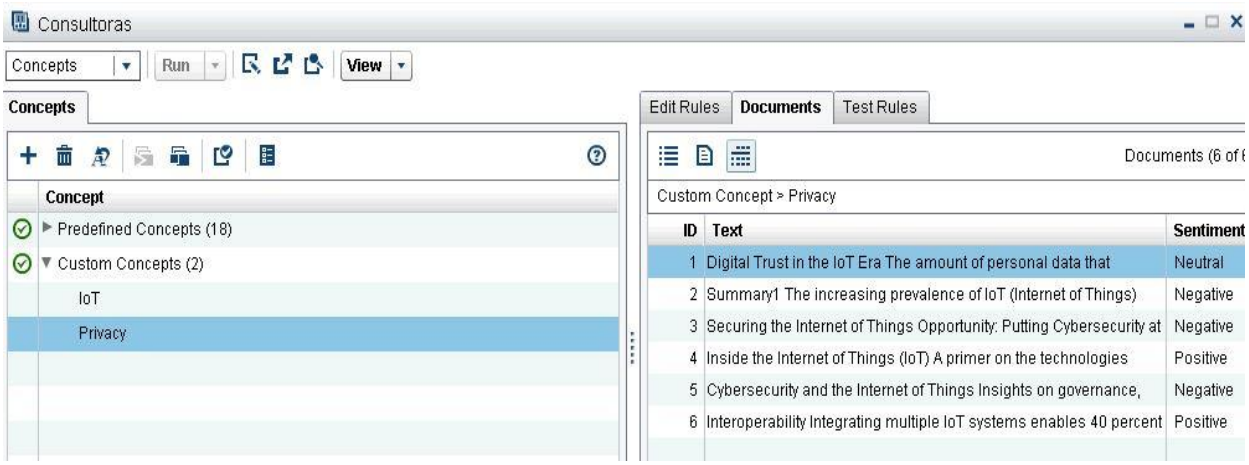

Figura 50. Análise de consultoras à privacidade dos dados na IoT - Conceitos customizados – Análise de sentimentos Privacy
Fonte: Elaborado pelo autor

A tabela 8 e o gráfico 5 mostram um resumo dos resultados obtidos pela análise dos conceitos.

Conceitos – Documentos de análise à privacidade de dados nos produtos IoT		
	IoT	**Privacy**
Sentimentos positivos	2	2
Sentimentos negativos	0	3
Sentimentos neutros	1	1
%Sentimentos positivos	67%	33%
%Sentimentos negativos	0%	50%
%Sentimentos neutros	33%	17%

Tabela 8. Análise de consultoras à privacidade dos dados na IoT - Análise de sentimentos - Tabela
Fonte: Elaborado pelo autor

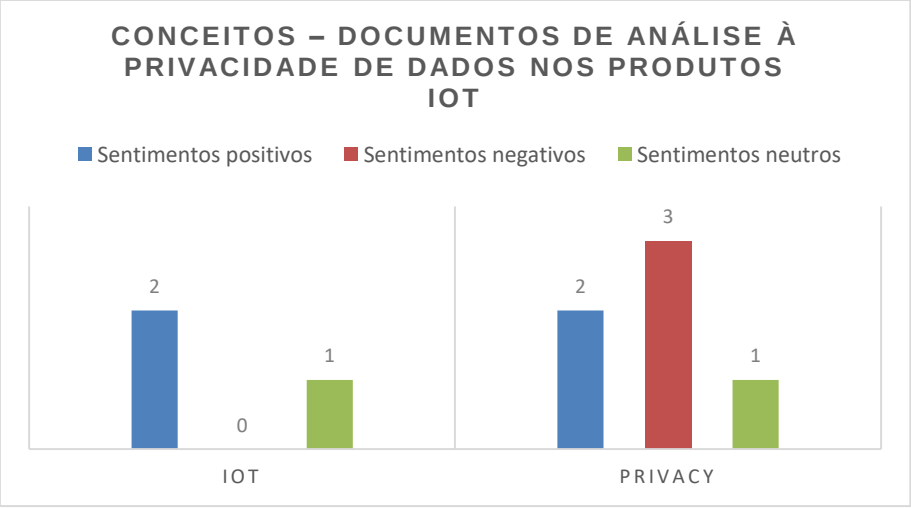

Gráfico 5. Análise de consultoras à privacidade dos dados na IoT - Análise de sentimentos – Gráfico
Fonte: Elaborado pelo autor

Visto o conceito “IoT” não ter obtido nenhum sentimento de cariz negativo, significa que as consultoras de TI têm uma boa imagem da IoT e das suas potencialidades futuras e presentes. Em relação ao conceito “Privacy”, apesar da diferença entre os sentimentos positivos e negativos não ser muito grande, a percentagem maior recai sobre o sentimento negativo, significando assim que as consultoras enquadram com um cariz negativo a privacidade dos dados na IoT, pelo menos à data de hoje, visto este ser um tema ainda em “erupção” e a emergir na vida das organizações e dos consumidores.

4.2.4.2. Análise de termos

Tal como descrito no ponto 4.2.4., o *software* encontrou 13546 termos. A figura 51 ilustra quais os termos que aparecem mais vezes no conjunto dos 6 documentos.

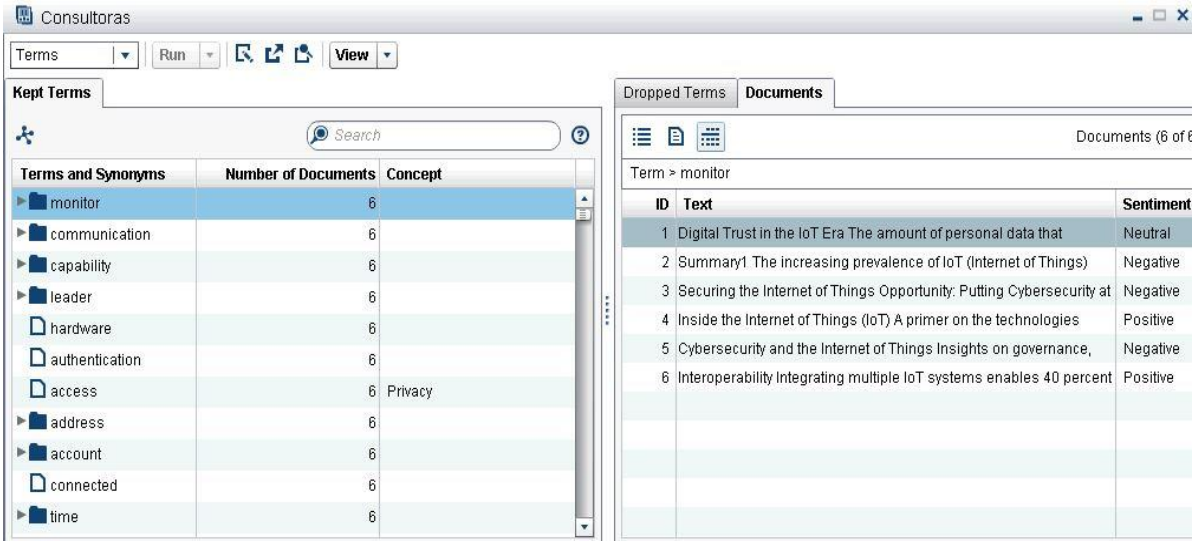

Figura 51. Análise de consultoras à privacidade dos dados na IoT – Termos
Fonte: Elaborado pelo autor

A tabela 9 e o gráfico 6 resumem a análise de sentimento dos 10 termos mais repetidos (“Monitor”, “Communication”, “Capability”, “Privacy”, “Hardware”, “Authentication”, “Access”, “Address”, “Account”, “Connected”), descartando o termo “leader” e adicionando o termo “Privacy” visto este último ser o tema central da dissertação

Termos – Análise à privacidade de dados nos produtos IoT por parte de consultoras TI										
	Monitor	**Communication**	**Capability**	**Privacy**	***Hardware***	**Authentication**	**Access**	**Address**	**Acc**	**Connected**
Sentimentos positivos	2	3	2	2	1	1	1	2	2	2
Sentimentos negativos	3	2	3	3	3	4	3	3	3	3

Sentimentos neutros	1	1	1	1	2	1	2	1	1	1
Total	6	6	6	6	6	6	6	6	6	6
%Sentimentos positivos	33%	50%	33%	33%	17%	17%	17%	33%	33%	33%
%Sentimentos negativos	50%	33%	50%	50%	50%	67%	50%	50%	50%	50%
%Sentimentos neutros	17%	17%	17%	17%	33%	17%	33%	17%	17%	17%

Tabela 9. Análise de consultoras à privacidade dos dados na IoT – Termos - Top 10 - Tabela
Fonte: Elaborado pelo autor

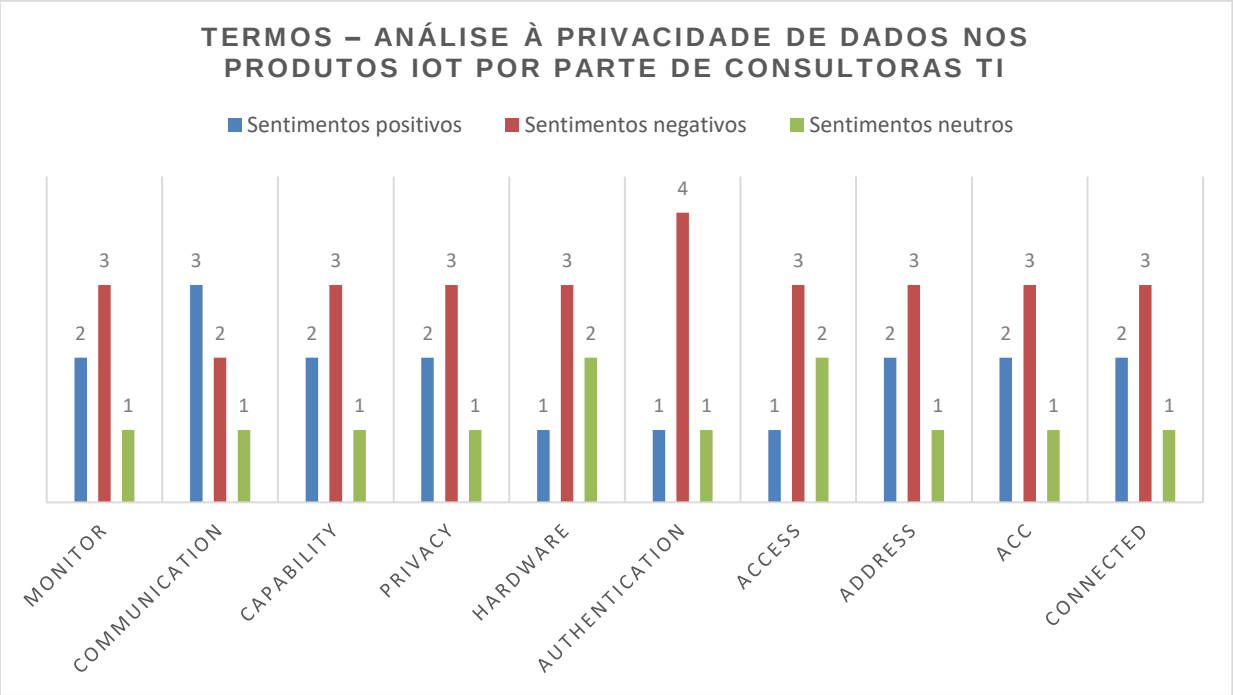

Gráfico 6. Análise de consultoras à privacidade dos dados na IoT – Termos - Top 10 – Gráfico
Fonte: Elaborado pelo autor

Através da análise da tabela 9 e do gráfico 6, conclui-se que na sua grande maioria, todos os termos apresentam um cariz negativo, à excepção do termo “Communication”. O termo central desta dissertação, “Privacy”, tal como no ponto 4.2.4.1., em que se analisou o conceito “Privacy” e as suas expressões associadas, obteve uma pontuação igual, ou seja, um cariz negativo (50%) e um baixo cariz positivo (apenas 17%).

Através desta análise, podemos concluir que, nas análises das consultoras à privacidade dos dados na IoT são atribuidas um grau de negatividade à privacidade (50% negativo), acesso (50% negativo) e autenticação (67%), bem como a todos os restantes termos, à excepção do termo “Comunication” (50% positivo e 33% negativo).

4.2.5. Comparação das análises dos pontos 4.2.2 e 4.2.3

Visto a dissertação ter como objetivo geral dar a entender a forma como os fornecedores, consultoras e os consumidores da IoT estão a abordar o desafio da privacidade e segurança dos dados, é útil fazer-se uma comparação entre os resultados obtidas nas análises às políticas de privacidade dos fornecedores, das análises aos documentos de análise à privacidade dos produtos IoT, (comparação entre os resultados obtidos nos pontos 4.2.2, 4.2.3). Esta comparação irá permitir dar uma noção sobre se as práticas e processos que as fornecedoras de produtos IoT estabeleceram para garantir a privacidade dos dados dos seus utilizadores, correspondem à realidade vivenciada pelos seus utilizadores. Para esta comparação, o aluno apenas se limitou a comparar os resultados obtidos pela análise do *software*, e a elaborar as respetivas descrições sobre esses mesmos resultados.

4.2.5.1. Comparação da análise de conceitos

Na análise de conceitos de ambas as análises, os conceitos customizados (e as respetivas expressões) utilizados foram os termos “IoT” e “Privacy”, cuja descrição está no ponto 4.2.2.1.

Assim, o *software* procurou em todos os documentos por cada expressão dos conceitos acima descritos, e atribuiu um sentimento positivo, negativo ou neutro, dependendo do contexto onde a expressão é referenciada.

A tabela 10 e o gráfico 7 mostram os resultados obtidos na análise de conceitos dos pontos 4.2.2.1. e 4.2.3.1:

Comparação da análise de conceitos				
	IoT – Políticas de privacidade dos fornecedores	**IoT – Documentos de análise**	**Privacy – Políticas de privacidade dos fornecedores**	**Privacy – Documentos de análise**
Sentimentos positivos	3	0	15	1
Sentimentos negativos	0	0	4	6
Sentimentos neutros	0	0	2	1
%Sentimentos positivos	100%	0%	71%	13%
%Sentimentos negativos	0%	0%	19%	74%
%Sentimentos neutros	0%	0%	10%	13%

Tabela 5. Comparação análise de conceitos - Tabela
Fonte: Elaborado pelo autor

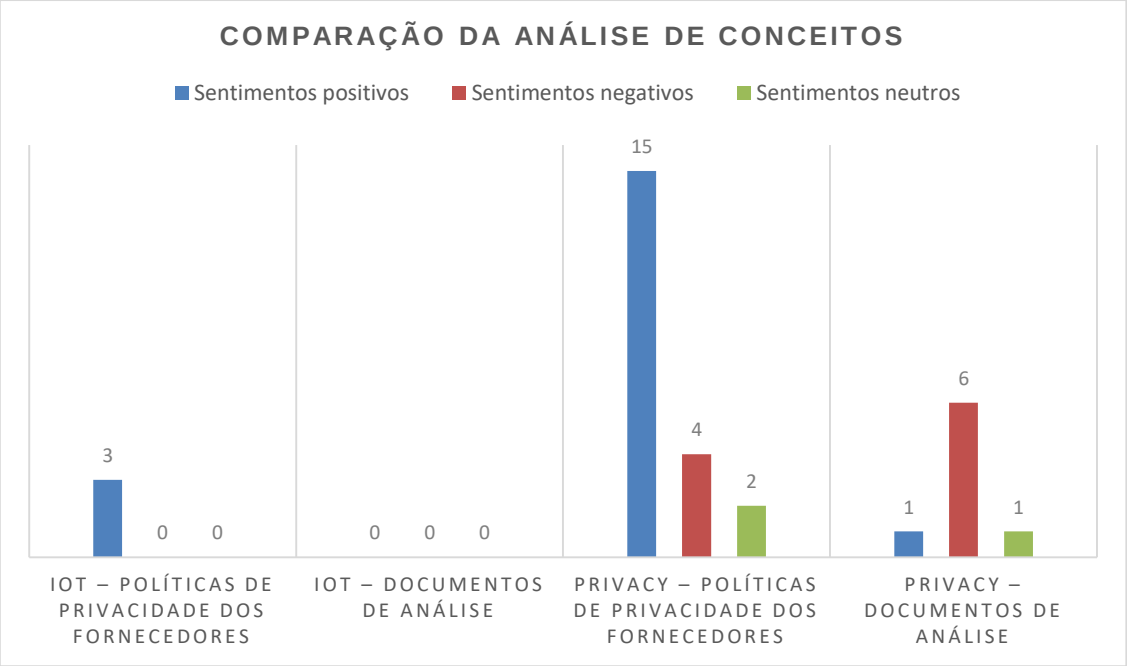

Gráfico 7. Comparação análise de conceitos – Gráfico
Fonte: Elaborado pelo autor

Pela análise da tabela 10 e do gráfico 7, temos vários aspetos conclusivos:

1. Em relação ao conceito IoT, as suas expressões associadas ("IoT" e "Internet of Things") apenas foram encontradas na análise às políticas de privacidade dos produtos IoT dos fornecedores, obtendo um sentimento positivo de 100%, não tendo sido encontrado qualquer registo deste conceito nos documentos de análise à privacidade de produtos IoT. Isto significa que, nas suas políticas de privacidade IoT, os fornecedores passam um cariz totalmente positivo desta temática aos seus consumidores, e apesar de ser um tema ainda a emergir, os fornecedores acreditam nas suas características, potencialidades e benefícios para os utilizadores;
2. A comparação entre os resultados obtidos às análises do conceito "Privacy" e suas expressões associadas (ver expressões no ponto 4.3.1.1) mostram-nos duas realidades dispâras, a transmitida nas políticas de privacidade dos produtos IoT e as vivenciadas pelos analistas e utilizadores destes produtos. Isso é refletido na diferença entre a percentagem de sentimentos positivos e negativos de ambas as análises. Na 1ª análise, as políticas de privacidade transmitem uma ideia de segurança e privacidade dados dos utilizadores, obtendo este conceito uma pontuação de 71% de sentimentos positivos, 19% negativos e 10% negativos. Olhando para a 2ª análise, podemos verificar que a realidade do nível de privacidade dos dados vivenciada pelos utilizadores de alguns dos produtos da 1º análise é bem diferente. Isto porque, o conceito "Privacy" obteve aqui uma pontuação de apenas 13% sentimentos positivos (contra os 71% da 1ª análise) e 74% de sentimentos negativos (contra os 19% da 1ª análise).

4.2.5.2. Comparação da análise de termos

Em relação à análise de termos efetuada, o *software* encontrou 8765 termos na 1ª análise, referente às políticas de privacidade dos fornecedores de produtos IoT e 2532 termos na 2ª análise, referente aos documentos de análise de produtos IoT. A comparação efetuada entre os termos das duas análises baseou-se fundamentalmente no termo central da dissertação, o termo "Privacy", bem como nos termos em comum das duas análises (ver pontos 4.2.2.2 e 4.2.3.2)

A tabela 11 e o gráfico 8 fazem uma comparação entre os termos em comum das duas análises. Os termos da análise das políticas de privacidade de fornecedores de produtos IoT irão designar-se pelo nome do termo e do acrónimo PP ("Nome do termo" - PP). Os termos das análises aos documentos de análise à privacidade dos produtos IoT irão referenciar-se pelo nome do termo e do acrónimo DA ("Nome do termo" - DA).

Da análise dos termos dos pontos 4.2.2.2 e 4.2.3.2, surgiram os seguintes termos em comum: "Privacy", "Data", "Information", "Access" e "Device".

Comparação da análise de termos										
	Privacy - PP	**Privacy - DA**	**Data - PP**	**Data - DA**	**Information - PP**	**Information - DA**	**Access - PP**	**Access - DA**	**Device - PP**	**Device - DA**
Sentimentos positivos	18	1	18	1	18	1	15	1	17	1
Sentimentos negativos	5	3	5	4	4	3	5	5	3	5
Sentimentos neutros	2	2	2	2	2	2	2	1	2	0
Total	25	6	25	7	24	6	22	7	22	6
%Sentimentos positivos	72%	17%	72%	14%	75%	17%	68%	14%	77%	17%
%Sentimentos negativos	20%	50%	20%	57%	17%	50%	23%	72%	14%	83%
%Sentimentos neutros	8%	33%	8%	29%	8%	33%	9%	14%	9%	0%

Tabela 11. Comparação análise de termos - Tabela
Fonte: Elaborado pelo autor

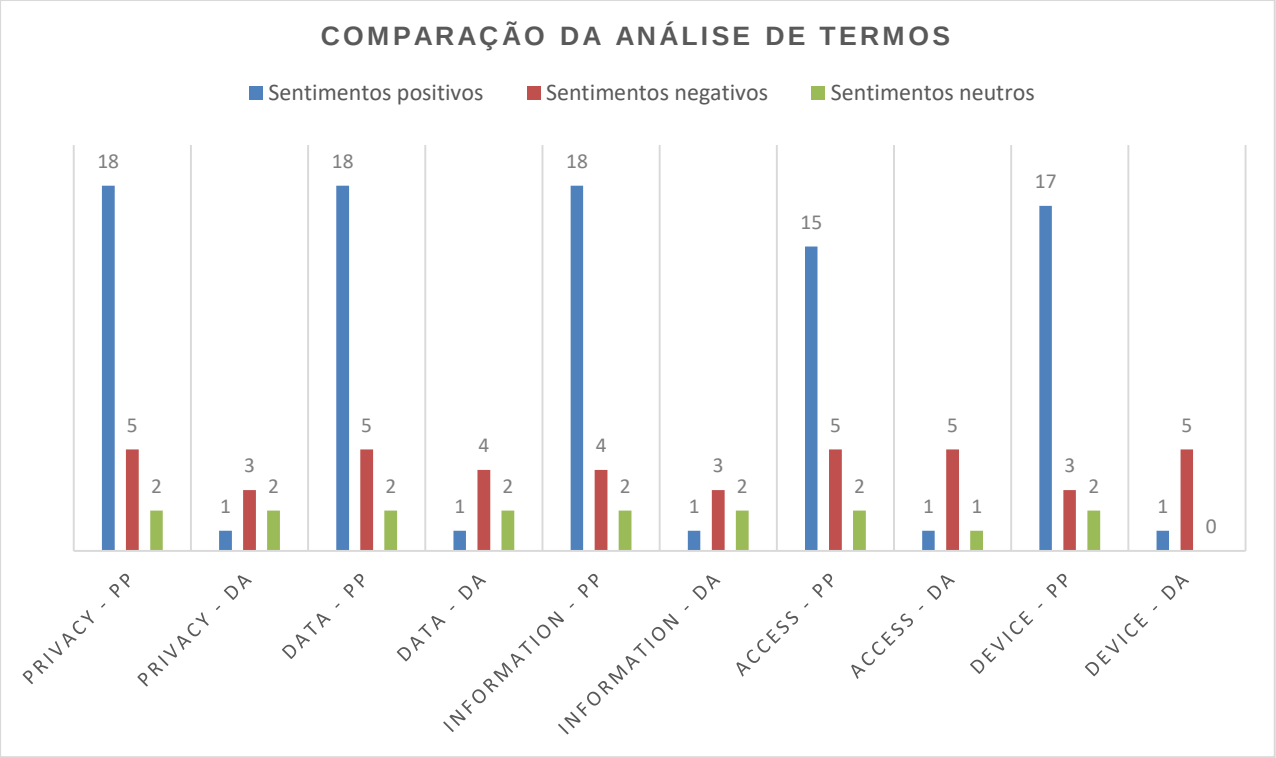

Gráfico 8. Comparação análise de termos – Gráfico
Fonte: Elaborado pelo autor

Através da análise da tabela 11 e do gráfico 8, surgem as seguintes conclusões:

1. Nenhum dos termos comparados entre si apresenta uma pontuação sentimental semelhante;
2. A pontuação positiva de cada termo é muito maior nos termos das políticas de privacidade do que nos documentos de análise. O oposto se passa com a pontuação negativa, que apresenta valores muito mais altos nos documentos de análise do que nas políticas de privacidade;
3. Analisando estes factos, podemos concluir, tal como na comparação da análise de conceitos, que os resultados nos mostram duas realidades díspares, a transmitida nas políticas de privacidade dos produtos IoT e as vivenciadas pelos analistas e utilizadores destes produtos. No caso da privacidade (“Privacy”), olhando para a alta percentagem de sentimentos positivos (72%), os fornecedores apresentam garantias de privacidade nos produtos aos seus utilizadores, sendo este facto um pouco diferente quando olhamos para a percentagem negativa (50%) da privacidade dos produtos presente nos documentos de análise desses mesmos produtos. O mesmo acontece com os termos dados (“Data”) e informação (“Information”). Estes termos apresentam apenas uma pontuação negativa de 20% e 17% respetivamente nas políticas de privacidade. No entanto, comparando com as análises feitas à privacidade dos dados dos produtos, a pontuação negativa destes dois termos sobe até aos 57% no caso dos dados e 50% no caso da informação. Uma subida bastante acentuada, o que revela grandes imparidades. Também nos termos acesso (“Access”) e dispositivo (“Device”) estas imparidades

acontecem, apresentando estes termos altas percentagens de sentimentos positivos nas políticas de privacidade, 68% e 77% respetivamente, apresentando no entanto percentagens baixíssimas quando comparado com os documentos de análise (14% e 17%);

4. Estes resultados não põem em causa a veracidade das políticas de privacidade dos produtos IoT, apenas confronta a realidade nelas apresentadas, com a realidade vivenciada pela utilização desses mesmos produtos.

5. Conclusão e perspetivas de trabalho futuras

Neste capítulo será elaborada uma breve síntese das atividades desenvolvidas ao longo da dissertação e do seu contributo para um conhecimento aprofundado da IoT, assim como do estudo de caso efetuado e as propostas que dele emanaram, culminando com as principais conclusões, encerrando o capítulo com as perspetivas de trabalho futuro.

5.1. Conclusões

A IoT é o novo paradigma tecnológico que irá transformar o modo como vivemos, trabalhamos e aprendemos. É o início de um ciclo de renovação tecnológica que auxiliará na otimização e automatização de tarefas quotidianas básicas. Enquanto há uma grande oportunidade para criar novos produtos e serviços personalizados, essa oportunidade vem com um custo associado, que é a privacidade dos dados pessoais. Com a tendência de aumento de dispositivos e utilizadores conectados, haverá também um enorme volume de dados a fornecer informações pessoais, sobre a forma como cada indivíduo utiliza certo aparelho ou aplicação. Estas informações deixam rastos sobre os seus comportamentos quotidianos, disponibilizando informação sensível que se quer privada e anónima. Proteger a privacidade dos dados, requer um complexo equilíbrio de autenticação, autorização e consciência contextual.

Esta dissertação teve como objetivo:

- Analisar a forma como algumas das organizações fornecedoras de IoT estão a abordar os temas da privacidade e barreiras de segurança nos seus dispositivos;
- Analisar a forma como a privacidade dos dados nos produtos IoT é vista por analistas da área;
- Esclarecer junto de consultoras de TI, qual o seu entendimento e visão para com a privacidade dos dados na IoT;
- Comparar a forma de abordagem dos fornecedores em relação à privacidade dos dados nos seus produtos IoT com a visão de analistas e consultoras para esse mesmo tema.

O facto de a dissertação ser apenas um estudo de caso, o número de organizações, tanto fornecedoras como consultoras, é bastante reduzido tendo em conta o enorme universo de organizações envolvidas na temática da IoT, tanto na área de dispositivos pessoais, estilo de vida, casas inteligentes, etc., tendo esse fator condicionado os resultados obtidos nas análises, tanto dos questionários, como das análises efetuadas pelo *software* SAS Contextual Analysis.

Visto esta temática ser um dos maiores desafios da IoT, a sua clarificação poderá ser uma mais-valia para entender este mercado, onde se incluem consumidores e fornecedores, dando uma perspetiva sobre a forma como este desafio é abordado por ambos (com a devida limitação do número reduzido da amostra analisada).

Através das análises efetuadas às políticas de privacidade dos fornecedores de produtos IoT, em comparação com as análises realizadas por analistas sobre a privacidade desses mesmos produtos, constataram-se duas realidades dispâras, a transmitida pelas políticas de privacidade dos produtos IoT e

as vivenciadas pelos analistas e utilizadores destes produtos. Isso é refletido na diferença entre a percentagem de sentimentos positivos e negativos de ambas as análises. (ponto 4.2.5.). Tal como o relatório da Comissão Europeia recomenda, desde o ínicio da conceção de um produto IoT, este deve ser concebido para atender aos requisitos fundamentais que sustentam o direito ao esquecimento, portabilidade de dados, privacidade e os princípios da proteção de dados (CE, 2013). Através das análises foi possível concluir que, apesar de estes requisitos estarem contemplados nas políticas de privacidade de dados dos produtos IoT analisados, o mesmo não se passa na realidade, pelo que se pode constatar nas análises efetuadas aos documentos de análise à privacidade de produtos IoT.

Ainda assim, segundo os questionários aplicados às organizações fornecedoras, onde se procurou obter respostas às questões "porque é que a IoT está a ter um elevado impacto global na sociedade?", "de que forma se está a dar o comportamento das organizações na IoT?", "como está a correr o desenvolvimento da IoT em Portugal?", "qual a visão das organizações para a privacidade dos dados?", "como está a decorrer o processo de adequar a privacidade dos dados dos utilizadores aquando do desenvolvimento dos produtos IoT por parte das organizações?", todas elas garantiram que a sua preocupação com a segurança e privacidade dos dados dos seus utilizadores, afirmando que estes dois vetores são garantidos desde a conceção inicial de qualquer produto IoT (ponto 4.1.2.).

O facto de a dissertação ser apenas um estudo de caso, o número de organizações, tanto fornecedoras como consultoras, foi bastante reduzido, tendo isso condicionado os resultados obtidos nas análises.

Apesar de as empresas analisadas estarem sediadas nos EUA, onde a legislação, normas e *standards* sobre a IoT ainda não são uma realidade (ponto 2.5.), e apesar de a informação contida nas suas políticas de privacidade garantir a privacidade da informação dos seus consumidores, as análises de analistas à privacidade desses mesmos produtos diz-nos o contrário. Apesar deste fator, através dos questionários realizados às empresas fornecedoras, foi possível entender que a maior parte tem a perfeita noção de que os consumidores dos seus produtos preferem ter um dispositivo barato e menos seguro, do que um dispositivo caro e seguro (ponto 4.1.2.). Ainda através das respostas dadas aos questionários, foi percetível que uma parte das organizações prevê que no futuro, à medida que o preço da segurança, e a facilidade em garantir essa mesma segurança, os produtos IoT irão ter um paralelismo entre o preço/qualidade/segurança.

5.2. Perspetivas de trabalho futuras

Tendo em conta as conclusões obtidas através das análises aos questionários de privacidade de dados efetuadas às empresas fornecedoras de produtos IoT, bem como das análises aos documentos de privacidade de dados na IoT, perspetiva-se que no futuro há muito trabalho a fazer nesta área, nomeadamente em garantir a privacidade dos dados dos consumidores por parte das empresas fornecedoras, que irão adotar melhores soluções técnicas que garantam essa mesma privacidade.

Além disso, perspetiva-se que os seus documentos de políticas de privacidade dos dados dos produtos IoT irão ser atualizados, de forma a esclarecer como as informações dos utilizadores são

recolhidas, armazenadas, processadas, analisadas e divulgadas. Isto irá permitir que os utilizadores dos produtos IoT de uma determinada empresa se sintam mais confiantes e conheçam melhor a forma como os seus dados pessoais são tratados pela mesma. Esses mesmos métodos de garantia de privacidade dos consumidores devem realmente ser aplicados nos produtos IoT, e não apenas contemplados nas políticas de privacidade, tal como se constatou ser a realidade atual, após as análises efetuadas às mesmas ao longo das atividades desenvolvidas na dissertação.

Outra medida necessária para que a privacidade e segurança dos dados dos consumidores na IoT seja uma realidade, é a necessidade de legislação. Na Europa, esta mesma legislação está bem encaminhada para se tornar efetiva em 2017, faltando apenas aprovação do Conselho Europeu. Nos EUA, a entrada em vigor de uma legislação está a decorrer de forma mais lenta, existindo neste momento apenas um relatório da FTC, onde descreve as melhores práticas para a IoT, de forma a ir ao encontro da proteção da privacidade dos consumidores.

Em relação ao trabalho desenvolvido na dissertação, pode-se dar como perspetivas de trabalho futuras, o estudo de todas, ou da maior parte das organizações fornecedoras, ao invés de apenas o estudo de um número reduzido de organizações elaborado na dissertação. Outra perspetiva de trabalho futura, passará por analisar se as diretrizes e regulamentos de privacidade dos dados na Europa e EUA (ponto 2.5) já estão em vigor e em caso positivo estudar o seu impacto. Adicionando a estas, também seria interessante estudar a forma como os consumidores finais dos produtos IoT se sentem em relação à privacidade desses mesmos produtos, bem como o estudo da posição da comissão nacional de proteção de dados referente a esta temática da privacidade dos dados na IoT. Por último, de notar que a temática da IoT não se esgota nas análises referenciadas nesta dissertação. O tema da privacidade dos dados é apenas um mundo num enorme universo.

Referências

- Altimeter (2015). *Consumer Perceptions of Privacy in the Internet of Things*. Acedido em 18, Março, 2016, em http://go.pardot.com/l/69102/2015-07-12/pxzlm
- Amplio (2014). *Definição*. Acedido em 14, Abril, 2016, em http://www.amplio.com.br/rfid/definicao
- Araújo, C., Lopes, E. M. F. P., Lopes, J., & Pinto, L. N. R. (2008). *Estudo de Caso*
- Assepro (2013). *Entenda como funciona a Internet das oisas e qual o papel do RFID. Ace*dido em 30, Janeiro, 2016, em http://www.assespro-mg.org.br/index.php/entenda-como-funciona-a-internet-das-coisas-e-qual-papel-do-rfid/
- Awasthi, G. (2015). *Internet of Things - An Architectural Perspective*. Acedido em 30, Janeiro, 2016, em http://www.slideshare.net/gawasthi22/internet-of-things-arch-perspective
- Barbin (2014). *Uma etiqueta inteligente.* Acedido em 5, Maio, 2016, em http://www.unicamp.br/unicamp/ju/625/uma-etiqueta-inteligente
- Bartunek, J. M. & SEO, M. (2002). Qualitative research can add new meanings to quantitative research. Journal of Organizational Behavior, v. 23, n.2.
- Biswas, S. (2011). *Home Automation*. Acedido em 14, Abril, 2016, em http://saikatbiswas14.blogspot.pt/
- Bogdan, R. & Bilken, S. (1994). *Investigação qualitativa em educação*. Porto: Porto Editora
- Booktec (2014). *Four Phases of Library* RFID *System*. Acedido em 14, Abril, 2016, em http://www.rfid-library.com/eng_four.html
- Bulmer, M. (1997). Sociological research methods. London: Macmillan
- Consumers International. (2016). *Searching for the Meaning of Apple Homekit*. Acedido em 28, Maio, 2016, em http://www.consumersinternational.org/media/1657273/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf
- Contactless Intelligence (2015). *NXP debuts device to accelerate* NFC *adoption in* IoT. Acedido em 14, Abril, 2016, em https://contactlessintelligence.com/2015/06/24/nxp-debuts-device-to-accelerate-nfc-adoption-in-IoT/
- Davenport, T. (2015). *The Analytics of Things*. Acedido em 4, Abril, 2016, em https://www.linkedin.com/pulse/analytics-things-tom-davenport
- DEV Tecnologia (2015). *O que é a Internet das Coisas?* Acedido em 25, Julho, 2016, em http://devtecnologia.com.br/internet-das-coisas-iot/
- Dreibi, G. (2014). *Segurança e falta de padrões dificultam popularização da Internet das Coisas.* Acedido em 25, Maio, 2016, em http://tecnologia.ig.com.br/especial/2014-04-25/seguranca-e-falta-de-padroes-dificultam-popularizacao-da-internet-das-coisas.html
- Escritório do Comissário de Privacidade do Canada (2013). *The Internet of Things - An introduction to privacy issues with a focus on the retail and home environments.* Acedido em 18, Abril, 2016, em https://www.priv.gc.ca/information/research-recherche/2016/IoT_201602_e.pdf

- Europol (2014). *The Internet Organised Crime Threat Assessment (IOCTA).* Acedido em 25, Maio, 2016, em https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta

- Feierman, A. (2015). *Searching for the Meaning of Apple Homekit*. Acedido em 28, Abril, 2016, em http://www.*Smart*erhomeautomation.com/articles/searching-for-the-meaning-of-apple-homekit/

- Freixo, M. (2010). *Metodologia científica: fundamentos, métodos e técnicas*. Lisboa. Instituto Piaget.

- FTC (2013). *Internet of Things - Privacy and Security in a Connected World.* Acedido em 18, Abril, 2016, em https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world

- Gartner (2015a). *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015*. Acedido em 15, Março, 2016, em http://www.gartner.com/newsroom/id/3165317/

- Gartner (2015b). *Address Cybersecurity Challenges Proactively to Ensure Success With Outsourced IoT Initiatives*. Acedido em 15, Março, 2016, em https://www.gartner.com/doc/3046917/address-cybersecurity-challenges-proactively-ensure

- Harris, R. (2015*). MediaTek Releases Platform to Create Wi Fi Enabled IoT Devices and Wearables*. Acedido em 10, Março, 2016, em https://appdevelopermagazine.com/2363/2015/2/10/MediaTek-Releases-Platform-to-Create-*Wi-fi*-Enabled-IoT-Devices-and-Wearables/

- Hawkins, A. (2016). *What does General Data Protection Regulation actually mean for marketers*. Acedido em 28, Maio, 2016, em http://www.*Smart*insights.com/marketplace-analysis/digital-marketing-laws/what-general-data-protection-regulation-actually-means/

- Hernández, R. (2015). *F-Secure – Internet das Coisas promete muitos benefícios, mas privacidade ainda é um ponto a se preocupar*. Acedido em 18, Março, 2016, em http://www.consultcorp.com.br/noticias/126-f-secure-internet-das-coisas-promete-muitos-beneficios-mas-privacidade-ainda-e-um-ponto-a-se-preocupa

- HP (2014). *HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack*. Acedido em 15, Março, 2016, em http://community.hpe.com/t5/Protect-Your-Assets/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284

- IIC (2014). Disponível em: https://www.youtube.com/watch?v=zhKUdwdf0dI. Acedido em 15, Março, 2016

- IEEE (2015). *IEEE begins building solid foundation for the Internet of Things.* Acedido em 24, Maio, 2016, em http://standards.ieee.org/news/2014/P2413.html

- Intel (2014, Junho 12). *Green Cities: San Jose implements Intel IoT solutions* [Ficheiro de vídeo]. Retirado de http://www.intel.com/content/www/us/en/internet-of-things/videos/*Smart*-city-san-jose-video.html

- IoT Analytics (2014). *Why the Internet of Things is called Internet of Things: Definition, history, disambiguation*. Acedido em 30, Março, 2016, em http://iot-analytics.com/internet-of-things-definition/

- IoT Analytics (2015). *The 10 most popular Internet of Things applications right now*. Acedido em 4, Abril, 2016, em http://iot-analytics.com/10-internet-of-things-applications/

- IoT Philipphines. (2015). *Smart Cities*. Acedido em 10, Março, 2016, em http://www.IoTphils.com/solutions/*Smart-cities*/

- Juniper Research (2014). *Smart homes ~ It's an Internet of Things Thing.* Acedido em 4, Abril, 2016, em http://www.connectedplusshow.com/assets/she14_wp.pdf

- Kash, W. C. (2014). *Internet Of Things: 8 Cost-Cutting Ideas For Government*. Acedido em 7, Fevereiro, 2016, em http://www.informationweek.com/government/leadership/internet-of-things-8-cost-cutting-ideas-for-government/d/d-id/1113459

- Klein, C. (2015). *2016 predictions for IoT and Smart homes*. Acedido em 4, Abril, 2016, em http://thenextweb.com/insider/2015/12/23/2016-predictions-for-iot-and-*Smart*-homes/

- Lawson, S. (2014). *Why Internet of Things 'standards' got more confusing in 2014.* Acedido em 23, Maio, 2016, em http://www.pcworld.com/article/2863572/iot-groups-are-like-an-orchestra-tuning-up-the-music-starts-in-2016.html

- Lawson, S. (2015). *Internet of Things standards groups get ready to rumble at CES.* Acedido em 14, Maio, 2016, em http://www.pcworld.com/article/2994794/internet-of-things/iot-standards-groups-get-ready-to-rumble-at-ces.html

- Libelium (2014). *Bluetooth Low Energy to Connect Sensors with Smartphones and Tablets*. Acedido em 14, Abril, 2016, em http://www.libelium.com/*Bluetooth*-low-energy-ble-4-0-*Smart*-connect-sensors-*Smartphone*

- Loh, S. (2008). *Definição de Text Mining*. Acedido em 26, Setembro, 2016, em http://miningtext.blogspot.pt/2008/11/definio-de-text-mining.html

- Libelium (2015). *50 Sensor Applications for a Smarter World*. Acedido em 24, Fevereiro, 2016, em http://www.libelium.com/top_50_iot_sensor_applications_ranking/

- Malik, A. (2014). *Why Wi-fi will be the technology of choice for the Internet of Things*. Acedido em 14, Abril, 2016, em http://www.networkworld.com/article/2917793/internet-of-things/is-*wi-fi*-going-to-be-the-technology-of-choice-for-IoT.html

- Matias, B. (2014). *(IoT) – Internet of Things – A importância das normas.* Acedido em 18, Maio, 2016, em http://brunomatias.com/IoT-internet-of-things-a-importancia-das-normas/

- McKinsey (2015). *Unlocking the potential of the Internet of Things.* Acedido em 25, Maio, 2016, em http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

- Myers, M. (1997) *Qualitative Research in Information Systems*. Acedido em 24, Março, 2016, em http://www.qual.auckland.ac.nz

- Nichols, S. (2015). *CES 2015: AllSeen Alliance to bring order to the Internet of Things*. Acedido em 18, Abril, 2016, em http://www.zdnet.com/article/ces-2015-*AllSeen*-alliance-to-bring-order-to-the-internet-of-things/

- Null, C. (2015). *The state of IoT standards: Stand by for the big shakeout.* Acedido em 24, Maio, 2016, em http://techbeacon.com/state-iot-standards-stand-big-shakeout

- Peter (2014). *Google-owned Nest and Samsung join forces for the future of home automation.* Acedido em 24, Março, 2016, em http://blog.gsmarena.com/google-owned-nest-samsung-join-forces-future-home-automation/

- OWASP (2016). *Welcome to OWASP.* Acedido em 25, Julho, 2016, em https://www.owasp.org/index.php/Main_Page

- Rouse, M. (2011). *Natural language processing (NLP).* Acedido em 25, Julho, 2016, em http://searchcontentmanagement.techtarget.com/definition/natural-language-processing-NLP

- *SAS* (2014). *Machine Learning*. Acedido em 26, Setembro, 2016, em http://www.sas.com/en_id/insights/analytics/machine-learning.html

- *SAS* (2015). *SAS Contextual Analysis*. Acedido em 14, Abril, 2016, em http://www.sas.com/content/dam/SAS/en_us/doc/factsheet/sas-contextual-analysis-106758.pdf

- Soley, R. (2015). *First European testbed for the Industrial Internet Consortium*. Acedido em 28, Abril, 2016, em http://blog.bosch-si.com/categories/manufacturing/2015/02/first-european-testbed-for-the-industrial-internet-consortium/

- Sousa, G. (1998). *Metodologia da Investigação, Redacção e Apresentação de trabalhos Científicos*. 1ª Edição. Porto. Livraria Civilização editora.

- Stake, R. E. (1994). *Case Studies. In N. Denzin Y. Lincoln, Handbook of qualitative research (pp. 236-247)*. Newsbury Park: Sage

- Stake, R. E. (1999). *Investigación con estudio de casos*. Madrid: Morata

- Symantec (2015). *State of Privacy Report 2015*. Acedido em 18, Março, 2016, em https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf

- RS Components (2014). *11 Internet of Things (IoT) Protocols You Need to Know About.* Acedido em 14, Abril, 2016, em http://www.rs-online.com/*design*spark/electronics/knowledge-item/eleven-internet-of-things-IoT-protocols-you-need-to-know-about

- Thousand Oaks (2003), CA: SAGE Publications

- Turck, M. (2014). *The Internet Of Things Is Reaching Escape Velocity*. Acedido em 4, Maio, 2016, em http://techcrunch.com/2014/12/02/the-internet-of-things-is-reaching-escape-velocity/

- VERGARA, *S. C. Métodos de pesquisa em administração*. São Paulo: Atlas, 2005

- Verizon (2015). *Explore the pillars of Smart Cities solutions*. Acedido em 21, Janeiro, 2016, em http://www.verizonenterprise.com/solutions/connected-machines/*Smart-cities*/Verizon (2015).

- Whaley, E. (2015). *The "Internet of Things" – Is Legislation Coming?* Acedido em 24, Abril, 2016, em http://www.troutmansanders.com/the-internet-of-things--is-legislation-coming-02-03-2015/

- Wheatley, M. (2015). *Intel Survey: Smart homes to be a Commonplace by 2025?* Acedido em 10, Março, 2016, em http://realtybiznews.com/intel-survey-*Smart*-homes-to-be-commonplace-by-2025/98730580/

- Witchalls, C. (2013). *The Internet of Things business index: A quiet revolution gathers pace*. Acedido em 15, Abril, 2016, em https://www.arm.com/files/pdf/EIU_Internet_Business_Index_WEB.PD

- A World Foundation for Smart Communities (2012), *THE CONCEPT OF 'SMART CITIES'. TOWARDS COMMUNITY DEVELOPMENT?* Acedido em 12, Julho, 2016, em http:// http://www.netcom-journal.com/volumes/articlesV263/Netcom375-388.pdf

- WP29 (2014). *Opinion 8/2014 on the on Recent Developments on the Internet of Things.* Acedido em 28, Maio, 2016, em http://ec.europa.eu/justice/data-protection/article-

29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

- Yin, R. (2003). Case Study Research: *Design* and Methods

- *Z-Wave* Alliance (2014). *About Z-WaveTechnology*. Acedido em 14, Abril, 2016, em http://*z-wave*alliance.org/about_*Z-wave*_technology/

- Zemlin, J. (2014). *Technology Leaders Establish Open Interconnect Consortium to Advance Interoperability for* IOT. Acedido em 18, Abril, 2016, em http://usatcorp.com/industry-leaders-establish-open-interconnect-consortium-advance-interoperability-internet-things/

- *Zigbee* (2016). *Zigbee Alliance Creating End-to-End IoT Product Development Solution that Brings Its Industry-Leading Applications Library to Thread Group's IP Network Protocol.* Acedido em 24, Maio, 2016, em http://www.*Zigbee*.org/*Zigbee*-alliance-creating-end-to-end-IoT-product-development-solution-that-brings/

ANEXOS

Anexo 1 – Questionário Geral

Privacidade e segurança dos dados na IoT
Questionário – (Nome da organização)

1) Segundo dados divulgados pelo Gartner, 6,4 biliões de "coisas" conectadas estarão em uso até 2016, o que significa 30% a mais que em 2015. De que forma o(a) (nome da organização) está a ver este crescimento exponencial da Internet das Coisas? Já previam este boom da conectividade entre dispositivos?

.

2) Na vossa opinião, Portugal está a fazer uma boa aposta na IoT? Se sim, quanto tempo acham que vai demorar até as *Smart Cities* serem uma realidade em Portugal?

3) De que forma o(a) (nome da organização) se está a posicionar em relação à IoT?

4) De que forma os serviços e produtos de IoT do(a) (nome da organização) estão construidos de forma a garantir a privacidade do consumidor e a segurança dos seus dados?

5) Quais são, no entendimento do(a) (nome da organização), os maiores desafios que os fornecedores de produtos IoT podem ter de forma a assegurar a privacidade e segurança dos dados dos seus clientes?

6) Testes realizados pela HP encontraram, em média, 25 vulnerabilidades em cada dispositivo IoT examinado. Os testes indicam que os dispositivos IoT examinados apresentaram ameaças como o heartbleed (divulgação dos dados do utilizador), vulnerabilidade a ataques e grandes falhas nos processos de autorização de acesso, encriptação e construção de *interface*s. Acham que este irá ser um problema presente e futuro das IoT, ou apenas se deve ao facto de ser uma realidade recente, e por isso a segurança dos dispositivos ainda está por evoluir?

7) A principal questão sobre a privacidade na Internet das Coisas penso que ainda estará por responder: quem atuará como fiscal sobre esse mercado?

Pedro Santos
Dissertação de Mestrado em Sistemas de Informação Organizacionais – ESCE IPS

Anexo 2 – Questionário preenchido - SAS

1) Segundo dados divulgados pelo Gartner, 6,4 biliões de "coisas" conectadas estarão em uso até 2016, o que significa 30% a mais que em 2015. De que forma o SAS está a ver este crescimento exponencial da Internet das Coisas? Já previam este boom da conectividade entre dispositivos?

R: Sim, o SAS tem estado a acompanhar passo a passo esta tendência que entende transformadora e está a fazer muito trabalho nesta área.
Existem diferentes áreas de desenvolvimento nas soluções SAS onde este tema é fundamenta, por exemplo:

- No desenvolvimento de uma solução de *Event Stream Processing* que permite tratar eventos em tempo real e aplicar regras e modelos analíticos;
- No desenvolvimento de nova tecnologia e modelos analíticos – Asset Performance Analytics - com uma aplicação prática a exemplos de tempo real. Como por exemplo na monitorização do funcionamento das Turbinas Eólicas, frotas de transporte, antenas de comunicação etc;
- Na melhoria das tecnologias de análise e visualização dos dados para poderem funcionar com dados em tempo real.

2) Na vossa opinião, Portugal está a fazer uma boa aposta na IoT? Se sim, quanto tempo acham que vai demorar até as *Smart Cities* serem uma realidade em Portugal?

R: Portugal tem feito alguns esforços e desenvolvido projetos nesta área mas de forma comparativa com outros países europeus está longe de estar a fazer uma boa aposta. A questão principal tem no nosso entendimento a ver com a falta de programas e políticas governamentais ou regulamentação que promova estes desenvolvimentos.
No que respeita às *Smart Cities* o conceito é muito abrangente e é muito difícil prever quando podemos ter uma cidade verdadeiramente inteligente. Alguns projetos como por exemplo de monitorização do consumo de energia de forma digital ou de gestão de trafego ou comunicações têm sido bem-sucedidos mas, para se ter um nível de integração destes projetos ou passar daqui para gestão centralizada dos principais recursos duma cidade vai levar algumas décadas, isto porque tem de se refazer alguns projetos estruturantes que são muito dispendiosos

3) De que forma o SAS se está a posicionar em relação à IoT?

R: Como o principal fornecedor do mercado capaz de tratar grandes volumes de informação em tempo real e simultaneamente, trazer um nível de tratamente "inteligente" a esta informação com a aplicação de real-time analitics. Na verdade, o SAS está a apostar fortemente naquilo que chama a analítica das coisas.
O nosso entendimento é que só com a utilização de modelos analíticos em tempo real podemos verdadeiramente acrescentar valor às diferentes áreas de negócio que têm à sua disposição esta informação. Alguns exemplos são: a identificação de situação de fraude em tempo real em cartões de crédito ou acesso a sistema de informação corporativos – *Cybersecurity*; a identificação e antecipação de situações de falha no funcionamento de dispositivos críticos para as empresas como: frotas de veículos, geradores, antenas, ATM's etc; a otimização do funcionamento de dispositivos como os pontos de venda – vender machines; a monetização de dados com base nos perfis de utilização dos consumidores dependendo da sua localização e atividade, etc.

4) De que forma os serviços e produtos de IoT do SAS estão desenhados de forma a garantir a privacidade do consumidor e a segurança dos seus dados?

R: No que respeita à privacidade e segurança o SAS segue os *standards* do mercado e a legislação em vigor. Uma preocupação em particular tem sido com os aspetos associados à encriptação e o SAS garante que todos os dados e acessos dos utilizadores podem ser feito num ambiente seguro encriptado.

5) Quais são, no entendimento do SAS, os maiores desafios que os fornecedores de produtos IoT podem ter de forma a assegurar a privacidade e segurança dos dados dos seus clientes?

R: São bastante diversos e complexos, os mais importantes na opinião do SAS são:

- Garantir que existe uma arquitetura de sistemas de base suficientemente aberta e flexível para acomodar os (novos) *standards* e desenvolvimento no que respeita à segurança e encriptação dos dados;
- Garantir que são desenvolvidos *standards* de mercado abertos e aceites pelos diferentes fornecedores para a comunicação, armazenamento e processamentos dos dados da IoT;
- Garantir que a legislação evolui num sentido prático e tecnicamente exequível e que é efetivamente integrada e aplicada nos sistemas disponibilizados.

6) Testes realizados pela HP encontraram, em média, 25 vulnerabilidades em cada dispositivo IoT examinado. Os testes indicam que os dispositivos IoT examinados apresentaram ameaças como o heartbleed (divulgação dos dados do utilizador), vulnerabilidade a ataques e grandes falhas nos processos de autorização de acesso, encriptação e construção de *interface*s. Acham que este irá ser um problema presente e futuro das IoT, ou apenas se deve ao facto de ser uma realidade recente, e por isso a segurança dos dispositivos ainda está por evoluir?

R: O problema da segurança e aceso aos dados vai ser sempre um problema no mundo do IT e em particular neste ambientes onde os dados estão muito descentralizados e exigem sistema de comunicação e integração complexos. Apesar de na realidade atual, os consumidores darem mais importância ao preço do produto, do que à segurança e privacidade do mesmo, muito do trabalho já está feito nas três principais áreas:

- No processamento local com a disponibilização ambiente *Linux* e *Browsers* seguros;
- Nas comunicações seguras/encriptadas entre os sistemas locais e o processamento centralizado;
- Nos sistemas para o processamento centralizado que podem funcional “on-premisses” ou em “*cloud*” com arquiteturas muito seguras.

7) A principal questão sobre a privacidade na Internet das Coisas penso que ainda estará por responder: quem atuará como fiscal sobre esse mercado?

R: A questão da regulamentação e da sua aplicabilidade terá necessariamente de se resolver e evoluir em linha com os desenvolvimentos tecnológicos e com os requisitos e direitos dos consumidores. Quem legislará deverá ser sempre a autoridade máxima de regulação do ambiente onde os dados estão a ser tratados e ou utilizados, no nosso caso a União Europeia, e quem cuidará da aplicabilidade dessa regulamentação serão os diferentes organismos locais, no nosso caso a CNPD, ANACOM etc.

Pedro Santos
Dissertação de Mestrado em Sistemas de Informação Organizacionais – ESCE IPS

Anexo 3 – Questionário preenchido - Microsoft

1) Segundo dados divulgados pelo Gartner, 6,4 biliões de "coisas" conectadas estarão em uso até 2016, o que significa 30% a mais que em 2015. De que forma A Microsft está a ver este crescimento exponencial da Internet das Coisas? Já previam este boom da conectividade entre dispositivos?

R: A Microsoft está a posicionar-se no mercado IoT com os seguintes produtos:

- Azure IoT Hub – *Software* para recolher informação de dispositivos (sensores, PCs) (lado do servidor)

- Windows Core:
  - Windows 10 – Sistema operativo que corre nos dispositivos IoT (raspberry Pi) (lado do cliente) – Como é windows, tem segurança (certificados que evitam jailbreak).
  - Band 2 – Pulseira que rastreia dados gerados pelo utilizador, como os batimentos cardíacos, qualidade do sono, calorias, conexão com o telemóvel, etc.
  - Hololens - é o primeiro computador holográfico com o Windows 10. É totalmente isolado – sem fios, telefones ou necessidade de ligação a um PC. Microsoft HoloLens permite disfrutar de hologramas no nosso ambiente físico e fornece uma nova maneira de ver o mundo.

2) Na vossa opinião, Portugal está a fazer uma boa aposta na IoT? Se sim, quanto tempo acham que vai demorar até as *Smart Cities* serem uma realidade em Portugal?

R: As empresas em Portugal, estão a fazer um bom trabalho na implementação da realidade IoT no país. No caso da Microsoft, não se limita apenas a vender produtos específicos para consumidores finais, apostando sobretudo na sua plataforma Azure para IoT, especificamente criada para as organizações.

3) De que forma a Microsoft se está a posicionar em relação à IoT?

R: A resposta a esta pergunta vai ao encontro da resposta dada na 1ª pergunta.

4) De que forma os serviços e produtos de IoT da Microsoft estão desenhados de forma a garantir a privacidade do consumidor e a segurança dos seus dados?

R:

- Segurança:
  - Dispositivo - Pin do telemovel, etc;
  - Em trânsito - Protocolo garante a encriptação do dispositivo – Protocolo AMQT);
  - Em repouso: 1) segurança fisica dos datacenters, 2) segurança ao nivel da rede- logica da firewall – microsoft uma tem uma *red team* que só realiza ataques aos servidores, e tem uma *blue team* que só defende esses mesmos ataques e mede os tempos de

resposta. 3) ao nível do host e 4) segurança ao nível do *hardware* (servidor protegido por password de 2h dada por um processo).

- Privacidade:
  - Garantir que os dados que têm não fazem nada com eles (como a google faz publicidade dos seus dados).

- *Compliance*:
  - A Microsoft para além de cumprir e ter certificações nas mais diversas normas internacionais de *compliance*, como a ISO 27001, EUMC, HIPAA, etc., assume contratualmente com os seus consumidores, o cumprimento da sua privacidade e segurança, onde conta com uma série de controlos específicos, desde encriptação de dados, monotorização de incidentes, controlo de acessos, gestão de conta, etc.

- Transparência:
  - Existe um contrato com a entidade sobre a transparência dos serviços prestados

5) Quais são, no entendimento da Microsoft, os maiores desafios que os fornecedores de produtos IoT podem ter de forma a assegurar a privacidade e segurança dos dados dos seus clientes?

R:
- Garantir que os dispositivos enviam informação cifrada;
- Aplicações com encriptação são mais caras e ficam mais lentas

6) Testes realizados pela HP encontraram, em média, 25 vulnerabilidades em cada dispositivo IoT examinado. Os testes indicam que os dispositivos IoT examinados apresentaram ameaças como o heartbleed (divulgação dos dados do utilizador), vulnerabilidade a ataques e grandes falhas nos processos de autorização de acesso, encriptação e construção de *interface*s. Acham que este irá ser um problema presente e futuro das IoT, ou apenas se deve ao facto de ser uma realidade recente, e por isso a segurança dos dispositivos ainda está por evoluir?

R: Por agora, os consumidores preferem ter um dispositivo barato e menos seguro, do que um dispositivo caro e seguro. No futuro, à medida que o preço da segurança for diminuindo, e a facilidade em garantir essa mesma segurança, os produtos IoT irão ter um paralelismo entre o preço/qualidade/segurança.

7) A principal questão sobre a privacidade na Internet das Coisas penso que ainda estará por responder: quem atuará como fiscal sobre esse mercado?

R: Quem atua como fiscal na Internet? A resposta a esta pergunta passa muito por aí.

Anexo 4 – Questionário preenchido - Oracle

1) Segundo dados divulgados pelo Gartner, 6,4 biliões de "coisas" conectadas estarão em uso até 2016, o que significa 30% a mais que em 2015. De que forma a Oracle está a ver este crescimento exponencial da Internet das Coisas? E se já previam este boom da conectividade entre dispositivos?

2) Na vossa opinião, Portugal está a fazer uma boa aposta na IoT? Se sim, quanto tempo acham que vai demorar até as *Smart Cities* serem uma realidade em Portugal?

3) De que forma a Oracle se está a posicionar em relação à IoT?

R: A Oracle fornece uma infraestrutura dimensionável para integrar e proteger os dados recebidos de todos os diferentes dispositivos e componentes de um ecossistema de Internet das Coisas (IoT). A nossa plataforma de IoT totalmente integrada fornece os dados e recursos de análise avançada, além de segurança total para a criptografia de dados, dispositivos e usuários.

- O Oracle Internet of Things (IoT) Cloud Service oferece a capacidade de analisar altos volumes de informações relacionadas à IoT, em tempo real, usando dispositivos conectados. Em sintonia com o foco da Oracle nos setores de atividades, o Oracle IoT Cloud Service é bem adaptado para casos de uso como monitorização e manutenção de equipamento remoto para o setor industrial e rastreio de ativos no setor da logística/transporte. O Oracle IoT Cloud Service permite que as organizações conectem-se facilmente a dispositivos que utilizam a IoT, analisem dados em tempo real e integrem completamente aplicações e processos de negócios com dados da IoT. Ele oferece topologias flexíveis para que os dispositivos se conectem ao Oracle IoT Cloud Service – usando bibliotecas de clientes, *software* de *gateway*, ou diretamente, usando a API REST. O produto é integrado estreitamente à plataforma Oracle PaaS e aos serviços SaaS com conectores prontos para uso, por exemplo, para o Oracle Business Intelligence Cloud Service, para permitir que os usuários corporativos executem análises de BI em dados processados pelo Oracle IoT *Cloud* Service.
- O Oracle Mobile Platform simplifica a mobilidade corporativa, permitindo que o cliente desenvolva, conecte e implemente com segurança qualquer aplicativo em qualquer dispositivo, por qualquer fonte de dados

4) De que forma os serviços e produtos de IoT da Oracle estão desenhados de forma a garantir a privacidade do consumidor e a segurança dos seus dados?

R: Como prioridade máxima para a Oracle, a segurança foi construída do zero no Oracle IoT *Cloud* Service, para facilitar a criação de relacionamentos de identidade e confiança com o dispositivo e pontos finais de aplicações. O ciclo de vida de todos os pontos finais e dispositivos conectados (seja de forma direta ou indireta) é gerenciado pelo Oracle IoT *Cloud* Service desde o registo inicial, passando pela ativação, até uma eventual desativação. Dentro desse processo, os pontos finais são registados e autenticados de forma exclusiva, de acordo com políticas estabelecidas pelo utilizador e implementadas usando OAuth2, e todas as mensagens são criptografadas usando HTTPS. A combinação desses recursos com as funcionalidades de segurança subjacentes do Oracle Public *Cloud* comprova a priorização da segurança por parte da Oracle para a IoT.

5) Quais são, no entendimento da Oracle, os maiores desafios que os fornecedores de produtos IoT podem ter de forma a assegurar a privacidade e segurança dos dados dos seus clientes?

6) Testes realizados pela HP encontraram, em média, 25 vulnerabilidades em cada dispositivo IoT examinado. Os testes indicam que os dispositivos IoT examinados apresentaram ameaças como o heartbleed (divulgação dos dados do utilizador), vulnerabilidade a ataques e grandes falhas nos processos de autorização de acesso, encriptação e construção de *interface*s. Acham que este irá ser um problema presente e futuro das IoT, ou apenas se deve ao facto de ser uma realidade recente, e por isso a segurança dos dispositivos ainda está por evoluir?

7) A principal questão sobre a privacidade na Internet das Coisas penso que ainda estará por responder: quem atuará como fiscal sobre esse mercado?

Pedro Santos
Dissertação de Mestrado em Sistemas de Informação Organizacionais – ESCE IPS

Anexo 5 – Questionário preenchido pelo aluno - IBM

1) Segundo dados divulgados pelo Gartner, 6,4 biliões de "coisas" conectadas estarão em uso até 2016, o que significa 30% a mais que em 2015. De que forma a IBM está a ver este crescimento exponencial da Internet das Coisas? E se já previam este boom da conectividade entre dispositivos?

R: Em Março de 2015, a IBM anunciou que vai investir 3 mil milhões de dólares nos próximos quatro anos na criação de uma nova unidade de negócio na área da Internet das Coisas (IoT) e que também está a desenvolver uma plataforma aberta baseada na *cloud* para ajudar os clientes e parceiros de negócio de todos os setores a integrarem melhor e em tempo real os dados e a informação das mais variadas fontes diretamente nas operações de negócio.
As novas soluções e ofertas IBM serão disponibilizadas numa plataforma aberta para, por um lado, levar aos programadores e operadores das empresas a capacidade de projetar e fabricar dispositivos cada vez mais e melhor conectados e, por outro, criar sistemas que tirem partido dos dados empresariais e da IoT para ajudar na tomada de decisões de negócio.

2) Na vossa opinião, Portugal está a fazer uma boa aposta na IoT? Se sim, quanto tempo acham que vai demorar até as *Smart Cities* serem uma realidade em Portugal?

R: O trabalho pioneiro da IBM na área de *Smart*er Planet e de *Smart*er *Cities* baseava-se já nas aplicações práticas da IoT e levou ao desenvolvimento de soluções que ajudassem a reduzir a criminalidade, a minimizar o risco no trabalho diário dos bombeiros ou a monitorizar a qualidade da água.

3) De que forma a IBM se está a posicionar em relação à IoT?

R: A IBM estima que 90% de todos os dados gerados por dispositivos como *Smartphone*s, tablets, veículos conectados e outros aparelhos nunca são analisados ou usados para tomar decisões. Sendo que mais de 60% desses dados começam a perder valor e atualidade milésimos de segundos depois de serem gerados. Para resolver esta questão, a IBM anuncia novas ofertas:

- IBM IoT *Cloud* Open Platform: Novos serviços de analítica para desenhar e disponibilizar soluções verticais na área da Internet das Coisas na IBM *Cloud* para os clientes da indústria. Esta plataforma aberta também está disponível para os clientes e parceiros do ecossistema IBM que queiram criar as suas próprias soluções orientadas para os dados. A IBM vai disponibilizar, por exemplo, um serviço baseado na *cloud* que vai ajudar as seguradoras a extrair novo conhecimento a partir de veículos conectados, com o objetivo de definir tabelas de preços mais dinâmicas e a prestação de serviços personalizados;
- Watson Internet of Things: Parceria entre a IBM e a Cisco resultou numa solução de grandes capacidades de business analytics na *Cloud*;
- IBM Bluemix IoT Zone: Novos serviços IoT a partir da plataforma-como-um-serviço IBM Bluemix que vai permitir a integração fácil de dados para o desenvolvimento e implementação de novas aplicações IoT baseadas na *cloud*, ou melhorar as atuais;
- IBM IoT Ecosystem: Expansão do ecossistema de parceiros na área da Internet das Coisas, como as empresas AT&T, ARM, Semtech e The Weather Company – de modo a garantir a integração segura e contínua de soluções e serviços de dados na plataforma aberta da IBM.

4) De que forma os serviços e produtos de IoT da IBM estão desenhados de forma a garantir a privacidade do consumidor e a segurança dos seus dados?

5) Quais são, no entendimento da IBM, os maiores desafios que os fornecedores de produtos IoT podem ter de forma a assegurar a privacidade e segurança dos dados dos seus clientes?

R: Na opinião da IBM, a segurança e privacidade dos dados dos consumidores devem ter em atenção duas perspetivas: a dos fabricantes das coisas – o *design* e construção de produtos e sistemas IoT seguros; dos operadores das coisas – a utilização correta e segura dos produtos ou sistemas IoT implementados.

6) Testes realizados pela HP encontraram, em média, 25 vulnerabilidades em cada dispositivo IoT examinado. Os testes indicam que os dispositivos IoT examinados apresentaram ameaças como o heartbleed (divulgação dos dados do utilizador), vulnerabilidade a ataques e grandes falhas nos processos de autorização de acesso, encriptação e construção de *interface*s. Acham que este irá ser um problema presente e futuro das IoT, ou apenas se deve ao facto de ser uma realidade recente, e por isso a segurança dos dispositivos ainda está por evoluir?

R: Segundo a opinião da IBM, esta realidade será ultrapassada à medida que o preço da privacidade e segurança dos produtos for diminuindo.

7) A principal questão sobre a privacidade na Internet das Coisas penso que ainda estará por responder: quem atuará como fiscal sobre esse mercado?

Pedro Santos
Dissertação de Mestrado em Sistemas de Informação Organizacionais – ESCE IPS

Anexo 6 – Questionário preenchido pelo aluno - HP

1) Segundo dados divulgados pelo Gartner, 6,4 biliões de "coisas" conectadas estarão em uso até 2016, o que significa 30% a mais que em 2015. De que forma a HP está a ver este crescimento exponencial da Internet das Coisas? E se já previam este boom da conectividade entre dispositivos?

2) Na vossa opinião, Portugal está a fazer uma boa aposta na IoT? Se sim, quanto tempo acham que vai demorar até as *Smart Cities* serem uma realidade em Portugal?

3) De que forma a HP se está a posicionar em relação à IoT?

R: A Hewlett Packard Enterprise oferece um dos portfólios mais abrangentes de soluções de computação da IoT, análise de dados, segurança e conectividade, além de um ecossistema de parceiros de nível superior. Elas incluem:

- Computação: A HPE otimiza o valor da análise da IoT por meio de plataformas de computação comprovadas desde a borda até a nuvem — permitindo absorção, computação e análise de dados. As ofertas da HPE na borda incluem HPE Moonshot, servidores ProLiant e sistemas HPE Edgeline IoT.
- Conectividade: As soluções da HPE unificam o acesso, o gerenciamento e a configuração de dispositivos — possibilitando uma conectividade segura em qualquer ambiente operacional desde a borda até a nuvem. Ofertas incluem equipamentos de rede Aruba e HPN.
- Segurança: A HPE Security permite que as organizações reduzam e respondam pró-ativamente aos riscos inerentes que os dispositivos da IoT apresentam, incluindo maior conectividade e uma superfície de ataque mais ampla. O HPE Security Fortify fornece testes de segurança abrangentes em dispositivos, redes, dispositivos móveis e nuvens. Além disso, o HPE SecureData suporta proteção centrada em dados estáticos, em uso e em movimento para dados de dispositivos da IoT. Outras ofertas incluem o Aruba ClearPass e soluções Suite B, que propiciam controle de acesso à rede e criptografia de dados.
- Análise de dados: Com seu amplo portfólio de soluções que incluem *software*, *hardware* e serviços, a HPE pode utilizar dispositivos e sensores como novas fontes de dados, para criar insights históricos e preditivos e liberar resultados de negócios. As soluções da HPE para análise de dados da IoT incluem o portfólio HPE Vertica Analytics (*software*), infraestrutura otimizada para big data (*hardware*), Aruba Meridian Service e Analytics & Location Engine (dados contextuais e de localização).
- Serviços: A HPE oferece um pacote abrangente de serviços para reunir e oferecer suporte a soluções de conectividade, segurança, dados e computação para acelerar o retorno do investimento para clientes com iniciativas da IoT.
- Ecossistema: A HPE possui um ecossistema global e próspero de parceiros de alto nível que inclui fornecedores de soluções do setor, ISVs, SIs e fornecedores de tecnologia da IoT. Por exemplo, como membro do Microsoft Azure certificado para Internet das coisas (IoT), a HPE irá ajudar as empresas a colocar as soluções da IoT em funcionamento rapidamente com um ecossistema de dispositivos e plataformas.

4) De que forma os serviços e produtos de IoT da HP estão desenhados de forma a garantir a privacidade do consumidor e a segurança dos seus dados?

5) Quais são, no entendimento da HP, os maiores desafios que os fornecedores de produtos IoT podem ter de forma a assegurar a privacidade e segurança dos dados dos seus clientes?

R: Um estudo da HP concluiu que 100% dos dispositivos de segurança doméstica avaliados contêm vulnerabilidades significativas, incluindo falhas na segurança de senha, criptografia e problemas de autenticação. Neste cenário, o estudo revela como o mercado está mal equipado do ponto de vista de segurança para o crescimento esperado em torno da IoT e questiona se os dispositivos de segurança conectados realmente tornam as residências mais seguras.

Para o estudo, a HP utilizou o HP Fortify On Demand - plataforma de testes de aplicações - e avaliou dez dos principais sistemas de segurança do mercado norte-americano com componentes de aplicações móveis e de nuvem. Entre as principais conclusões, descobriu que nenhum dos sistemas requeria o uso de uma senha forte e que 100% deles falharam em oferecer uma autenticação de dois fatores.

Questões com privacidade também foram abordadas pelo estudo. Todos os sistemas coletaram alguma forma de informação pessoal como nome, endereço e até mesmo números de cartões de crédito. A exposição dessas informações pessoais é preocupante devido aos problemas de busca de conta em todos os sistemas.

É importante observar que o uso de vídeo é o principal recurso de muitos sistemas de segurança doméstica, com visualização disponível por meio de aplicações móveis e *interface*s de web com base em nuvem. A privacidade de imagens de vídeo da parte interna da residência torna-se uma preocupação extra.

Para Jason Schmitt, vice-presidente e gerente geral da Fortify, linha de produtos do grupo Enterprise Security Products da HP, consumidores devem ser cuidadosos em relação à adoção de medidas que parecem simples e práticas. Da mesma forma, fabricantes de dispositivos devem assumir a responsabilidade de integrar segurança dos seus produtos para evitar expor seus clientes a sérias ameaças.

6) Testes realizados pela HP encontraram, em média, 25 vulnerabilidades em cada dispositivo IoT examinado. Os testes indicam que os dispositivos IoT examinados apresentaram ameaças como o heartbleed (divulgação dos dados do utilizador), vulnerabilidade a ataques e grandes falhas nos processos de autorização de acesso, encriptação e construção de *interface*s. Acham que este irá ser um problema presente e futuro das IoT, ou apenas se deve ao facto de ser uma realidade recente, e por isso a segurança dos dispositivos ainda está por evoluir?

7) A principal questão sobre a privacidade na Internet das Coisas penso que ainda estará por responder: quem atuará como fiscal sobre esse mercado?

Pedro Santos
Dissertação de Mestrado em Sistemas de Informação Organizacionais – ESCE IPS