9ª ed

mHealth: o impacto da nova diretiva Europeia de proteção de dados, caso de uso e avaliação

Ricardo Jorge Tomé Rodrigues Pires

MESTRADO EM
INFORMÁTICA MÉDICA
2º CICLO DE ESTUDOS

Setembro de 2016

9ª ed

mHealth: o impacto da nova diretiva Europeia de proteção de dados, caso de uso e avaliação

Ricardo Jorge Tomé Rodrigues Pires

MESTRADO EM
INFORMÁTICA MÉDICA
2º CICLO DE ESTUDOS

Orientador
Prof. Doutor Luís Antunes, professor associado da FCUP

Setembro de 2016

"O tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais." – Artº 2º, da Lei 67/98, de 26 de Outubro

Agradecimentos

Ao Professor Doutor Luís Antunes pela ajuda na escolha, no apoio, na dedicação, no incentivo e na orientação deste projeto académico que culminará na obtenção do grau de mestre.

Ao Pedro Cabral pelo seu contributo no desenvolvimento deste trabalho.

A todos que, direta ou indiretamente, contribuíram com um pouco do seu tempo para a construção deste trabalho, dentro e fora de paredes.

Também á minha namorada por todo o apoio que deu e continua a dar.

Por fim, mas nunca em último lugar, aos meus pais que com a ajuda deles este trabalho não seria impossível, mas teria sido certamente muito mais pesado.

Resumo

Proteção de dados e a privacidade na internet são termos que entraram no dia-a-dia de milhões de cidadãos a nível mundial. Fruto de graves revelações para a comunicação social sobre o abuso dos dados privados de cidadãos anónimos, forçaram a comunidade europeia a agir de forma célere a travar este tipo de prática nociva. O acordar para esta nova realidade obrigou a alterações profundas na regulamentação na forma como o fluxo de dados através da internet funcionava. Esta tese foca-se nas novas alterações ao regulamento da proteção de dados, relacionando a forma como as aplicações móveis relacionadas com a saúde tratam dos dados pessoais e sensíveis dos diversos utilizadores, e de que forma os mesmos estão protegidos quanto à sua privacidade. O alvo principal desta análise tem por base o mercado português e todas as aplicações móveis de ambiente *Android*, que sejam classificadas como aplicações "médicas" ou aplicações de "saúde e bem-estar".

Palavras-chave: Proteção de dados, privacidade, *Android*, aplicações móveis

Abstract

Data protection and privacy on the internet are terms that entered in millions of citizens lives worldwide. Due to some serious revelations to the media about the abuse of private data of anonymous citizens, led the European community to act in a fast way to stop this kind of harmful practice. The awakening to this new reality forced some serious changes to the way of how data flow through the internet was regulated. This work focuses on the new regulation of data protection in Europe, assessing the way of how health mobile applications process personal data and sensitive data from the users, and in what way the users are protected in terms of privacy. The main target of this analysis is the Portuguese market and all of the mobile applications from Android, which are classified as “medical” applications and “wellness and fitness” applications.

Keywords: Data protection, privacy, Android, mobile applications

Acrónimos

AES – *Advanced Encryption Standard*

AP – *Access Point*

ASLR – *Address Space Layout Randomization*

CBP – *College BeschermingPpersoonsgegevens*

CE – Comissão Europeia

CJEU – *Court of Justice of the European Union*

CIA – *Central Intelligence Agency*

CNPD – Comissão Nacional de Protecção de dados

CNPDPI – Comissão Nacional de Protecção de Dados Pessoais Informatizados

DPA – *Data Protection Authority*

FAQs – *Frequently Asked Questions*

FTC – *Federal Trade Commission*

GPEN – *Global Privacy Enforcement Network*

GPS – *Global Position System*

HIPAA – *Health Insurance Portability and Accountability Act*

MAC – *Media Access Control*

MMS – Multimedia Message Service

MSRM – Medicamentos Sujeitos a Receita Médica

MNSRM – Medicamentos não Sujeitos a Receita Médica

ND – Não Disponível

NSA – *National Security Agency*

OCDE – Organização para a Cooperação e Desenvolvimento Económico

PHI – *Protected Health Information*

PNV – Plano Nacional de Vacinação

PRISM – *Planning Tool for Resource Integration, Synchronization and Management*

S/MIME – *Secure/Multipurpose Internet Mail Extensions*

SMS – *Short Service Message*

SNS – Serviço Nacional de Saúde

SO – Sistema Operativo

SSL – *Secure Socket Layer*

TFUE – Tratado sobre o Funcionamento da União Europeia

TLS – *Transport Layer Security*

UDID –*Unique Device Identifier*

UE – União Europeia

WWW – *World Wide Web*

Índice

AGRADECIMENTOS ..... **III**

RESUMO ..... **V**

ABSTRACT ..... **VI**

ACRÓNIMOS ..... **VII**

ÍNDICE ..... **IX**

ÍNDICE DE TABELAS ..... **XI**

ÍNDICE DE FIGURAS ..... **XIII**

1. INTRODUÇÃO **2**

2. LEGISLAÇÃO/REGULAMENTAÇÃO **6**

2.1. *FRAMEWORK* LEGISLATIVO PORTUGUÊS 7

2.2. *FRAMEWORK* LEGISLATIVO EUROPEU 9

2.2.1. DIRETIVA 95/46/CE 11

2.2.2. NOVO REGULAMENTO EUROPEU DA PROTEÇÃO DE DADOS 13

2.3. UE *VS.* EUA 17

2.3.1. *SAFE HARBOR* 18

2.3.2. HIPAA 22

2.3.3. *PRIVACY SHIELD* 23

3. SISTEMA OPERATIVO MÓVEL **26**

3.1. ANDROID 27

4. PERMISSÕES **30**

4.1. PERMISSÕES E APLICAÇÕES EM ANDROID 31

4.2. TIPOS DE PERMISSÕES 33

4.3. RISCOS ASSOCIADOS 35

4.4. APLICAÇÕES EM PORTUGAL 38

4.5. VALIDAÇÃO DE APPS 40

4.5.1. *IMPLEMENTAÇÃO* 40

4.5.2. RESULTADOS 40

5. ESTUDOS ANÁLOGOS NA EU **44**

5.1. CASO ITALIANO 45

5.2. CASO HOLANDÊS 46

6. CONCLUSÕES/DISCUSSÃO 48

7. REFERÊNCIAS 52

ANEXOS 56

ANEXO I – LISTA DE PERMISSÕES 56

ANEXO II – LISTA DE APLICAÇÕES DE "SAÚDE E BEM-ESTAR" 58

ANEXO III - LISTA DE APLICAÇÕES "MÉDICAS" 67

Índice de tabelas

Tabela 1 - Permissões vs. riscos 37

Tabela 2 - Aplicações Android 38

Tabela 3 - Resumo dos resultados da validação das apps 42

Índice de figuras

Figura 1 - Lista de permissões de aplicações em Android v. 5.0.2 (a) e v. 6.0.1 (b)..... 32

Figura 2 - Ataque por Man in the Middle..... 40

1. Introdução

Nos últimos anos tem-se assistido a um desenvolvimento tecnológico impar com um crescimento exponencial nas comunicações. A par deste desenvolvimento foram surgindo produtos capazes de aproveitar as capacidades dos novos terminais de comunicação, de forma a facilitar a vida das pessoas, dando uma nova perspetiva sob as atividades diárias. Assim, este desenvolvimento catapultou a experiência que as pessoas têm nas suas atividades, tais como uma ida ao médico ou uma simples corrida, aproximando-as do que outrora estava apenas presente num filme de ficção científica. Através deste desenvolvimento houve, inclusive, um impacto no local de trabalho de uma grande parte da sociedade. Esta nova realidade tecnológica mais rápida, versátil e de mais fácil utilização, aumentou de forma drástica a produtividade dos trabalhadores para níveis que outrora só estavam ao alcance de equipas de trabalho, permitindo também uma maior liberdade que permite alternar de posto de trabalho tão rapidamente quanto sair do escritório e chegar a uma esplanada, continuando o trabalho já iniciado.

No entanto, nem tudo são facilidades. Este desenvolvimento tão acelerado acarreta problemas de regulamentação que nem sempre são percetíveis ao utilizador, até que algo grave aconteça. Como este *boom* tecnológico aconteceu nos últimos anos, nomeadamente a partir da entrada no séc. XXI, a regulamentação existente refere-se aos idos anos 90, não colocando a tecnologia existente atualmente a par do que está regulamentado em praticamente todos os países. E para este hiato, contribuíram e contribuem imensos fatores tais como a velocidade de desenvolvimento da tecnologia que está apenas limitada pela imaginação de quem desenvolve os produtos, pelas necessidades da sociedade e pelo capital disponível pelas empresas. Como existem várias entidades a desenvolver ideias e produtos, a urgência de colocar produtos inovadores no mercado é gigantesca. Na grande maioria das vezes existe a introdução de soluções no mercado para problemas que ainda não estão completamente definidos, ou em última instância ainda não existem de todo. E este tipo de atitude por parte das empresas perante o mercado coloca uma enorme pressão nas entidades reguladoras e governos a nível mundial, a fim de criar nova regulamentação para novos tipos de tecnologia e mercados emergentes.

Dado que criar nova regulamentação está dependente de diversos fatores, tais como só se conseguir regulamentar a utilização de um produto depois de o mesmo ser lançado no mercado, à luz da atual legislação da UE os produtos carecem de aprovação antes do

lançamento – *Conformité Européenne* (CE), e as instâncias pelos quais um projeto tem de passar até que seja formulado num projeto de lei até à lei *per se*. Existem outros fatores que podem ter um papel relevante neste tipo de atrasos tais como a vontade politica e/ou interesses económicos, lóbis, etc.

Dado que, à data é difícil, se não virtualmente impossível, regulamentar à escala global o mercado da internet, criam-se lacunas que são exploradas, por vezes até à exaustão, por várias grandes empresas, sem que sejam tomadas medidas sancionatórias. Visto não existir um consenso à escala global, são tomadas medidas internas, ou seja, cada país cria a sua própria regulamentação para a internet. Por outro lado, existe a realidade da Comunidade Europeia, onde a Diretiva 95/46/CE regulamenta o mercado da internet abrangendo todos os Estados-Membros, que são obrigados a seguir "*guidelines*" definidas.

Claramente não é a solução ideal para a resolução de um problema global, mas é uma solução mais eficaz do que o modelo onde cada país constrói a sua própria regulamentação, acabando assim por existir uma maior uniformidade. Vendo este problema da perspetiva da empresa que desenvolve produtos para terminais móveis, entre os quais aplicações móveis, é mais fácil criar *guidelines* para os seus produtos tendo como alvo vários países com as mesmas regras, do que ter que adaptar os seus produtos à realidade de cada país. Do ponto de vista do utilizador destas aplicações, este tipo de realidade é uma vantagem imensa visto que os seus direitos serão mais facilmente acatados por estas empresas.

A tendência do mercado para o aumento contínuo da utilização de aplicações na área da saúde e bem-estar, bem como aplicações médicas fez com que as empresas vissem aqui um novo mercado e uma potencial fonte de receitas. E é neste ponto que reside um dos principais problemas na falta de regulamentação do mercado. Dado que na EU a última diretiva de proteção de dados data de 1995, está completamente desenquadrada com a realidade atual. Já por diversas vezes se tentaram criar mecanismos de forma a proteger os cidadãos europeus tanto de empresas europeias bem como "estrangeiras", acabando por falhar por diversas razões. E foi esta falha na regulamentação que grandes empresas exploraram durante anos, tendo acesso a dados de cidadãos europeus, utilizadores deste tipo de aplicações, considerados em várias situações sensíveis. Este tipo de prática era ocultada do utilizador, não tendo consciência de que a aplicação faria recolha de dados, e que estes seriam utilizados pela empresa para os mais diversos fins, tais como a utilização para publicidade personalizada, ou em última instância venda a outras empresas, podendo em alguma altura esta prática prejudicar o utilizador.

Independentemente do fim dado aos dados, estes têm o potencial de gerar receitas avultadas para a empresa que recolhe e os vende, onde, salvo raras exceções, o utilizador estaria fora desta equação.

Com o novo regulamento europeu mais adaptado à realidade atual, espera-se proteger os cidadãos europeus desta prática tóxica e compulsivamente ocultada do utilizador deste tipo de aplicações.

O facto de a segurança informática, segurança dos dados pessoais e a privacidade ser tema que tem vindo a ganhar relevância a cada dia que passa, torna necessário fazer uma análise das fragilidades do sistema a que todos estamos sujeitos, sempre que utilizamos uma aplicação no nosso telemóvel. Por este motivo, esta tese tem como principal foco a exploração das fragilidades existentes em aplicações catalogadas como "saúde e bem-estar" e "médicas", fazendo referência a quais os perigos a que estamos sujeitos, e que tipo de abusos podemos sofrer por parte de terceiros.

Dado que o mercado das aplicações móveis é muito vasto é virtualmente impossível analisar pormenorizadamente em tempo útil, a análise conduzida limitar-se-á a aplicações móveis desenvolvidas em Portugal, ou que estejam associadas a marcas portuguesas, que estejam disponíveis na *Play Store* do *Android*, incluindo versões *free*, *freemium* e pagas.

Estruturalmente esta tese é constituída por 7 capítulos, sendo que os cinco aqui referidos constituem o núcleo desta tese. O segundo capítulo abrange a regulamentação pertinente ao tema, enunciando os pontos de cooperação entre a UE e os EUA, bem como o novo Regulamento Europeu em matéria de proteção de dados; o terceiro capítulo aborda o sistema operativo em análise; o capítulo quatro foca-se na temática das permissões existentes nas aplicações, no risco que lhes está inerente e na avaliação das aplicações analisadas no mercado português; o capítulo cinco apresenta dois casos em que se evidenciou a problemática da falta de regulamentação no mercado das aplicações móveis; por último o capítulo seis refere-se às conclusões de toda a análise feita às aplicações, bem como a interpretação do novo regulamento em função da análise de resultados.

2. Legislação/regulamentação

Num mundo cada vez mais ligado digitalmente, onde a presença de um computador ou de um dispositivo ligado à internet é uma constante, onde cada vez menos existe a necessidade de sair de casa para irmos ao banco, às compras, para falar com aquela pessoa com quem não vemos há anos, onde as empresas comunicam entre elas através da internet para realizarem os seus negócios, onde cada movimento por mais simples e banal que seja deixa uma marca quase permanente, torna-se necessário existir algum tipo de regulamentação deste espaço que lida com diversas pessoas, diversas entidades e diversos países.

A proteção de dados não é um tema dos últimos anos, nem tão pouco surgiu com a internet. Existem registos da necessidade de proteção de dados desde o início do Séc. XIX, Samuel Warren e Louis Brandeis escreveram o artigo *"The right to privacy"* motivados apenas pela divulgação da fotografia e da imprensa. Também durante a Segunda Guerra Mundial houve várias leis emitidas por alguns países de forma a proteger a identidade de judeus, evitando que fossem capturados pelo exército alemão (Langheinrich 2001).

Contudo, só em 1968 na Conferência Internacional das Nações Unidas para os direitos humanos a temática da proteção de dados foi discutida a nível internacional. Desde esse momento o tema tem sido abordado por diversos países, tendo tido alguns desenvolvimentos a nível de legislação, principalmente em países da UE. No entanto, este tema foi novamente submetido a discussão pelo Comité de Ministros da OCDE, onde se emitiram *guidelines* com os princípios básicos para proteção e livre circulação de dados entre países. No entanto este tipo de *guidelines* não tinham poder legal, o que permitia que os mesmos fossem alterados de acordo com os interesses dos países (Cate 1995).

2.1. *Framework* Legislativo Português

A história da informática em Portugal remonta a anos anteriores à década de 80 do Séc. XX. Sendo ainda os primórdios do que é hoje a informática, com a sua forma tosca e arcaica, com problemas e soluções adotadas que, atualmente seria considerado ridículo, deu as bases para a rede informática que existe hoje no país. De acordo com (Fernandes de Almeida 1981) a informática em Portugal teve origem numa necessidade, profundamente agrícola, e desenvolveu-se um pouco às escuras, sem grande formação técnica, e sem uma legislação que suportasse uma tecnologia tão inovadora à época. Com o desenvolvimento de sistemas de comunicação dentro e além-fronteiras, surgiu a necessidade de se proceder a uma regulamentação deste tipo de atividade até então sem qualquer tipo de proteção legal. Dado ser um mercado pioneiro no país, já existiam mostras de o mesmo poder ser utilizado para questões pessoais, mesmo que o computador estivesse num ambiente laboral. Já na década de 80 do século passado começaram a ser distribuídos computadores pessoais, apesar de os mesmos só se poderem ligar à rede em determinadas empresas, visto que à data não existia uma rede informática e de internet abrangendo o país, tal como hoje é conhecida.

É na primeira versão da Constituição da República Portuguesa de Abril de 1976, que questão da proteção de dados informáticos foi prevista através Artigo 35º. Contudo, só em Abril de 1991 surge a primeira lei que se foca na proteção de dados pessoais, transmitidos apenas em suporte informático. Definia a Lei nº 10/91, de 29 de Abril, vários aspetos que até então nunca haviam sido considerados, tais como qual o tipo de dados que são considerados pessoais e os que são de domínio público, o tratamento automatizado de dados, o fluxo de dados além-fronteiras, entre outros, sendo assim a base para todas as leis da mesma temática. É através desta lei que é criada uma autoridade regulatória especializada na proteção de dados do foro informático. Nasce assim a Comissão Nacional de Proteção de Dados Pessoais Informatizados – CNPDPI.

Dada a natureza desta tecnologia onde há desenvolvimentos quase diariamente, foram necessárias atualizações periódicas de forma a acompanhar esse mesmo progresso. De forma a reforçar a proteção de dados pessoais da lei anterior, foi promulgada a Lei nº 28/94, de 29 de Agosto. As alterações aos artigos 11º, 17º, 24º, 33º e 44º tiveram em vista as novas necessidades no mercado, bem como a crescente necessidade pela partilha de dados além-fronteiras.

Em Outubro de 1998 foi promulgada a Lei nº 67/98, de 26 de Outubro que transpõe para a ordem jurídica a Diretiva nº 95/46/CE do Parlamento Europeu e do Conselho,

revogando a anterior. Esta Lei vai de encontro aos objetivos da Comunidade Europeia, de criar relações mais próximas entre os Estados-Membros, de eliminar as barreiras entre estes e na temática da proteção de dados a uniformização das regras a nível da comunidade, de forma a assegurar a livre circulação das pessoas, das mercadorias, dos serviços e dos capitais.

Durante o seu período de vigência a Lei anterior manteve-se inalterada, sem sofrer qualquer tipo de atualização. Apenas no ano de 2015 a Lei nº 67/98, de 26 de Outubro foi atualizada pela Lei nº 103/2015, de 24 de Agosto, fazendo um aditamento de um artigo referente à inserção de dados falsos.

2.2. *Framework* Legislativo Europeu

A 13 de Dezembro de 2007, data da assinatura do Tratado de Lisboa entrando em vigor em Dezembro de 2009, várias reformas foram adotadas de forma a apoiar ou complementar as políticas dos Estados-Membros da UE. O Tratado de Lisboa instaurou uma hierarquia relativa às normas de direito derivado, tal como refere (Raffaelli 2015), estabelecendo nos artigos 289º, 290º e 291º do TFUE – Tratado sobre o Funcionamento da União Europeia, uma distinção entre atos legislativos, atos delegados e atos de execução. Considerando que o direito derivado é constituído pelos atos adotados pelos órgãos da UE, no desenvolvimento das competências que os tratados lhes conferem, estes atos não têm todos a mesma natureza jurídica, nem o mesmo alcance jurídico. Neste domínio, e de acordo com (Campos 2014), existem diversos instrumentos jurídicos para os processos legislativos definidos hierarquicamente.

Regulamentos

O regulamento, previsto no artigo 288º, possui três características essenciais sendo em primeiro lugar, de caráter geral, aplicando-se a uma generalidade de destinatários, tais como os Estados-Membros da UE. Em segundo lugar o regulamento goza de aplicabilidade direta, não necessitando de nenhum mecanismo de receção para vigorar internamente, devendo ser respeitado por todas as entidades (particulares, Estados-Membros, Instituições da União). A aplicabilidade direta depende apenas do preenchimento das condições de vigência e validade das normas da União. Em terceiro lugar, o regulamento é obrigatório em todos os seus elementos, o que significa que os destinatários não podem adaptar o seu conteúdo à sua realidade. Os regulamentos, são normativamente autossuficientes, ou seja, regulam a totalidade da matéria, não carecendo de alterações à forma original.

O regulamento visa uniformizar e garantir o direito da União em todos os Estados-Membros, tornando incompatíveis quaisquer normas nacionais que são incompatíveis com as disposições do regulamento.

Diretivas

As diretivas previstas no artigo 288º, caracterizam-se por serem atos da União que impõe aos Estados-Membros a realização de certos objetivos dentro de um certo prazo, deixando, no entanto, uma liberdade quanto à forma e ao meio de os alcançar.

A diretiva distingue-se do regulamento, visto que, ao contrário destes, as diretivas, apesar de poderem conter uma disciplina geral, têm como destinatários apenas os Estados-Membros. A diretiva, em oposição ao carácter obrigatório em todos os elementos do regulamente, apenas vinculam o Estado-membro quanto ao objetivo a alcançar. Enquanto o regulamento goza de aplicabilidade direta, a diretiva carece de um ato nacional de incorporação para poder vigorar internamente. Ou seja, o legislador nacional deve fazer uma transposição para o direito interno, que adapte o direito nacional aos objetivos fixados pela diretiva. Em Portugal, a transposição de diretivas deve revestir a forma de Lei ou Decreto-lei para um reconhecimento normativo.

Decisões, recomendações e pareceres

A decisão tem caráter obrigatório em todos os seus elementos, podendo ser individual ou geral. A noção de decisão foi alterada com o Tratado de Lisboa, visto que esta já não tem que indicar destinatários, aumentando assim o número de matérias e situações em que pode ser utilizada. Em princípio, as decisões não têm caráter geral, e a sua vigência depende da notificação.

As recomendações e os pareceres não criam quaisquer direitos ou obrigações, mas visam o fornecimento de indicações sobre a interpretação e o conteúdo do direito da UE.

2.2.1. Diretiva 95/46/CE

A Diretiva 95/46/CE teve a sua origem na não ratificação das *guidelines* com os princípios básicos para a proteção e livre circulação de dados entre países, emitidas pela OCDE (Organização para a Cooperação e Desenvolvimento Económico). Dado não existir uma uniformização nesta temática dentro da UE (União Europeia), no início dos anos 90 do séc. XX, a Comissão Europeia publicou um *draft* que em 1995 acabou por dar origem à primeira diretiva sobre a proteção de dados em solo europeu. Esta diretiva foi concebida com o principal objetivo de ser aplicada ao processamento de dados pessoais, processamento este que pode ter vários níveis de automatização, bem como ao processamento de dados que embora não fazendo parte de processamentos automáticos, estes poder ser associados a outros processos de agregação de dados.

Com a aprovação da Diretiva, e não tendo esta um carater vinculativo, carece de uma transposição para o direito interno de cada Estado-Membro. Com a adaptação da Diretiva à realidade de cada país, existirá uma uniformização no que toca à privacidade e proteção de dados dentro do espaço da UE, não estando estabelecido limites máximos para este tema. A diretiva estabelece, sim, limites mínimos que têm a condição de ser transversais a todos os Estados-Membros, sendo estes, segundo (Cate 1995), garantir que o tratamento de dados pessoais é preciso, atual, específico, explicito, relevante e não excessivo. Estava também previsto um processo de anonimização dos dados, processo este que visava garantir a não identificação da fonte dos dados, além do estritamente necessário ao inicialmente proposto. Todos os processamentos posteriores a um processo de anonimização, seja para fins históricos, estatísticos ou científicos, estão dependentes da salvaguarda que a legislação de cada país tenha em vigor, podendo não ser considerados incompatíveis com a Diretiva. No entanto, toda e qualquer circunstancia que ultrapasse os objetivos definidos pela Diretiva, prevê que os dados sejam eliminados ou retificados.

Contudo, todas os processos a que os dados possam estar sujeitos, desde a sua recolha a um qualquer tratamento, estão sujeitos a um consentimento válido atribuído pela pessoa em causa. Fica atribuída à legislação de cada país a responsabilidade de determinar um responsável pelos processamentos a executar, seja este público ou privado, e se este coloca em causa as liberdades fundamentais ou o direito à vida privada.

Existem, no entanto, exceções que preveem o processamento de dados sem o consentimento da pessoa. Na área da saúde é um dos casos onde é possível ter acesso a

dados sensíveis, bem como efetuar o processamento dos mesmos. Neste caso, a pessoa responsável por este processo encontra-se obrigada a estar sob sigilo profissional (Herveg & Poullet 2004).

Dado que a livre circulação de pessoas e bens é um dos pilares base pela qual a UE foi criada, e sendo os dados pessoais considerados como um bem, é essencial que estes possam ultrapassar fronteiras entre Estados-Membros, mantendo o mesmo nível de proteção do país de origem. Desta forma, a Diretiva considera que a existência de diferenças ao nível das legislações entre os diferentes Estados-Membros é um entrave à livre circulação de dados, tendo um impacto direto no exercício de diversas atividades económicas e sociais, bem como um impacto direto na liberdade do cidadão. Assim, a harmonização das leis nesta temática em todos os Estados-Membros promove uma eliminação deste tipo de obstáculos, promovendo um nível de proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados.

Ainda à luz desta Diretiva, as transferências de dados pessoais para países fora da UE foram tidas em consideração. Contudo, a norma gerou bastante contestação devido à rigidez com que a questão foi abordada. De acordo com o definido pela Diretiva, as transferência para países terceiros, só poderiam ser realizadas caso estes oferecessem o mesmo nível de segurança que a existente na UE. E por mesmo nível de segurança, entenda-se que segundo (Salbu 2000), as transferências teriam que obedecer aos princípios definidos pelos Artigos 25º e 26º que adequa as normas existentes na UE a terceiros, dando permissão a transferências quando estão asseguradas as condições exigidas, e cessando quaisquer transferências ou tentativas de transferências quando as condições não se encontram asseguradas.

2.2.2. Novo Regulamento Europeu da proteção de dados

A rapidez com que a tecnologia evoluiu nas últimas décadas transformou o panorama das comunicações a nível global. Hoje em dia existem novas formas de partilha de informação, tais como as redes sociais ou mesmo o armazenamento de informação em *cloud*. Paralelamente a estas novas práticas, os dados pessoais tornaram-se um bem extremamente valioso para um sem número de empresas. A utilização destes dados pode ser considerada um atentado à privacidade e uma ofensa à liberdade do indivíduo, colocando a sua integridade em causa aquando da má utilização dos mesmos.

Nos últimos anos tem-se verificado um grande desenvolvimento no que toca a redes sociais, principalmente o Facebook e o Twitter. Praticamente a par deste desenvolvimento existiu um crescimento exponencial na área da publicidade, tendo agora acesso à utilização intensiva de plataformas que antigamente não existiam. Com a invasão das redes sociais no dia-a-dia das pessoas, são várias as empresas que utilizam a imensa quantidade de dados gerados a cada minuto por milhões de utilizadores, para prestarem diversos tipos de serviços, tais como publicidade personalizada ao utilizador, venda desses mesmos dados a empresas terceiras, entre outros. Este tipo de prática é comummente experienciada quando um utilizador procura um determinado artigo numa loja *online*, onde nas visitas seguintes, as sugestões para compras estão de alguma forma relacionadas com as pesquisas anteriores. Isto acontece, também, numa rede social, onde qualquer sugestão que é feita ao utilizador, tem por base os "gostos", tipicamente designados de "*likes*", e todas as interações que são realizadas noutros *sites*.

Tendo por base o estudo realizado por (Furnell et al. 2007), este tipo de práticas, bem como a falta de sensação de controlo dos dados pessoais por parte dos utilizadores, faz com que exista uma quebra de confiança na utilização deste tipo de tecnologias. No espectro de todos os utilizadores existem determinados grupos que estão particularmente mais vulneráveis que outros, tal como os utilizadores pertencentes a faixas etárias mais baixas ou mais elevadas, onde a noção de segurança informática tende a desvanecer e as práticas de segurança são muitas vezes inexistentes. Mesmo utilizadores mais experientes podem experienciar algum tipo de vulnerabilidade, visto que pequenas interações podem eventualmente ser registadas.

Com vista a assegurar um elevado nível de proteção de dados, a restabelecer a confiança dos utilizadores e em maximizar o potencial da economia digital, incentivando o crescimento económico e a competitividade das empresas da UE, é necessário ter regras modernas e coerentes, com aplicação direta em toda a União.

A adoção da Diretiva 95/46/CE, foi um marco histórico em matéria de proteção de dados pessoais na Europa. Com a sua entrada em vigor há praticamente vinte anos, os seus objetivos continuam a ser tão válidos agora como no seu início, assegurando o funcionamento do mercado único europeu, bem como a proteção efetiva dos direitos e das liberdades das pessoas singulares. No entanto, o peso dos vinte anos faz-se sentir, fazendo com que a Diretiva não consiga acompanhar o desenvolvimento das novas tecnologias, nem das necessidades atualmente existentes na sociedade atual, não garantindo a eficácia necessária na proteção dos dados pessoais, nem o grau de uniformização que se exige na União.

Aquando da assinatura do Tratado de Lisboa, foi introduzida uma nova base jurídica tendo em consideração uma nova visão sobre a proteção de dados pessoais e a livre circulação dos mesmos, através do Artigo 16º do TFUE (Tratado sobre o Funcionamento da União Europeia). Por sua vez, em Janeiro de 2012, a Comissão Europeia apresenta a Reforma na Proteção de Dados na UE. Este novo quadro legislativo incluirá um regulamento que com a entrada em vigor substituirá a Diretiva até então existente, e uma nova diretiva que enunciará as regras relativas à proteção de dados pessoais tratados para efeitos de prevenção, investigação, deteção ou repressão de infrações penais e atividades judiciárias conexas. Em suma, o regulamento permitirá um melhor controlo das pessoas sobre os seus dados, e em simultâneo modernizará e uniformizará a legislação em todo o espaço da União. Por sua vez a diretiva centrar-se-á no sector judicial e criminal do quadro (European Commission 2015).

Este novo regulamento prevê que as pessoas possam ter um maior controlo e uma maior perceção sobre os seus dados pessoais que circulam na internet, principalmente em território europeu. De acordo com (Commission 2012), são definidos quatro pontos essenciais que estão à disposição dos utilizadores garantindo um maior nível de segurança e confiança:

- Direito ao acesso

  As pessoas terão mais e melhor acesso aos seus dados, e de que forma os mesmos são processados. Os dados devem estar disponíveis de uma forma simples e clara a todos;
- Direito à portabilidade dos dados

  Os dados devem ser poder transferidos de um *service provider* para outro de forma simples;

- Direito ao esquecimento

  Todas as pessoas têm o direito de ver os seus dados eliminados sempre que o desejem, ou quando já não existir qualquer interesse em mantê-los;
- Direito a ser notificado sempre que exista violação dos dados

  As pessoas devem ser prontamente notificadas sempre que uma base de dados, contendo os seus dados, seja comprometida, de forma a estas tomarem as devidas previdências;
- Aplicação mais eficaz das regras

  As entidades reguladoras terão a legitimidade para aplicar coimas até 4% do volume de faturação anual global, caso não cumpram o definido no regulamento.

Este novo quadro legislativo abrange regras ajustadas a um mercado único digital. Ou seja, a necessidade do mercado da atualidade exige que uma entidade ou empresa esteja em constante contato com os diversos parceiros, na sua maioria em países distintos, obrigando a que um enorme fluxo de informação seja transferido entre Estados-Membros. Esta realidade obriga a que exista uma grande compatibilidade entre as diversas legislações dos diferentes Estados de forma a existir o menor número de constrangimentos, tornando o mercado altamente competitivo. Desta forma, a unificação das regras entre países é um ponto essencial. Assim e de acordo com (European Commission 2015), o novo regulamento introduz regras mais atuais face às novas necessidades do mercado único digital:

- Um continente, uma lei

  Existirá apenas um conjunto de normas transversal a todos os Estados-Membros de forma a facilitar e tornar mais barato o comércio dentro da UE;
- *One-stop-shop*

  As empresas terão apenas de lidar com um DPA e não com 28;
- Regras Europeias em solo Europeu

  Todas as empresas externas à UE têm de se sujeitar às mesmas regras quando oferecem serviços à UE;
- *Risk-based aproach*

  As novas regras evitaram que as obrigações sejam do tipo *one-size-fits-all*, optando por avaliar o risco caso a caso;
- Regras adequadas à inovação

  O regulamento garantirá que existirão salvaguardas na proteção de dados incluídos nos produtos e serviços desde as fases iniciais do desenvolvimento.

Atualmente, no mundo globalizado, a aplicação destas regras fará com que os cidadãos europeus gozem dos mesmos direitos sempre que os seus dados sejam transferidos para países dentro da UE, bem como para países terceiros. Isto significa que as normas da EU nesta matéria devem ser aplicadas independentemente da localização geográfica da empresa ou do serviço do tratamento de dados.

2.3. UE *vs.* EUA

A política de proteção de dados não podia ser mais distinta entre os EUA e a UE. Na UE a proteção de dados tem, à data, a base na Diretiva 95/46/CE que garante uma espécie de uniformização nesta matéria em todos os Estados-Membros. Por sua vez, nos EUA não existe apenas uma entidade reguladora que seja dedicada a supervisionar toda a matéria de proteção de dados. A nível federal, em matéria de proteção e dados a responsabilidade em causa depende do tipo de lei ou tipo de regulamentação em causa. No contexto de serviços financeiros, existem várias entidades reguladoras aplicam a lei *Gramm-Leach-Bliley*. Por sua vez, na área da saúde o *Department of Health and Human Services*, aplica a HIPAA – *Health Insurance Portability and Accountability Act*. Para lá da indústria regulada, a FCT – *Federal Trade of Commission*, é a principal entidade reguladora, aplicando a *US. Section 5* da *FTC Act*, a principal ferramenta em matéria de proteção de dados.

Pelo facto de existirem grandes diferenças nesta matéria entre os dois lados do Atlântico, tornou-se imprescindível existir uma aproximação da proteção de dados dos EUA à legislação europeia de forma a estender a cobertura de proteção existente aos cidadãos europeus.

2.3.1. *Safe Harbor*

O interesse e a necessidade de a UE em regular o mercado digital único, no que toca à proteção dos direitos e liberdades dos cidadãos europeus, dentro desta, chocou com os interesses dos EUA, quando surgiu a necessidade de expandir esta necessidade para território norte-americano. Contudo, a abordagem em prática nesta temática diverge em vários aspetos da europeia. Como consequência, no final dos anos 90 deram-se inicio a negociações entre a UE e os EUA de forma a encontrar um ponto de equilíbrio entre as duas perspetivas em matéria de privacidade e proteção de dados, que levaram ao estabelecimento do *Safe Harbor* entre ambos.

Dada a abordagem tomada tanto pela UE como pelos EUA em matéria de proteção de dados serem completamente distintas, e de acordo com as regras definidas pela Diretiva 95/46/CE, os EUA foram reconhecidos como um país "não adequado" para a transmissão de dados de cidadãos europeus. O princípio por trás da proteção de dados existentes nos EUA prende-se com o facto de defenderem que a autorregulação por diferentes setores da economia, promove um desenvolvimento mais acelerado da tecnologia, não existindo assim um constrangimento através de leis. E neste ponto encontra-se um dos motivos da divergência, visto que, a UE defende que a utilização de leis equivalentes entre os Estados-Membros, promove-se uma maior fluidez na transmissão de dados entre países, bem como um nível de proteção e privacidade de dados superior. No entanto, o facto de ambos divergirem na forma como abordam o tema, ambos defendem que a proteção e privacidade de dados pessoais é necessária para a criação de um mercado único digital entre ambos.

Em 1998 torna-se claro que a Diretiva europeia implicaria graves consequências para as empresas norte-americanas, a não ser que os EUA conseguissem provar que o seu modelo de autorregulação fosse eficaz e fosse de encontro ao exigido pela UE, através da Diretiva. Com vista a um princípio de acordo entre a UE e os EUA, ainda em 1998, são publicados em carta aberta princípios para um "*Safe Harbor*" dirigido às empresas norte-americanas (Farrell 2003). Desta forma, objetivo principal destes princípios seria manter o mesmo tipo de regulamentação existente nos EUA, adaptando apenas a política de proteção de dados das empresas interessadas em manter a transferência de dados entre UE e EUA. Neste acordo estariam abrangidos qualquer tipo de dados pessoais, recebidos por uma empresa norte-americana, independentemente do suporte em utilização.

Tendo por base (Assey & Eleftheriou 2001), cada empresa que estivesse interessada em fazer parte do *Safe Harbor* teria de concordar com os sete princípios, resumidamente apresentados:

- Notificação

  As empresas devem informar a pessoa sobre que tipo de informação será recolhida, como será recolhida, a quem será divulgada, qual o propósito da sua recolha e de como podem contactar as entidades participantes no processo;
- Escolha

  A pessoa deve ter a opção de não participar nessa recolha de dados quando o propósito da recolha de informação não está de acordo com o objetivo inicialmente proposto;
- Acesso

  As empresas devem dar acesso aos dados recolhidos da pessoa para correções ou apagar informação que esteja incorreta;
- *Onward Transfer*

  Este principio é aplicado quando a empresa detentora dos dados pretende transferi-los para uma terceira entidade. Neste caso a empresa original tem de garantir que os terceiros oferecem o mesmo nível de proteção previsto na Diretiva europeia;
- Segurança

  As empresas portadoras dos dados devem garantir os níveis de segurança adequados de forma a prevenir eventuais maus usos desses mesmos dados, perdas, alterações, destruição e mesmo acesso não autorizados;
- Integridade dos dados

  A empresa compromete-se a não utilizar os dados de uma forma que viole o propósito inicial para o qual os dados foram recolhidos, ou para o qual a pessoa deu o seu consentimento. De forma a assegurar a integridade dos dados, as entidades devem tomar as devidas providencias para garantir que os dados são seguros para o uso pretendido, objetivos, completos e atualizados;
- Cumprimento

  Devem existir mecanismos que assegurem a aplicação destes princípios e consequências para a empresa quando os mesmos não são tidos em consideração.

Além dos princípios do *Safe Harbor* foram também definidas uma serie de perguntas frequentes, FAQ's, que dão uma interpretação dos princípios em casos mais específicos. Na totalidade são quinze perguntas que entre elas abrangem todos os aspetos enunciados no acordo.

No entanto, o *Safe Harbor* teve falhas desde o seu início, nomeadamente problemas na aplicação do acordo, uma vez que a sua aplicação só seria possível em empresas sobre jurisdição da FTC (*U.S. Federal Trade of Commission*). Ou seja, empresas que operavam fora da alçada da FTC não poderiam ser sujeitas ao acordo do *Safe Harbor*. Devido a falhas dentro do acordo, gerou-se muita controvérsia pelo facto de empresas norte-americanas que faziam recolha de dados diretamente na Europa não estarem sujeitas às mesmas condições que as restantes. A ambiguidade do Artigo 4º da Diretiva europeia fez com que o *Safe Harbor* não pudesse ser invocado em determinados casos (Efining et al. 2003).

Com o desenrolar de todos os eventos relacionados com as falhas na estruturação e implementação do *Safe Harbor*, houve dois casos que tiveram impacto a nível global, influenciando diretamente as decisões em torno do acordo e colocaram em causa, tanto a sua integridade como a sua continuidade.

Max Schrems, um estudante austríaco de direito processou o Facebook no seguimento de trabalho de curso onde se fazia referência à falta de consciência deste relativamente às políticas de privacidade e proteção de dados na Europa. Schrems acusa diretamente o Facebook de guardar toda a informação que havia sido eliminada por todos os utilizadores na Europa, bem como a utilização da função de reconhecimento facial em fotos de utilizadores, invadia a privacidade dos utilizadores.

No seguimento do caso trazido à luz por parte de Schrems, em Junho de 2013, Edward Snowden, um antigo trabalhador da CIA (*Central Intelligence Agency*) e da NSA (*National Security Agency*), fez a divulgação de documentos secretos que revelavam um programa de espionagem. Definido como PRISM (*Planning Tool for Resource Integration, Synchronization and Management*), era um programa de espionagem da NSA iniciado no mandato de George W. Bush como parte da *Protect America Act* de 2007. Anos mais tarde foram analisadas as possibilidades de expandir o programa a vigilâncias mais profundas a nível mundial a comunicações e armazenamento de informação, tal como serviços de *email*, chamadas de voz e vídeo, VoIP, transferência de dados e a redes sociais, dado que o maior fluxo de dados é realizado através os EUA.

À luz das revelações tanto de Schrems como de Snowden, o Parlamento Europeu colocou em causa o cumprimento do acordo do lado americano e com base numa decisão do CJEU – (*Court of Justice of the European Union*), em Outubro de 2015 suspende o fluxo de dados entre os dois lados do Atlântico, declarando o *Safe Harbor* como inválido (ECJ 2015).

Como consequência desta decisão, os EUA são declarados como "não adequados", deixando no limbo as empresas que transferiam dados da Europa para os EUA. Desta forma, as empresas são obrigadas a arranjar soluções de forma a cumprir os critérios impostos pela Diretiva e pelo CJEU, até à existência de uma nova decisão (Coudert 2015).

2.3.2. HIPAA

A *Health Insurance Portability and Accountabilit Act*, mais conhecida como HIPAA, é uma lei aprovada pelo Congresso dos Estados Unidos e promulgada pelo então presidente Bill Clinton em 1996, foi e é até à data uma das mais importantes reformas de saúde, introduzindo disposições para a privacidade e proteção de dados de saúde.

A HIPAA subdivide-se em cinco secções, cada uma focando-se em diferentes áreas da saúde norte-americana, sendo a primeira, *Health care access, portability and renewability*; a segunda, *Preventing health care fraud and abuse, administrative simplification, medical liability reform*; a terceira, *Tax-related provisions governing medical savings accounts*; a quarta, *Application and enforcement of group health insurance requirements*; e por último a quinta, *Revenue offset governing tax deductions for employers* (Ferenc 2013).

A HIPAA estrutura a forma como a privacidade é abordada pelas diversas entidades relacionadas com saúde nela visadas, dando a possibilidade de as pessoas acederem aos seus dados de saúde, bem como a prevenção do acesso indevido a estes dados. As regras de privacidade incluídas na lei, protegem todos e quaisquer dados de saúde que sejam passíveis de identificação, independentemente de os mesmos serem transmitidos ou simplesmente armazenados de forma eletrónica ou por qualquer outro meio conhecido da PHI (*Protected Health Information*). As regras incluídas além de regularem o armazenamento, o fluxo e a divulgação da PHI, regulam também a forma como os dados são obtidos, sendo através de uma entidade de saúde, uma seguradora ou qualquer outra entidade que seja reconhecida pela HIPAA e lide com dados de saúde, independentemente da finalidade pretendida (Alshugran & Dichter 2014; Alshugran et al. 2015).

A HIPAA entrou em vigor em Abril de 2003, e apesar de ser um regulamento dispendioso e com um nível de complexidade que aumentou a dificuldade de implementação, acabou por produzir grandes efeitos na indústria da saúde, aumentando o nível de confiança e segurança de todos os intervenientes.

2.3.3. *Privacy Shield*

Desde o fim do acordo de *Safe Harbor* que as transferências de dados entre os ambos os lados do Atlântico se encontravam numa espécie de limbo. Este tipo de transferências entre empresas que estavam abrangidas pelo acordo de *Safe Harbor*, tiveram que adotar medidas que com uma base legal e que pudessem salvaguardar a proteção de dados. De acordo com (Degraw et al. 2015) e (Van Overstraeten et al. 2015), estavam disponíveis algumas opções que possibilitavam o fluxo de dados tais como:

- O uso de modelos contractuais da Comissão ou acordos *ad hoc* ou intra-grupos;
- O estabelecimento de regras vinculativas entre empresas;
- Obter o "*consentimento inequívoco*" sobre os dados pessoais transferidos.

Em Fevereiro de 2016, chegou-se a um acordo político que definiu um novo *Framework* para o fluxo de dados entre UE e EUA, o *Privacy Shield*. Este novo *Framework* revoga e substitui todos os acordos anteriores em vigor. No entanto, este acordo requer à data, a aprovação por parte de todos os estados-membros, bem como do Parlamento Europeu.

Com a aplicação do *Privacy Shield*, são impostas duras obrigações às empresas norte-americanas de forma a ir ao encontro do requerido pelo CJEU (*Court of Justice of the European Union*), bem como pelas diferentes DPAs europeias. Algumas destas imposições passam pelo incremento das monitorizações e um cumprimento mais robusto e apertado das regras decretadas no acordo, face ao que havia sido imposto pelo *Safe Harbor*. De acordo com (European Commission 2016), o *Privacy Shield* foca-se principalmente em quatro categorias, essenciais à manutenção do fluxo de dados entre os dois lados do Atlântico:

- <u>Imposição de obrigações às empresas e uma aplicação mais robusta</u>

  Neste ponto reside uma maior transparência e uma maior eficácia no que diz respeito à aplicação dos novos mecanismos de supervisão, para que as empresas norte-americanas estejam em concordância com as regras subscritas. Ainda neste ponto, estão incluídas as salvaguardas na transferência de dados de entidades norte-americanas para países terceiros, "*onward transfers*". Como parte da supervisão, o *U.S. Department of Commerce* compromete-se a supervisionar a forma como as empresas cumprem as

regras impostas pelo acordo. No caso de falharem os termos do acordo, estas empresas enfrentam graves consequências;

- Estabelecimento de limites e salvaguardas ao acesso do Governo Norte-americano

  Pela primeira vez, o Governo norte-americano, fornece à UE garantias que o acesso a dados por parte de entidades públicas para a aplicação da lei, para segurança nacional ou por parte de outras entidades, estarão sujeitas a limitações, salvaguardas e mecanismos de supervisão. Os EUA estabelecerão mecanismos onde todas as queixas e investigações por parte da UE serão acompanhadas por uma *Ombudsperson* (cargo de alguém nomeado pelo governo que investiga queixas e tenta encontrar as melhores soluções, sendo que este cargo pode tem um certo nível de independência);

- Proteção do direito de privacidade dos cidadãos europeus com diversas compensações

  Qualquer cidadão europeu que considere que os seus dados são alvo de abuso, terá ao seu dispor medidas acessíveis de forma a fazer valer os seus direitos, tais como a resolução de problemas relacionados com o direito à privacidade, sem custos para o queixoso. É neste ponto que são também estipulados *deadlines* na resposta às eventuais queixas que possam surgir;

- Reunião de revisão anual do mecanismo

  Este ponto permitirá à Comissão Europeia avaliar regularmente o funcionamento do *Privacy Shield*, em todos seus aspetos, incluindo as limitações e as salvaguardas relacionadas com matéria de segurança nacional. A Comissão em conjunto com o *U.S. Department of Commerce* emitirão a avaliação juntamente com os reguladores europeus e norte-americanos e o provedor norte-americano.

Com o acordo alcançado entre ambas as partes, estão reunidas as condições para o que é esperado pela Comissão Europeia, desenvolvendo e promovendo bases legais para a proteção de dados e o direito à privacidade de cidadãos europeus. Desde o início da divulgação da intenção de estabelecer este novo acordo transatlântico, as empresas e

entidades interessadas, são incentivadas a fazer as devidas preparações para a implementação imediata do acordo, assim que este entre em vigor.

3. Sistema Operativo Móvel

A necessidade de as pessoas estarem em contacto permanente umas com as outras, é provavelmente tão antiga como a própria história do homem. Com o desenrolar da história da humanidade novas formas de comunicação foram encontradas, até que no passado recente, séc. XX, deu-se início à revolução tecnológica a nível das telecomunicações, onde os telemóveis desempenharam o papel principal. Nos últimos anos os telemóveis conheceram um desenvolvimento tal que permitiu estarem acessíveis às massas, onde anteriormente estavam apenas disponíveis às carteiras mais abastadas, dado os preços astronómicos que atingiam.

As primeiras versões eram bastante rudimentares nas suas funções e tinham simplesmente como funções básicas como, realizar chamadas e em alguns casos e um pouco mais tarde, o envio de SMS (*Short Service Message*). À medida que os telemóveis foram amadurecendo ganharam novas capacidades tais como guardar contactos, utilização de calendário, entre outras funções que permitem facilitar a vida das pessoas.

Com o desenvolvimento de mais e melhores capacidades computacionais, os anos os telemóveis foram adotando cada vez mais funcionalidades que até então eram restritas aos computadores. Desta forma, algumas gamas de telemóveis passaram a denominar-se *smartphones*, dadas as novas capacidades "inteligentes", passando a fazer parte do dia-a-dia das pessoas. Também a evolução do *software* teve um papel preponderante nesta conquista tecnológica. Com a contínua evolução da capacidade computacional dos telemóveis, também os SOs (Sistemas Operativos) foram evoluindo, capacitando os telemóveis com novas funcionalidades e aplicações, de novas formas de interação entre equipamentos e de novas formas de comunicação. Atualmente os telemóveis tem um elevado nível de personalização derivado das novas características dos SOs com que são equipados, chegando em certas situações a equiparar-se aos SOs existentes nos computadores.

3.1. Android

O Android é um sistema operativo *open-source*, o que significa que tem o seu código-fonte é disponibilizado ao público permitindo proceder a alterações à versão original do sistema, tal como praticado pela grande maioria de fabricantes de equipamentos que utilizem este SO. Este é desenvolvido pela Open Handset Alliance, liderada pela Google, e baseado no *kernel* do Linux, tendo aparecido ao público pela primeira vez em 2008, no seguimento do lançamento do iOS da Apple.

Antes de o Android ser chegar ao público na versão conhecida, o seu desenvolvimento foi um pouco atribulado, sofrendo alterações profundas, dado as novidades e preferências do mercado. Inicialmente, este tinha como alvo telemóveis sem *ecran* táctil, daí o primeiro protótipo ser um telemóvel baseado num Blackberry com teclado físico. Contudo, o lançamento do iPhone e do LG Prada, ambos de *ecran* tátil capacitivo, obrigaram a alterar profundamente o Android, direcionando-o para equipamentos com características semelhantes aos novos telemóveis (Ahmad et al. 2013).

Por ser um SO bastante versátil, comparativamente ao iOS que é apenas utilizado no iPhone, iPad e iPod, o Android tem versões desenvolvidas pela própria Google para tv, carros e *wearables*, como relógios. No entanto, dadas as características *open-source* do Android, este é utilizado por outras empresas criando variações do Android original que são utilizadas em consolas, camaras digitais entre as mais diversas aplicações, com ou sem *ecran* tátil.

Dada a sua elevada versatilidade, o Android é tido como o SO mais utilizado a nível mundial para dispositivos móveis. Tendo por base índices de *marketshare*, no segundo trimestre de 2015 o Android lidera a tabela de preferências dos utilizadores com 82.8%, visto que este consegue abranger um maior número de equipamentos e marcas. Com percentagens de utilização mais baixa encontra-se o iOS com 13.9%, já que este é apenas utilizado em equipamentos da Apple. Com números bem menos expressivos estão todos os outros SOs tais como o Windows Phone, BlackBerry OS, entre outros (IDC 2015).

Tal como os restantes SOs dedicados a equipamentos móveis, o Android possui várias características de segurança, que segundo (Al-Qershi et al. 2014), podem ser agrupadas em cinco pontos distintos:

- Permissões de aplicações

  A instalação e utilização de aplicações pressupõe a aprovação ou não de permissões para que estas possam aceder a recursos/dados existentes no equipamento;

- Proteção de componentes

  O funcionamento do Android é baseado na interação de quatro componentes (*Activity, Service, Content Provider e Broadcast Receiver*). Estas componentes estão protegidos de acessos por parte de aplicações maliciosas. Este método é descrito por (Enck et al. 2009) como sendo uma encapsulação que tanto pode ser considerada pública, como privada;

- Assinatura de aplicações

  As aplicações disponibilizadas na Play Store têm de ser assinadas digitalmente, de forma a validar o autor e a garantir que o código da aplicação não foi de forma alguma corrompido, após ser assinada;

- *Memory Management Unit*

  É um processo de *hardware* que previne que processos de determinada aplicação aceda a memórias de outras aplicações;

- *Type Safety*

  É uma característica de programação em que o Android previne ataques direcionados a *buffers* e à memória. Este método é alcançado através da utilização de linguagens de programação mais seguras, tal como Java, e a utilização de *binders*, neste caso o *OpenBinder*, que assegura a comunicação entre diferentes linguagens, garantindo o funcionamento do mecanismo.

Alguns aspetos de segurança que o Android possui, são herdados a partir do Linux tal como o *Portable Operating System Interface* que cria o processo de *sandboxing*, e o *file access*. Neste caso o processo de *sandboxing* não é mais do que um mecanismo de segurança implementado pelo Android, para que as aplicações instaladas sejam executadas num ambiente restrito, onde todos os recursos necessários ao funcionamento da aplicação sejam controlados. Assim, as aplicações são executadas sem

colocar em causa a integridade do SO, deixando ao utilizador a tomada de decisão sobre quais os recursos do equipamento a que esta deve ter acesso. A utilização do processo de *file access* permite controlar utilizadores e processos de aceder a ficheiros restritos, prevenindo acessos ilegais. A utilização de ambos os processos permite manter a integridade do sistema operativo, separando os processos principais do sistema dos processos que permitem o funcionamento das aplicações.

4. Permissões

Por defeito, uma aplicação móvel requer o acesso a recursos existentes no sistema, para que esta possa funcionar. A quantidade e o tipo de recursos necessários dependem do tipo de aplicação, bem como das funcionalidades que a mesma possua. Os recursos básicos para que a aplicação funcione não são mais do que o processador, a memória RAM, bem como espaço de armazenamento. Para que determinadas funções existentes na aplicação possam funcionar, é necessário aceder a outro tipo de recursos que não estão acessíveis por defeito e não são considerados, tais como acesso ao *Bluetooth* ou mesmo à camara, tem que existir uma autorização do utilizador para que a aplicação possa aceder aos recursos necessários.

No fundo, o mecanismo de permissões não é mais do que um sistema de segurança, que tem como missão evitar o acesso a recursos que não são necessários ao funcionamento da aplicação. Contudo, existem várias situações onde se verifica que a aplicação requer mais permissões do que as necessárias para que as funções possam funcionar, existem também situações onde a única forma de instalar a aplicação é aceitar as permissões exigidas. Tal como analisado por (Kaur & Upadhyay 2014), muitas vezes esta prática é fruto da falta de conhecimento ou desleixe do programador, e neste caso, sem intenções maliciosas. No entanto, existem situações onde as permissões podem ser colocadas com o propósito de ter acesso aos recursos do equipamento, sem que haja consciência do utilizador para esta prática. Esta última, é feita com intenções maliciosas.

Com a falta de algum tipo de regulamentação ou normas sobre a forma de criar um sistema de permissões eficaz, cada empresa adota a solução que melhor se adapta ás suas necessidades. Contudo, a exigência dos utilizadores tem vindo a aumentar por novos e melhores mecanismos de segurança e de permissões, garantindo a sua privacidade e a proteção dos seus dados.

Fruto desta exigência, as empresas proprietárias dos SOs, tem vindo a alterar estes mecanismos, alterando o papel que o utilizador tem nesta matéria. Nesta nova realidade o utilizador tem mais poder de decisão, face aos modelos anteriores, estando à sua responsabilidade a autorização ou revogação das permissões das aplicações. No entanto, esta nova metodologia está longe de ser perfeita, carecendo ainda de mais desenvolvimento e transparência, sendo este ponto analisado posteriormente nesta tese.

4.1. Permissões e aplicações em Android

O modo de funcionamento do Android obriga a que todas as aplicações instaladas no sistema sejam assinadas digitalmente. No entanto, este não obriga a que os programadores se registem na Play Store e tenham certificados emitidos pela Google. Ou seja, os programadores podem criar tantos certificados quanto desejarem e publicar as aplicações, sem que a Google consiga monitorizar este tipo de atividade. Contudo, para que os programadores possam disponibilizar as aplicações através da Play Store, são obrigados a pagar uma determinada quantia para que as aplicações possam ser certificadas por pessoal certificado pela Google, que atestam a validade das aplicações no que toca às características de segurança e funcionamento da aplicação (Mohamed & Patel 2015).

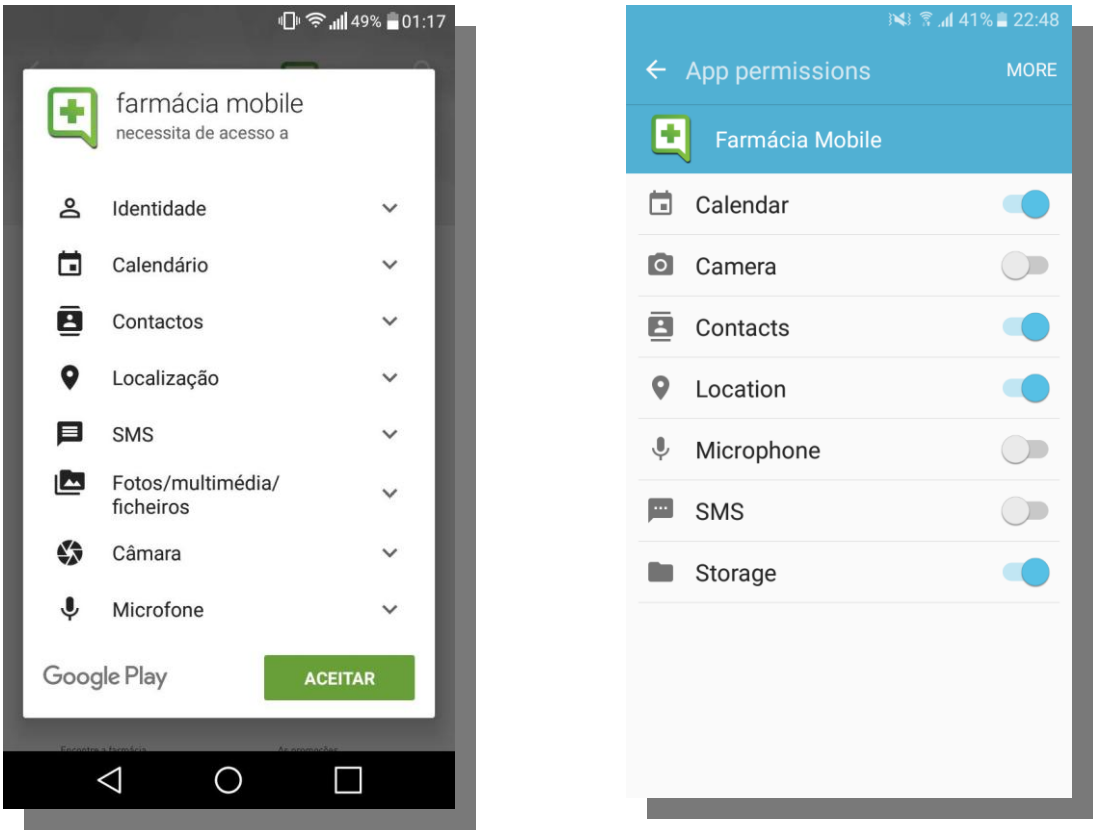
Um dos maiores problemas do Android, relativamente ás aplicações, reside no facto de que estas podem ser instaladas a partir de uma fonte externa à Play Store. Esta prática pode, em certos casos, comprometer a segurança tanto do equipamento, como do utilizador e dos seus dados. Apesar de existirem lojas de aplicações externas à Google que são de confiança tal como a Amazon App Store, é possível fazer o *download* de aplicações que possam em alguma altura ter sido pirateadas, acabando por recolher informações do equipamento, do utilizador, realizar comunicações de valor-acrescentado, entre outros. Isto acontece porque se torna aliciante adquirir aplicações de forma gratuita, que de outra forma teria custos na sua compra.

No que se refere ao modelo de permissões de aplicações utilizado, este tem sofrido inúmeras alterações desde o lançamento do Android. Durante a instalação de uma aplicação na Play Store, é apresentada uma lista de permissões para aceder a recursos que esta necessita para que as funcionalidades possam ser utilizadas. Contudo, as descrições das permissões são muitas vezes incompreensíveis pelo utilizador. Ao contrário da política utilizada pela Apple, a política de permissões utilizada até à quinta versão do Android baseia-se num modelo de *"take-it-or-leave-it"*. Ou seja, o utilizador em condições normais, onde o SO não foi de alguma forma modificado, só poderá instalar aplicações caso autorize todas as permissões exigidas pela aplicação. Em caso de não concordar o *download* e a instalação da aplicação cessará nesse preciso momento.

Contudo, durante a versão 4.3, e por um curto período e tempo, o utilizador teve a possibilidade de fazer a gestão das permissões, de uma forma semelhante ao iOS da Apple, através de uma opção nas definições que se demonstrava difícil de encontrar. Esta opção esteve disponível até à versão 4.4, sendo posteriormente removida na versão

4.4.2, tendo a Google emitido um comunicado a afirmar que essa opção seria apenas um erro, não estando prevista nessa versão do Android.

Com a introdução do Android 6.0, a política de permissões foi revista, tendo-se aproximado do modelo utilizado no iOS da Apple. Neste novo modelo o utilizador pode autorizar ou revogar permissões das aplicações a partir do momento em que a aplicação se encontre instalada. Contudo, a arquitetura das aplicações mais antigas nem sempre permite que esta funcione quando uma permissão seja revogada (Mohamed & Patel 2015; Shabtai et al. 2010; Kelley et al. 2012).



a) b)

Figura 1 - Lista de permissões de aplicações em Android v. 5.0.2 (a) e v. 6.0.1 (b)

4.2. Tipos de permissões

De acordo com (Kaur & Upadhyay 2014), no Android existem 5 de categorias distintas de permissões, cada uma focando-se em áreas diferenciadas do sistema.

- Permissões para o acesso a recursos externos

  Esta categoria lida com permissões para o acesso a recursos existentes no equipamento, tais como o acesso à internet, o envio e receção de SMS, o acesso à memória externa, acesso ao Bluetooth, entre outros. Incluem-se 11 diferentes permissões nesta categoria;

- Permissões para o acesso à informação do utilizador

  Nesta categoria está subjacente o acesso à informação estruturada do utilizador. Existem 14 permissões que permitem o acesso aos alarmes, ao uso de credenciais, à leitura e edição do calendário, à gestão de contas e contactos, entre outras;

- Permissões para acesso aos sensores do equipamento

  Estão incluídas 9 permissões que têm por base o acesso aos sensores existentes no equipamento tais como a gravação de áudio, acesso à camara, acesso à localização, acesso à vibração, entre outros;

- Permissões para o acesso ao estado do sistema e às suas definições

  Nesta categoria estão incluídas 18 permissões, sendo consideradas das mais importantes. Estas permissões dão acesso ao estado do sistema, acesso ao histórico (*read/write*), a alterações às configurações do sistema, acesso ao estado da rede e WIFI (*access/modify*), alterar definições de áudio, entre outras. Com algumas permissões é possível saber se o telemóvel está ou não em modo de chamada;

- Outros tipos de permissões

  Nesta categoria existem permissões mais variadas que não se enquadram nas restantes categorias. São permissões tão distintas como saber a dimensão de pacotes recebidos, alterar a *time-zone*, limpar a *cache*, determinar limite de processos, terminar processos a correr em *background*, entre outras.

4.3. Riscos associados

No panorama das permissões, independentemente do cuidado que se tenha, existe sempre o risco de se expor informação a terceiros, seja por aplicações maliciosas, seja por mau desenho da aplicação em si. O facto de as permissões, na generalidade dos casos, não serem apresentadas de uma forma clara, precisa e transparente, deixam uma sensação de dúvida e confusão ao utilizador, levando a más tomadas de decisão. Neste contexto, este pode ser arrastado para situações constrangedoras e delicadas, podendo ser prejudicado de formas bastante graves.

De acordo com (Sheppard 2013), nem sempre as aplicações e os programadores fazem um uso abusivo das permissões incluídas nas aplicações. No entanto, são vários os casos onde as permissões são utilizadas de forma abusiva, dadas as falhas que muitas das permissões apresentam, tanto na sua implementação, como na sua apresentação ao utilizador.

Existem várias formas de utilização abusiva das permissões, sendo que na grande maioria dos casos, estes ataques estão para lá da perceção do utilizador. Alguns ataques podem com a "simples" violação de um simples telemóvel, fazer a recolha de dados tais como os contactos, os *emails*, a informação existente noutras aplicações, entre outros, e dependendo da natureza do ataque, criar perfis de pessoas individuais, ou fazer a agregação de informação. Em casos mais extremos, é possível traçar o perfil exato do utilizador do telemóvel com base nos critérios pretendidos e na informação recolhida. Este tipo de prática ocorre sem o consentimento e o conhecimento do utilizador, colocando em risco não só este, mas também todas as pessoas que sejam identificadas através da informação recolhida. Estes casos podem ganhar proporções mais graves, caso a informação recolhida infira na condição física ou de saúde do utilizador, sendo estes considerados dados sensíveis e em condições normais, alvo de processamento com níveis de segurança mais elevado.

A utilização excessiva de permissões não justificada, pode criar falhas na proteção da privacidade do utilizador. Este tipo de prática acontece na maioria das vezes com o propósito de rentabilização do investimento. Ou seja, uma aplicação que tenha uma permissão para aceder à localização, embora esta não tenha função associada que verifique esta exigência, pode ser utilizada com o propósito de enviar publicidade direcionada ao utilizador com base na sua localização geográfica e noutros dados já existentes no seu perfil. Em várias aplicações, a utilização de permissões excessivas não garante a segurança, nem em alguns casos informam se os dados obtidos, são alvo de

processamento e de algum tipo de armazenamento fora do equipamento. Existem casos de aplicações que além de enviarem para servidores dados pessoais e/ou sensíveis, enviam também dados relacionados com o equipamento em utilização, tais como o MAC *address*, o ID do equipamento, entre outras informações que só deveriam ser enviadas em casos muito específicos e com os devidos protocolos de (Sheppard 2013; van der Meulen & Vollebregt 2015; Chan 2011).

Para se ter uma melhor perceção sobre quais os tipos de riscos associados a cada uma das categorias de permissões mencionadas em 4.2, a tabela seguinte agrega alguns dos mais importantes, de acordo com (Olmstead & Atkinson 2015).

Tabela 1 - Permissões vs. Riscos

Categoria	Permissões	Riscos
Permissões para o acesso a recursos externos	• Internet access • Text messages (send/receive) • External storage access (read/write) • Bluetooth • NFC • Use_Sip • Calls access • Receive MMSs	• APPS maliciosas conseguem instalar apps de terceiros • Monitorização e envio de informação, incluindo dados de segurança • Realização de comunicações de valor acrescentado • Envio de dados para servidores externos
Permissões para o acesso à informação do utilizador	• Set alarms • Use credentials • Calendar (read/write) • Text messages (read/write) • Authenticate accounts • Accounts (manage/get) • Contacts (read/write) • Subscribed feeds (read/write) • Read logs	• Recolha da lista de contactos • Envio do log de SMSs para servidores
Permissões para acesso aos sensores do equipamento	• Record audio • Access camera • Access location (fine/coarse) • Access location extra commands • Vibrate • Access flashlight • GPS receiver	• Análise da localização do equipamento • Acesso à camara sem o conhecimento do utilizador • Gravação de áudio sem o conhecimento do utilizador
Permissões para o acesso ao estado do sistema e às suas definições	• Access system state • Access history bookmarks (read/write) • Write settings • Phone state (read/modify) • Wake lock • Battery status • Accessing Bluetooth admin • Network state (access/change) • Modify audio settings • Get tasks • WIFI state (access/modify) • Synchronization settings (read/write) • Read synchronization states and change configuration	• Identificação física do equipamento através do IMEI, IMSI ou número de telefone • Introdução da informação do equipamento em *blacklists*
Outros tipos de permissões	• Receive boot completed • Get package size • Expand status bar • Set time zone • Clear application cache • Set process limit • Set animation scale • Reorder tasks • Kill background process	

4.4. Aplicações em Portugal

Com a crescente preocupação nas políticas de privacidade e proteção de dados nas aplicações móveis, tornou-se essencial fazer uma avaliação das aplicações existentes no mercado português. Dada a dimensão deste mercado, é virtualmente impossível fazer uma análise integral da Play Store, existindo, assim, a necessidade de ter em conta critérios de seleção.

A análise focou-se em apenas duas categorias, "saúde e bem-estar" e "médicas". Contudo, dentro de cada uma das categorias existem aplicações a nível mundial, sendo por isso necessário selecionar apenas as que tem definido um programador português, ou que em última instância estejam associadas a marcas portuguesas.

Este estudo incidiu sobre as permissões utilizadas nestas aplicações, onde a cada uma das permissões foi atribuído um código, tendo sido criada uma lista (Anexo I) de acordo com a organização das permissões apresentada aquando do *download* e instalação das aplicações.

Na tabela seguinte são apresentadas as aplicações com o maior número de *downloads* na Play Store e algumas das aplicações que tem um elevado número de permissões.

Tabela 2 - Aplicações Android

Nome	Último update	Versão	Permissões	Downloads
A Minha Barriga	10/15	1.2	2.1, 3.1, 5.1, 5.2, 7.1, 7.2, 8.1, 8.2, 11.3, 11.4, 11.8	100 000 – 500 000
O Meu Bebé	11/15	1.3	2.1, 3.2, 5.1, 5.2, 7.1, 7.2, 8.1, 8.2, 11.3, 11.4, 11.8, 11.13	50 000 – 100 000
Farmácias Portuguesas	05/16	3.0.7	2.1, 3.2, 5.1, 5.2, 7.1, 7.2, 8.1, 8.2, 9.1, 11.2, 11.3, 11.4, 11.9, 11.6	10 000 – 50 000
MyCUF	02/16	2.0.9	4.1, 4.2, 11.3, 11.6, 11.18	10 000 – 50 000
Médis	03/15	1.0.1376	5.1, 5.2, 6.3, 7.1, 7.2, 8.1, 8.2, 11.3, 11.4	10 000 – 50 000
iFDepressão	03/16	1.0.1	6.2, 7.1, 7.2, 8.1, 8.2, 9.*, 10.1, 11.3, 11.4, 11.10, 12.1, 14.1	1000 – 5000
Farmácia mobile	06/15	1.0	2.1, 4.1, 4.2, 3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 13.1, 7.1, 7.2, 8.1, 8.2, 9.1, 14.1, 11.2, 11.3, 11.4, 11.7, 11.10, 11.11, 11.8, 11.13, 11.15, 11.6, 11.12	1000 – 5000
Alerta Pílula	11/13	1.0.4	2.1, 3.2, 5.1, 5.2, 5.3, 6.2, 10.1, 11.3, 11.4, 11.7, 11.12, 11.11, 11.14, 11.6, 11.10	500 – 1000
iGlycemia	11/14	1.0.0	2.1, 3.1, 3.2, 3.3, 5.1, 5.2, 6.1, 6.2, 6.4, 7.1, 7.2, 8.1, 8.2, 9.1, 14.1, 10.1, 11.3, 11.4, 11.7, 11.10	100 – 500

Da pesquisa das aplicações, em Maio de 2016, de acordo com os critérios de seleção, foram encontradas 57 aplicações. Das 57 aplicações 35 pertencem à categoria de "Saúde e bem-estar", sendo que as restantes 22 pertencem à categoria "médica".

4.5. Validação de apps

Para se perceber de que forma as aplicações selecionadas na Tabela 2 funcionam, foi necessário proceder a uma análise ao fluxo de dados aquando da sua utilização.

4.5.1. Implementação

A validação das aplicações implicou que fosse implementado um ataque do tipo "*man in the middle*", através do **mitmproxy**, utilizando um certificado que as aplicações reconhecessem. Por sua vez o telemóvel, ligar-se-ia à internet através de um *proxy* criado para o efeito. Ou seja, o telemóvel ao invés de fazer a ligação através da *wifi* existente, a ligação seria feita através do computador, que neste caso desempenharia a função de AP (*Access Point*). Desta forma, é possível analisar todo o trafego realizado com a utilização normal da aplicação, através do **mitmproxy**.

Figura 2 - Ataque por Man in the Middle

4.5.2. Resultados

A partir dos ataques realizados foi possível inferir de que modo cada uma das aplicações seguem o cumprimento das permissões solicitadas.

Uma das primeiras linhas de defesa quanto a ataques prende-se com a validação do certificado utilizado para o estabelecimento das ligações de dados, o que nenhuma das aplicações em análise efetuou, deixando a validação ao critério do telemóvel. Com esta falha detetada é então possível fazer uma análise detalhada de todo o trafego de dados entre a aplicação e o servidor. Esta análise é apenas interrompida caso exista algum tipo de cifra que impossibilite a leitura dos dados existentes no trafego.

De entre as nove aplicações, três mostravam indícios de alguma preocupação quanto à privacidade e à segurança dos dados.

A aplicação "A Minha Barriga" apesar de processar parte dos dados em HTTPS, a localização de GPS é processada em HTTP POST, o que de alguma forma compromete a privacidade do utilizador.

A aplicação "Médis" tem, no fundo os mesmos problemas da aplicação anterior, onde a localização do utilizador é processada através de um HTTP GET.

Por sua vez a aplicação "MY CUF", apesar de as ligações serem feitas em HTTPS, todos os objetos estão em formato JSON. Neste caso, conseguindo ultrapassar a cifra da ligação, é possível analisar todo o conteúdo de uma forma relativamente simples. Neste caso é possível ter acesso a informação altamente sensível tal como identificação do utilizador e o historial clinico, bem como acesso às marcações de consultas e historial de pagamentos de serviços.

Nas aplicações "Farmácias Portuguesas" e "Farmácia Mobile" as ligações são feitas através de HTTPS, recorrendo à API do Google para processamento da localização.

Nas aplicações "O Meu Bebé" e "iGlycemia" o conteúdo é estático, não realizando qualquer tipo de ligação.

Por último as aplicações "IFDepressão" e "Alerta Pilula" não foram possíveis de ser acedidas.

A Tabela 3, sumariza o teste realizado a cada uma das aplicações e para cada caso identificando quais os resultados obtidos.

Tabela 3 - Resumo dos resultados da validação das apps

Aplicações	Valida o Certificado	Algo suspeito	Observações
A Minha Barriga	Não	Sim	Envio da localização através de HTTP POST
O Meu Bebé	Não	Não	Conteúdo estático
Farmácias Portuguesas	Não	Não	Todas as ligações feitas através de HTTPS
MyCUF	Não	Sim	Todas as ligações feitas através de HTTPS, mas os objetos estão em formato JSON
Médis	Não	Sim	Envio da localização através de HTTP GET
iFDepressão	Não	Não	Não abre
Farmácia mobile	Não	Não	Todas as ligações feitas através de HTTPS
Alerta Pílula	Não	Não	Necessita de código para funcionar
iGlycemia	Não	Não	Conteúdo estático

5. Estudos análogos na EU

Fruto das tendências dos últimos anos, o desporto e a saúde tem estado no topo das prioridades dos utilizadores. Juntamente com a pressão constante de melhorar a cada dia, ou a necessidade de comparar os resultados obtidos com o dia anterior ou mesmo com um grupo de pessoas, existe um grande fluxo de dados pessoais a circular na internet que acaba por fugir ao controlo do utilizador. Este fluxo de dados torna-se apetecível para empresas que conseguem gerar lucros através do processamento destes dados.

Como o número de *smartphones* e aplicações aumentou vertiginosamente nos últimos anos, foram várias as vozes que se levantaram na defesa do consumidor/utilizador, expondo práticas condenáveis por parte das empresas que recolhiam e/ou tratavam esses dados. Desta forma, nos últimos dois anos surgiram estudos a nível europeu, que levantaram questões sobre que tipo de dados circulam na internet, obtidos através de aplicações móveis e se de facto os dados são protegidos através de mecanismos eficazes, estando de acordo com a lei de cada país, independentemente de os dados serem considerados sensíveis ou não.

5.1. Caso Italiano

Um dos primeiros casos a surgir em domínio público aconteceu em 2014 por parte da DPA italiana que anunciou que iria investigar aplicações móveis da área da saúde.

Como este tipo de aplicações estava em crescimento e as mesmas tinham na sua posse perfis com bastante sensibilidade, podendo em casos mais graves afetar a privacidade do utilizador.

Esta investigação foi realizada no âmbito da iniciativa europeia promovida pela GPEN (*Global Privacy Enforcement Network*), uma entidade que promove a cooperação de várias DPAs a nível mundial, focou-se nas aplicações relacionadas com a área da saúde, pelo facto de já anteriormente terem existido casos de algumas queixas sobre o abuso dos dados pessoais a nível europeu.

No fundo a investigação focou-se na forma como as aplicações iam de encontro às leis de privacidade e proteção e dados, e também de que forma estas seguiam as *guidelines* emitidas pela entidade reguladora para o processamento dos dados de saúde. Nesta investigação incluíram não só as aplicações que eram italianas, mas incluíram aplicações que sendo originárias de outros países, eram disponibilizadas e operavam em Itália.

Os resultados da investigação revelaram detalhes de alguma preocupação, relativamente às políticas de proteção de dados, bem como às informações fornecidas ao utilizador.

Na maioria das aplicações analisadas das diferentes plataformas (Android, iOS, Windows, etc.) eram requeridas várias permissões tais como a localização, o ID do equipamento e o acesso a outras contas, câmara e contactos. Ainda em cerca de metade das aplicações investigadas, não fornecem informação antes da instalação, ou então fornecem informação muito generalizada e dúbia. Em determinados casos foi observado que as políticas de privacidade, embora sem valor legal, o texto não se encontrava adequado ao tamanho do ecrã, impossibilitando a sua análise, ou então estas políticas não se encontravam disponíveis de forma alguma. Noutro conjunto de aplicações observou-se que existia um elevado de pedido de permissões para as quais não havia uma função específica associada.

Ainda durante a investigação, a reguladora extrapolou os resultados alegando que os mesmos problemas poderão ser encontrados em aplicações de outras áreas, tais como jogos, serviços bancários, entre outros (Personali 2014; Rapp 2014).

5.2. Caso Holandês

Em Novembro de 2015 a DPA Holandesa, CBP (*College Bescherming Persoonsgegevens*), publicou um relatório sobre uma investigação á aplicação de fitness da Nike, a Nike+ Running.

A Nike+ Running é uma aplicação que permite ao utilizador fazer o registo da sua atividade física, bem como melhorar a sua condição física através de planos de treino existentes na mesma e comparar os resultados com outros utilizadores. E até este ponto estaria tudo bem, não fosse o facto de em momento algum o utilizador dar o seu expresso consentimento de que aceita que os seus dados sejam processados de alguma forma. Neste ponto a reguladora faz um comunicado que a aplicação não dá informação suficiente ao utilizador sobre que dados são tratados, de que forma e onde são tratados. Um outro ponto em que a reguladora se foca é no facto de a Nike fazer o processamento de dados de saúde sem qualquer tipo de consentimento do utilizador. Outra acusação que a reguladora faz sobre a aplicação recai na falta de uma base legal para o processamento de dados, apesar de a Nike informar em traços gerais e mínimos que esta informa o utilizador e pede autorização para a recolha dos mesmos.

Em contraposição a Nike afirma que em momento algum a aplicação processa dados de saúde e que dados de saúde não tinha, á data, uma definição clara. Em resposta, a reguladora esclarece que para o cálculo do algoritmo que a Nike usa para atribuir planos de treino ao utilizador, é necessário calcular distâncias, velocidade, tempo e localização. É necessário também a quantidade de calorias gastas, o comprimento de um único passo, o género, a altura e o peso do utilizador. Desta forma a aplicação calcula a os programas de treino e os "*Fuel points*", uma função da aplicação para medir o esforço do utilizador. Uma característica que foi colocada em causa e que tem um papel fulcral na investigação, foi o facto de a aplicação calcular uma média da performance do utilizador ao longo do tempo. Esta característica da aplicação permite inferir sobre a condição física do utilizador e consequentemente sobre a condição de saúde.

Por sua vez, a Nike alega que os dados recolhidos são armazenados de uma forma agregada, ou seja, dados de utilizadores em condições semelhantes são agregados em grupos de semelhantes, não sendo assim possível inferir especificamente sobre um utilizador. Apesar destes argumentos, a reguladora afirma que sendo estes dados considerados de saúde, a Nike não tem base legal para fazer o seu processamento, nem tão pouco o consentimento do utilizador.

Com esta ação, a Nike alterou o modo de funcionamento da aplicação, pedindo o consentimento do utilizador para processar os dados.

Esta mesma ação abriu um precedente em que a reguladora admite que o termo "dados de saúde" tem de ser considerado de uma forma mais geral, e não apenas os dados que estão relacionados com os dados clínicos. A reguladora, admite também que apesar de se ter focado apenas na Nike+ Running, estas medidas podem ser aplicadas a outras aplicações que utilizem dados de saúde, mesmo não sendo de fitness (van der Meulen & Vollebregt 2015; Persoonsgegevens 2015).

6. Conclusões/Discussão

Os últimos anos tem sido palco de grandes e importantes acontecimentos no campo da proteção de dados de cidadãos e na manutenção da privacidade informática. Até ao final do século passado proteção de dados era um tema que raramente era abordado em conversas do quotidiano, porque, no fundo, comparativamente aos dias de hoje, poucas eram as casas que dispunham de computador com acesso á internet, da mesma forma que os poucos telemóveis que existiam, para pouco mais serviam do que enviar e receber chamadas e mensagens.

Com a massificação da tecnologia móvel, e o desenvolvimento das tecnologias de informação e comunicação, novas oportunidades se abriram, dando acesso a um mundo novo.

Há medida que os anos foram avançando, a tecnologia evoluiu desenfreadamente, ultrapassando mentalidades e regras. E é neste ponto que os problemas começam a surgir, inicialmente de uma forma oculta. Com a falta de legislação adequada, as tecnologias de informação e comunicação expandiram-se sem qualquer tipo de controlo, existindo entidades, públicas e privadas, a terem completo proveito dessa situação.

Com as denúncias de Max Schrems sobre as violações aos regulamentos por parte do Facebook, abriu-se uma brecha numa regulamentação que se pensava segura, e um precedente seguido das declarações de Edward Snowden. As declarações de Snowden culminaram no fim do acordo de *Safe Harbor* entre os dois lados do Atlântico, levando a que a população se começasse a interessar mais pela proteção dos seus dados pessoais e pela sua privacidade.

É nesta base que assentou o tema desta tese, fazendo uma análise sobre qual o impacto que o Novo Regulamento Europeu em Proteção de Dados terá sobre as aplicações móveis ligadas á saúde, tendo em consideração o atual *Framework* em vigor.

Como as aplicações móveis surgiram a partir deste *boom* tecnológico, nem sempre existia uma legislação que regulamentasse este mercado. Tendo a adjuvante de que se vive num mercado global, as aplicações podem ser criadas num país com legislação diferente daquele em que é descarregada e utilizada. Esta lacuna fez com que os dados pudessem ser recolhidos, processados e utilizados sem que o utilizador tivesse conhecimento. Em muitos dos casos as aplicações não fornecem qualquer tipo de informação sobre o seu funcionamento, e em que casos pode acontecer recolha e processamento de dados. No entanto, e na sua grande maioria as aplicações

disponibilizam ao utilizador as chamadas "políticas de privacidade", que não são mais do que informações sobre o funcionamento da aplicação, sobre os dados que vai usar e no final contactos de quem desenvolveu ou da entidade que é detentora. Mesmo assim, em muitos destes casos as informações fornecidas são demasiado gerais e vagas, sendo que na grande maioria dos casos, estas políticas fazem apenas valer o superior interesse da entidade que detém a aplicação.

Com o Novo Regulamento, as aplicações que operarem em solo europeu serão obrigadas a seguir regras, que se tornam mais claras e acessíveis ao utilizador do que na anterior Diretiva, tais como o direito ao acesso aos dados pessoais, o direito ao esquecimento e o direito a ser notificado aquando da violação dos dados. Estarão também obrigadas a pedir o consentimento ao utilizador sempre exista a necessidade de recolha de dados, seja pelos sensores do equipamento, seja através de formulários.

Através do estudo realizado verifica-se que a proteção de dados ou manutenção da privacidade do utilizador, é um tema que nem sempre está incluído aquando da construção de uma aplicação. E este problema é agravado quando estão em causa aplicações de entidades de saúde, que têm na sua posse dados de extrema sensibilidade, que deveriam ser tratados com a maior das seguranças. Como comprovado, de forma relativamente simples é possível fazer a leitura de dados sensíveis de vários utilizadores, podendo prejudica-lo de formas variadas e graves.

Também nas aplicações analisadas, o uso excessivo de permissões é um caso preocupante, tendo em conta que existe um número significativo de versões do Android que por defeito dá autorização a todas as permissões da aplicação. No entanto, em situações onde as permissões são pedidas caso a caso, antes da utilização de uma determinada função, não é explicado claramente o porquê de a permissão ser necessária, não dando garantias de que mais dados possam vir a ser recolhidos.

Em última análise, esta tese pretende demonstrar o percurso já percorrido no que toca à matéria de proteção de dados, relacionando o caso de Portugal e as suas origens, com a adaptação à Diretiva Europeia de proteção de dados. Como já referido, o mercado digital é global, portanto, é impensável a Europa fechar-se nela própria. Daí existirem acordos de cooperação entre a Europa e os EUA, de forma não existirem quebras nas comunicações e nas trocas de informação entre ambos. Contudo, a história obrigou a que novas regras fossem criadas e novos acordos definidos, em prol de um mercado mais claro e transparente. É nesta medida que se espera que, no caso das aplicações móveis e dos equipamentos móveis, tais como telemóveis, tablets, etc., as regras criadas possam beneficiar o utilizador, criando um ambiente menos hostil, onde este era tido

como um mero peão, praticamente desprovido de poder de decisão. No fundo, esta tese pretende ser uma continuação do esforço exercido em vários países, como é o caso de Itália e da Holanda, demonstrando que ainda existe um caminho pela frente para um aumento da consciencialização das pessoas e das empresas no que toca a proteger os dados pessoais e a privacidade dos utilizadores deste tipo de serviços.

7. Referências

Ahmad, M.S. et al., 2013. Comparison between android and iOS Operating System in terms of security. *2013 8th International Conference on Information Technology in Asia - Smart Devices Trend: Technologising Future Lifestyle, Proceedings of CITA 2013*, pp.2–5.

Al-Qershi, F. et al., 2014. Android vs. iOS: The security battle. *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, pp.1–8. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6916629.

Alshugran, T. & Dichter, J., 2014. Extracting and modeling the privacy requirements from HIPAA for healthcare applications. *Systems, Applications and Technology Conference (LISAT), 2014 IEEE Long Island*, pp.1–5.

Alshugran, T., Dichter, J. & Faezipour, M., 2015. Formally Expressing HIPAA Privacy Policies for Web Services. , pp.295–299. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7293356.

Assey, J.M. & Eleftheriou, D.A., 2001. Privacy Safe Harbor: Smooth Sailing or Troubled Waters? , 97.

Campos, J.M. de, 2014. *Manual de Direito Europeu* 02–2014th ed., Coimbra Editora.

Cate, F.H., 1995. The EU Data Protection Directive, Information Privacy , and the Public Interest. *Iowa Law Review*, 80, pp.431–443.

Chan, C., 2011. Using online advertising to increase the impact of a library Facebook page. , 32(4/5), pp.361–370. Available at: http://dx.doi.org/10.1108/01435121111132347.

Commission, E., 2012. Proposal for a Regulation of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation. , 0011.

Coudert, F. (CiTiP), 2015. Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for data protection authorities. , (October). Available at: https://lirias.kuleuven.be/bitstream/123456789/511500/1/FannyCoudert_Post+CJEU+Schrems_final.pdf.

Degraw, J.S. et al., 2015. The U.S.-EU Safe Harbor Framework Is Invalid: Now What? , pp.1–5.

ECJ, 2015. Maximillian Schrems v. Data Protection Commissioner. , (117), pp.26–28.

Efining, D., Ata, D.E.D. & Egislation, P.R.L., 2003. An Analysis of the Use of Bilateral Agreements Between Transnational Trading Groups : The US/EU e-Commerce Privacy Safe Harbor. , (May 1999), pp.171–214.

Enck, W., Ongtang, M. & McDaniel, P., 2009. Understanding android security. *IEEE Security and Privacy*, 7(1), pp.50–57.

European Commission, 2015. Agreement on Commission's EU data protection reform will boost Digital Single Market. *European Commission Press Releases Database*, (December). Available at: http://europa.eu/rapid/press-release_IP-15-6321_en.htm.

European Commission, 2016. Transatlantic Data Flows : Restoring Trust through Strong Safeguards. Available at: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf.

Farrell, H., 2003. Constructing the International Foundations of E-Commerce—The EU-U.S. Safe Harbor Arrangement. *International Organization*, 57(02), pp.277–306.

Ferenc, D., 2013. *Understanding Hospital Billing and Coding*, Elsevier Health Sciences.

Fernandes de Almeida, J.M., 1981. História da informática em portugal: o subsistema de informação da cuf / quimigal. *Revista de Informática - Associação Portuguesa de Informática*, 2(3), pp.253–274. Available at: http://repositorium.sdum.uminho.pt/bitstream/1822/859/1/mesa8.pdf.

Furnell, S.M., Bryant, P. & Phippen, a. D., 2007. Assessing the security perceptions of personal Internet users. *Computers and Security*, 26(5), pp.410–417.

Herveg, J.A.M. & Poullet, Y., 2004. Directive 95/46 and the use of GRID technologies in the healthcare sector: selected legal issues. , (4), pp.233 – 240.

IDC, 2015. Smartphone OS Market Share, 2015 Q2. Available at: http://www.idc.com/prodserv/smartphone-os-market-share.jsp [Accessed June 28, 2016].

Kaur, A. & Upadhyay, D., 2014. PeMo: Modifying application's permissions and preventing information stealing on smartphones. *Proceedings of the 5th International Conference on Confluence 2014: The Next Generation Information*

Technology Summit, pp.905–910.

Kelley, P.G. et al., 2012. A conundrum of permissions: Installing applications on an android smartphone. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7398 LNCS, pp.68–79.

Langheinrich, M., 2001. Privacy by design—principles of privacy-aware ubiquitous systems. *Ubicomp 2001: Ubiquitous Computing*. Available at: http://link.springer.com/chapter/10.1007/3-540-45427-6_23.

van der Meulen, S. & Vollebregt, E., 2015. Dutch DPA finds fitness app violates data protection law. *eHealth Law & Policy*, 2(12), pp.03–04. Available at: http://www.e-comlaw.com/data-protection-law-and-policy/article_template.asp?from=dplp&ID=1436&Search=Yes&txtsearch=sensitive health data.

Mohamed, I. & Patel, D., 2015. Android vs iOS Security: A Comparative Study. *2015 12th International Conference on Information Technology - New Generations*, pp.725–730. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7113562.

Olmstead, K. & Atkinson, M., 2015. *Apps Permissions in the Google Play Store*,

Van Overstraeten, T., Cumbley, R. & Pauly, D., 2015. Safe Harbor invalid. What next for transfers of personal data to the US? , (October), pp.1–10.

Personali, G. per la protezione dei dati, 2014. Medical apps: More transparency is needed on data use. , (September). Available at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/3375236.

Persoonsgegevens, C. bescherming, 2015. *Selection from DPA investigation Nike+ Running app*, Available at: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/conclusions_dpa_investigation_nike_running_app.pdf.

Raffaelli, R., 2015. *EUROPEIA*,

Rapp, L., 2014. Filling the Gap: Legal and Regulatory Challenges of Mobile Health (mHealth) in Europe. *European Regional Initiative on ICT Applications, including eHealth*.

Salbu, S., 2000. The European Union data privacy directive. *Berkeley Technology Law Journal*, 15(418), pp.461–484.

Shabtai, A. et al., 2010. Google android: A comprehensive security assessment. *IEEE Security and Privacy*, 8(2), pp.35–44.

Sheppard, M., 2013. *Smartphone Apps, Permissions and Privacy*, Office of the Privacy Commissioner of Canada.

Anexos

Anexo I – Lista de permissões

1.	Device & app history	**1.1.**	Read sensitive log data
		1.2.	Retrieve running apps
2.	Identity	**2.1.**	Find accounts on the device
		2.2.	Add or remove accounts
		2.3.	Read your own contact card
3.	Contacts	**3.1.**	Modify contacts
		3.2.	Find accounts on the device
		3.3.	Read your contacts
4.	Calendar	**4.1.**	Add or modify calendar events and send email to guests without owners knowledge
		4.2.	Read calendar events plus confidential information
5.	Location	**5.1.**	Precise location (GPS and network based)
		5.2.	Approximate location (network based)
		5.3.	Access extra location provider commands
6.	Phone	**6.1.**	Write call log
		6.2.	Read phone status and identity
		6.3.	Directly call phone numbers
		6.4.	Read call log
7.	Photos/media/files	**7.1.**	Read the contents of the USB storage
		7.2.	Modify or delete the contents of the USB storage
		7.3.	Erase USB storage
		7.4.	Test access to protected storage
8.	Storage	**8.1.**	Read the contents of the USB storage
		8.2.	Modify or delete the contents of the USB storage
		8.3.	Test access to protected storage
9.	Camera	**9.1.**	Take pictures and videos
10.	Device ID & call information	**10.1.**	Read phone status and identity
11.	Other	**11.1.**	Bind to a notification listener service
		11.2.	Receive data from Internet
		11.3.	Full network access

		11.4.	View network connections
		11.5.	Read battery statistics
		11.6.	Prevent device from sleeping
		11.7.	Control vibration
		11.8.	Read Google service configuration
		11.9.	Mock location sources for testing
		11.10.	Change audio settings
		11.11.	Send sticky broadcast
		11.12.	Run on startup
		11.13.	Use accounts on the device
		11.14.	Disable your screen lock
		11.15.	Control flashlight
		11.16.	Pair with Bluetooth devices
		11.17.	Access Bluetooth settings
		11.18.	Make app always run
		11.19.	Enable app debugging
		11.20	In-app purchases
		11.21	Set wallpaper
		11.22	Control Near Field Communication
12.	WIFI Connection Information	**12.1.**	View wifi network connections
13.	SMS	**13.1.**	Receive text messages (SMS)
14.	Microphone	**14.1.**	Record Audio

Anexo II – Lista de Aplicações de "saúde e bem-estar"

Nome	Programador	Link	Data do último update	Versão	Permissões	Downloads
Saúde Online	BMAC, Laboratórios de Análises, SA	https://play.google.com/store/apps/details?id=pt.base.saudeonline&hl=pt_PT	25/08/14	1.2.1	2.1, 3.2, 11.2, 11.3, 11.4, 11.6, 11.7	100 – 500
Médis	Médis, Companhia Portuguesa de Seguros de Saúde,SA	https://play.google.com/store/apps/details?id=pt.medis.androidApp&hl=pt_PT	03/03/15	1.0.1376	5.1, 5.2, 6.3, 7.1, 7.2, 8.1, 8.2, 11.3, 11.4	10 000 – 50 000
Farmácias Portuguesas	Farminvest	https://play.google.com/store/apps/details?id=pt.anf.farmaciasportuguesas&hl=pt_PT	04/05/16	3.0.7	2.1, 3.2, 5.1, 5.2, 7.1, 7.2, 8.1, 8.2, 9.1, 11.2, 11.3, 11.4, 11.9, 11.6	10 000 – 50 000

My CUF	JOSÉ DE MELLO SAÚDE II, S.A.	https://play.google.com/store/apps/details?id=pt.saudecuf.myCUF&hl=pt_PT	05/02/16	2.0.9	4.1, 4.2, 7.1, 7.2, 8.1, 8.2, 11.3, 11.4	10 000 – 50 000
+ Registo Clínico	JOSÉ DE MELLO SAÚDE II, S.A.	https://play.google.com/store/apps/details?id=pt.saudecuf.appinovacao.codmedica	20/10/15	1.0	7.1, 7.2, 8.1, 8.2, 11.3, 11.4, 11.6	10 – 50
Pós Alta Cirurgia Ambulatório	JOSÉ DE MELLO SAÚDE II, S.A.	https://play.google.com/store/apps/details?id=pt.saudecuf.appinovacao.ambulatorio	20/10/15	1.0	7.1, 7.2, 8.1, 8.2, 11.3, 11.4, 11.6	100 – 500
TE.M.S - Tempos Médios de Espera	SPMS	https://play.google.com/store/apps/details?id=pt.proside.spms_tems	11/02/16	1.2	5.1, 5.2, 6.3, 11.3, 11.4	1000 – 5000
Cancro da Mama	Liga Portuguesa Contra o Cancro	https://play.google.com/store/apps/details?id=pt.lpcc.cancrodamama	06/10/15	1.0.0	12.1, 11.3, 11.4	100 – 500
A Minha Barriga	Angelini Farmacêutica Lda.	https://play.google.com/store/apps/details?id=pt.angelini.gravidez	05/10/15	1.2	2.1, 3.2, 5.1, 5.2, 7.1, 7.2, 8.1, 8.2,	100 000 – 500 000

					11.3, 11.4, 11.8	
Bebé Mitosyl	Sanofi	https://play.google.com/store/apps/details?id=com.sanofi.mommysbook.portugal	02/12/14	1.0	4.1, 4.2, 6.2, 6.3, 7.1, 7.2, 7.3, 8.1, 8.2, 10.1, 11.3, 11.4, 11.7	100 – 500
slim Simulator	beSlim	https://play.google.com/store/apps/details?id=beslim.slimsimulator	11/11/14	1.3	7.1, 7.2, 8.1, 8.2, 9.1, 11.3, 11.4	1000 – 5000
mCARAT	MEDIDA/CINTESIS	https://play.google.com/store/apps/details?id=com.phonegap.mcarat	03/05/12	1.0	3.1, 3.2, 5.1, 5.2, 5.3, 13.1, 6.2, 6.1, 6.4, 8.1, 8.2, 9.1, 14.1, 10.1, 11.7, 11.3, 11.4, 11.10	1000 – 5000
mCARAT Media	MEDIDA/CINTESIS	https://play.google.com/store/apps/details?id=andre.ribeiro.videoplayer	17/01/13	1.1	7.1, 7.2, 8.1, 8.2, 11.3, 11.4	10 – 50

Health Appointments	MEDIDA/CINTESIS	https://play.google.com/store/apps/details?id=com.medida.preparacaoconsultas	06/06/12	0.8	5.1, 5.2, 11.3, 11.4, 11.7, 11.9	1000 – 5000
Termas do Centro	Direct100	https://play.google.com/store/apps/details?id=mobi.direct100.termascentro	03/08/15	1.0	1.2, 2.1, 3.2, 5.1, 5.2, 7.1, 7.2, 8.1, 8.2, 11.3, 11.4, 11.6, 11.7, 11.12	1 – 5
myHut	stomachion	https://play.google.com/store/apps/details?id=com.pedronveloso.fitnesshut	04/05/16	1.2	11.3, 11.4	10 000 – 50 000
Labco	mediadetails	https://play.google.com/store/apps/details?id=com.mediadetails.labco_app	25/01/16	1.0.2	2.1, 3.1, 3.2, 3.3, 5.1, 5.2, 6.1, 6.2, 6.4, 7.1, 7.2, 8.1, 8.2, 9.*, 10.1, 11.3, 11.4, 11.10, 11.7	10 – 50
Nove Meses - A Minha Gravidez	Goody S.A.	https://play.google.com/store/apps/details?id=pt.bial.aminhagravidez.app	08/04/15	2.1	11.3, 11.4	50 000 – 100 000

eMed.pt - Poupe na Receita	Codepixel	https://play.google.com/store/apps/details?id=com.codepixel.infarmedAndroid	08/06/15	1	4.1, 4.2, 5.1, 5.2, 7.1, 7.2, 8.1, 8.2, 9.1, 12.1, 11.3, 11.4, 11.8, 11.9	10 000 – 50 000
A Mindfulness App	MindApps	https://play.google.com/store/apps/details?id=se.lichtenstein.mind.pt	02/05/16	1.51	5.1, 5.2, 7.1, 7.2, 8.1, 8.2, 11.6, 11.7, 11.3, 11.4, 11.8, 11.12	100 – 500
O Meu Bebé	Angelini Farmacêutica Lda.	https://play.google.com/store/apps/details?id=pt.angelini.bebe	05/11/15	1.3	2.1, 3.2, 5.1, 5.2, 7.1, 7.2, 8.1, 8.2, 11.3, 11.4, 11.8, 11.13	50 000 – 100 000
Champ@me	Fundação Champalimaud	https://play.google.com/store/apps/details?id=pt.fc.generic.prd	16/03/16	1.0.12	5.1, 5.2, 6.3, 7.1, 7.2, 8.1, 8.2, 9.1, 11.2, 11.3, 11.4, 11.8, 11.6	1000 – 5000
SPC Guidelines	IT People - Consultores LDA	https://play.google.com/store/apps/details?id=pt.itpeople.socieda	24/04/13	1.0	7.1, 7.2, 8.1, 8.2, 12.1, 11.3, 11.4,	1000 – 5000

		deportuguesadecardiologia			11.14	
Farmácia mobile	Going Solutions	https://play.google.com/store/apps/details?id=com.goingsolutions.farmaciamobile	12/06/15	1.0	2.1, 4.1, 4.2, 3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 13.1, 7.1, 7.2, 8.1, 8.2, 9.1, 14.1, 11.2, 11.3, 11.4, 11.7, 11.10, 11.11, 11.8, 11.13, 11.15, 11.6, 11.12	1000 – 5000
Pedro Cruz Clinic	Filipe A. Barroso	https://play.google.com/store/apps/details?id=pt.clinicapedrocruz	23/06/15	1.1.4	2.1, 3.2, 6.3, 7.1, 7.2, 8.1, 8.2, 11.2, 11.3, 11.4, 11.6, 11.12, 11.7	100 – 500
MiniSom Teste Audição Gratuito	MiniSom	https://play.google.com/store/apps/details?id=pt.minisom.MiniSom	22/01/14	1.0.2	5.1, 7.1, 7.2, 8.1, 8.2, 11.3, 11.4, 11.8	1000 – 5000

Farmácia Sá da Bandeira	Farmácia Sá da Bandeira	https://play.google.com/store/apps/details?id=pt.Coolsis.FarmaciaFSB	06/06/15	1.1.0	9.1, 11.3, 11.4	100 – 500
DietMed - Vademecum	DietMed - Produtos Dietéticos e Medicinais, Lda.	https://play.google.com/store/apps/details?id=pt.dietmed.catalogo	16/09/15	2.1.1	5.1, 5.2, 6.2, 7.1, 7.2, 8.1, 8.2, 14.1, 10.1, 11.3, 11.10	50 – 100
Farmácia Avenida	Farmácia Avenida	https://play.google.com/store/apps/details?id=pt.Coolsis.FarmaciaAVN	15/06/15	1.0.1	9.1, 11.3, 11.4	50 – 100
Smoking Control	Pedro Rodriges	https://play.google.com/store/apps/details?id=com.devextreme.SmokingControl_DevExtreme	26/08/15	1.1.19.0	11.3, 11.4	100 – 500
Cartão de Vacinas	outcomeWAI Solutions	https://play.google.com/store/apps/details?id=com.outcomewai.cartaodevacinas	09/01/16	1.2.2	1.2, 7.1, 7.2, 8.1, 8.2, 9.1, 11.3, 11.4, 11.12, 11.7	100 – 500
Instituto Médico e Dentário	WHITEROAD SOFTWARE, LDA	https://play.google.com/store/apps/details?id=pt.whiteroad.imdb	17/08/15	1.0.0	7.1, 7.2, 8.1, 8.2, 11.3, 11.4, 11.7, 11.6, 11.7	10 – 50

Pulse	Pedro Chambino	https://play.google.com/store/apps/details?id=pt.chambino.p.pulse	05/10/15	1.1	9.1, 11.*	50 – 100
Farmácia Mais Perto	Leo Farmacêuticos, Lda	https://play.google.com/store/apps/details?id=net.maria_design.farmaciamaisperto2&hl=pt_PT	17/07/15	0.0.2	11.3, 11.4	1 – 5
Nutrição Online	Z89 Develop	https://play.google.com/store/apps/details?id=com.nutricaonline.nutricao	17/03/16	1.1	2.1, 3.2, 5.1, 6.2, 7.1, 7.2, 8.1, 8.2, 10.1, 11.3, 11.6,11.12, 11.13, 11.18, 11.21, 12.1, 14.1	10 – 50
Instituto Implantologia	Mixlife Lda	https://play.google.com/store/apps/details?id=com.applook.clinica397732	03/05/16	1.1	11.3, 11.4, 12.1	5 – 10
BioCare	Awesome software S.A	https://play.google.com/store/apps/details?id=pt.mediaweb.appfelica	23/11/15	2.0	6.2, 7.1, 7.2, 8.1, 8.2, 10.1, 11.3, 11.4, 11.22	ND

Hut Training	Intelinova Software	https://play.google.com/store/apps/details?id=com.proyecto.fitnesshut.tg	01/04/16	1.1.7	2.1, 3.2, 6.2, 7.1, 7.2, 8.1, 8.2, 10.1, 11.2, 11.4, 11.6, 11.19	5000 – 10000
Fitness Club de Braga	Intelinova Software	https://play.google.com/store/apps/details?id=com.proyecto.fitnesclubdebraga.tg	29/04/16	1.0	2.1, 3.2, 6.2, 7.1, 7.2, 8.1, 8.2, 10.1, 11.2, 11.3, 11.4, 11.6, 11.19	ND

Anexo III - Lista de Aplicações “médicas”

Nome	Programador	Link	Data do último update	Versão	Permissões	Downloads
Pediatria	Rui Oliveira	https://play.google.com/store/apps/details?id=com.rhomobile.pediatria	14/11/13	1.0	4.1, 4.2, 11.3, 11.6, 11.18	10 000 – 50 000
Portuguese Dental Association	Ordem dos Médicos Dentistas	https://play.google.com/store/apps/details?id=com.omd.android	17/04/15	1.2.4	11.3, 11.4, 11.7	1000 – 5000
Blood Alive	Sociedade Portuguesa de Anestesiologia	https://play.google.com/store/apps/details?id=com.spa.BloodAlive	13/05/15	1.0	11.7	100 – 500
Alerta Pílula	Merck Sharp & Dohme Corp	https://play.google.com/store/apps/details?id=com.merck.AlertaPilulaPT	27/11/13	1.0.4	2.1, 3.2, 5.1, 5.2, 5.3, 6.2, 10.1, 11.3, 11.4, 11.7, 11.12, 11.11, 11.14, 11.6, 11.10	500 – 1000

MPScribe	Variograma	https://play.google.com/store/apps/details?id=com.variograma.mpscribe	09/06/15	1.16	2.1, 2.3, 3.2, 5.1, 5.2, 7.1, 7.2, 8.1, 8.2, 14.1, 11.3, 11.4, 11.6	10 – 50
Medic Book	AR Note	https://play.google.com/store/apps/details?id=com.ARNote.MedicalBook	30/08/15	7	7.1, 7.2, 8.1, 8.2, 9.1, 11.3, 11.4, 11.6, 11.7	1 – 5
iClinic Dental	yapp.pt	https://play.google.com/store/apps/details?id=com.easyeasyapps.framework.A656	22/03/14	1.1.4	11.3, 11.4	100 – 500
Avaliação e seguimento com HBP	QUODEM	https://play.google.com/store/apps/details?id=com.quodem.gsk.pt.criterioshbppt	14/09/15	1	11.3, 11.4, 12.1	ND
iGlycemia	Series	https://play.google.com/store/apps/details?id=pt.series.iglycemia	08/11/14	1.0.0	2.1, 3.1, 3.2, 3.3, 5.1, 5.2, 6.1, 6.2, 6.4, 7.1, 7.2, 8.1, 8.2, 9.1, 14.1, 10.1, 11.3, 11.4, 11.7,	100 – 500

					11.10	
dador.pt	Vodafone Portugal, Comunicações Pessoais, S.A.	https://play.google.com/store/apps/details?id=pt.vodafone.dador	12/11/13	1.0.1	1.2, 2.1, 3.2, 5.1, 5.2, 7.1, 7.2, 8.1, 8.2, 11.3, 11.4, 11.8, 11.6, 11.19	1000 – 5000
febre-i-dor	Memória Visual	https://play.google.com/store/apps/details?id=pt.benefarmaceutica.febreidor	16/02/16	1.2.5	2.1, 3.2, 7.1, 7.2, 8.1, 8.2, 11.3, 11.4, 11.6, 11.7, 11.12, 11.2, 11.13	1000 – 5000
Alerta Anel	Merck Sharp & Dohme Corp	https://play.google.com/store/apps/details?id=com.msd.circlet	23/03/16	2.0	2.1, 3.2, 5.1, 5.2, 5.3, 6.2, 10.1, 11.4, 11.7, 11.12, 11.6, 11.10,	1000 – 5000
iMed	ACIN - iCloud Solutions	https://play.google.com/store/apps/details?id=acin.app.mobile.imed	18/11/14	2.4.0	10.1, 7.1, 7.2, 8.1, 8.2, 12.1, 6.2, 11.3, 11.4, 11.16, 11.17	1000 – 5000

Clinica Valmor	Rdesign.pt	https://play.google.com/store/apps/details?id=pt.clinicavalmor.appcv	21/09/15	1.4	4.1, 4.2, 11.3, 11.4, 11.12	1 – 5
Magium Farma	Zeone Informatica, Lda	https://play.google.com/store/apps/details?id=pt.zeone.magium	30/10/15	01.00.00.2015 1030	7.1, 7.2, 8.1, 8.2, 11.3	50 – 100
Glico Me	FloatGroup	https://play.google.com/store/apps/details?id=pt.floathealth.glicome	16/03/16	ND	11.3, 11.7, 11.6, 11.12	50 – 100
Simpósio Nacional SPO 2015	Bitwoci	https://play.google.com/store/apps/details?id=bitwoci.pt.spo	06/11/15	1.0	11.3	5 – 10
Jornal Médico	Oficina do Site	https://play.google.com/store/apps/details?id=com.jmm.ods.jmedico	05/05/14	1.0.9	7.1, 7.2, 8.1, 8.2, 12.1, 11.3, 11.4	500 – 1000
TNVROM	appylab	https://play.google.com/store/apps/details?id=com.appylab.tnvrom	21/11/13	1.0	5.1, 7.1, 7.2, 8.1, 8.2, 11.3	100 – 500

Pregnancy Calculator	Mgfamiliar.net	https://play.google.com/store/apps/details?id=air.pt.mgfamiliar.apps.pregnancycalculator	03/11/12	1.0.0	11.3	100 – 500
LOV Dosagem	Sanofi	https://play.google.com/store/apps/details?id=com.sanofi.lovdosagem	18/11/13	1.0	11	100 – 500
Dicionário Médico	Estado da Arte	https://play.google.com/store/apps/details?id=com.xn__dicionriomdico_0gb6k.android	21/08/15	0.0.1	12.1, 11.3, 11.4	100 – 500
iFDepressão	Innovagency	https://play.google.com/store/apps/details?id=eutimia.selfguidedtool	08/03/16	1.0.1	6.2, 7.1, 7.2, 8.1, 8.2, 9.*, 10.1, 11.3, 11.4, 11.10, 12.1, 14.1	1000 – 5000
Medicare	Passos-Firmes, Lda	https://play.google.com/store/apps/details?id=com.medicare.cartao	08/04/16	1.0.0	7.1, 7.2, 8.1, 8.2, 11.2, 11.3, 11.4, 11.6, 11.7	10 – 50