Saúde Móvel: desafios globais à proteção de dados pessoais sob a perspectiva do direito da União Europeia

Mobile health: global challenges to the protection of personal data from the perspective of European Union law

Salud móvil: desafíos mundiales en la protección de datos personales desde la perspectiva del Derecho de la Unión Europea

Alexandra Rodrigues Araujo | alexandra.rodrigues.araujo@gmail.com
Universidade do Minho, Centro de Estudos em Direito da União Europeia. Braga, Portugal.
Centro Universitário Cesumar (UniCesumar), Programa de Pós-Graduação em Ciências Jurídicas. Maringá, Brasil.

Tiago Franklin Rodrigues Lucena | tiagofranklin@gmail.com
Centro Universitário Cesumar (UniCesumar). Instituto Cesumar de Ciência, Tecnologia e Inovação (ICETI). Maringá, Brasil.

Flávio Bortolozzi | flavio.bortolozzi.53@gmail.com
Centro Universitário Cesumar (UniCesumar). Instituto Cesumar de Ciência, Tecnologia e Inovação (ICETI). Maringá, Brasil.

Silene Maria Gonçalves | silene.mariag@yahoo.com.br
Centro Universitário Cesumar (UniCesumar). Maringá, Brasil.

Resumo

A saúde móvel ou *mHealth* – as práticas médicas e de saúde pública apoiadas por dispositivos móveis (telefones celulares, smartphones e tablets) – tem claro potencial para aumentar significativamente a qualidade e a eficiência dos cuidados de saúde. Contudo, constatam-se várias fragilidades na proteção dos dados pessoais utilizados nesse contexto. Este artigo tem como objetivo analisar os aspectos jurídicos mais importantes para que uma proteção efetiva dos dados pessoais na mHealth seja alcançada. Tendo este objetivo e, partindo das regras da União Europeia e das melhores práticas internacionais sobre a matéria, apresentamos uma série de pressupostos condensados em três eixos: maior responsabilidade de todos os atores envolvidos no tratamento de dados mHealth; maior transparência na forma como os dados são tratados, compartilhados e reutilizados; e maior controle dos usuários das tecnologias e da utilização de seus dados. O artigo procura contribuir com um panorama global a fim de levantar as reflexões para a criação e a validação de políticas locais.

Palavras-chave: direitos fundamentais; dados pessoais; dados relativos à saúde; saúde móvel; Direito da União Europeia.

Abstract

The mobile health or mHealth – medical and public health practices supported by mobile devices (cell phones, smartphones and tablets) – has the potential to significantly increase the quality and efficiency of health care services. However, the field has several weaknesses in terms of user personal data in this context. This article aims to analyze the most important legal aspects for an effective protection of personal data in mHealth. Having this objective and, based on the EU rules and best international practices in this field, we presented a series of assumptions that are condensed into three areas: greater responsibility of all actors involved in the treatment of mHealth data; greater transparency in how the data are processed, shared and reused; and greater control of users of the technologies and how their data is used. The paper seeks to contribute to an overview of the challenges in order to raise the discussions for the creation and validation of local policies.

Keywords: fundamental rights; personal data; Health data; mobile health; European Union Law.

Resumen

La salud móvil – prácticas médicas y de salud pública compatibles con los dispositivos móviles (teléfonos celulares, teléfonos inteligentes y tablets) – tiene el potencial de aumentar significativamente la calidad y eficiencia de los servicios de atención de la salud. Sin embargo, el campo tiene varios puntos débiles en términos de datos personales del usuario en este contexto. Este artículo tiene como objetivo analizar los aspectos legales más importantes para una efectiva protección de los datos personales en la salud móvil. Teniendo este objetivo y, en base a las normas de la UE y las mejores prácticas internacionales en este campo, hemos presentado una serie de supuestos que se condensan en tres áreas: una mayor responsabilidad de todos los actores involucrados en el tratamiento de los datos de salud móvil; una mayor transparencia en cómo se procesan los datos, compartir y reutilizar; y se utiliza un mayor control de los usuarios de las tecnologías y cómo sus datos. El trabajo busca contribuir a una visión general de los retos a fin de elevar las discusiones para la creación y validación de las políticas nacionales.

Palabras clave: derechos fundamentales; datos personales; datos relativos a la salud; salud móvil; Derecho de la Unión Europea.

INFORMAÇÕES DO ARTIGO

Contribuição dos autores: A autora Alexandra Araujo elaborou pesquisa documental e jurídica sobre o tema tendo como bases as Diretrizes Europeias. Os autores Tiago Lucena e Flávio Bertolozzi estabeleceram relação com o campo da mHealth, contribuíram com introdução e panorama do tema no Brasil com a revisão local das tecnologias, normativas e diretrizes. A autora Silene Gonçalves desenvolveu parte do tema em sua dissertação de mestrado e redigiu o manuscrito empreendeendo também as revisões críticas do conteúdo intelectual.

Declaração de conflito de interesses: O artigo não apresenta conflitos de interesses

Agradecimento/Contribuições adicionais: A CAPES pelo financiamento do projeto: "A transferência de dados pessoais para países terceiros ou organizações internacionais à luz do direito da União Europeia e do direito brasileiro" da pesquisadora Alexandra Araujo no âmbito do Programa de Pós-Graduação em Ciências Jurídicas da UNICESUMAR (Maringá/Paraná/Brasil) e pela bolsa de pesquisa da autora Silene Gonçalves e ao ICETI pelo apoio aos professores pesquisadores da UniCesumar.

Histórico do artigo: Submetido: 13.jun.2016 | Aceito: 15.set.2016 | Publicado: 23.dez.2016.

Introdução

A incorporação das tecnologias de informação e comunicação (TIC) no campo da saúde vem merecendo desde a década de 1970 o nome de *e-health* (Saúde Eletrônica). Nos anos 2000, a popularização de dispositivos móveis (telefones celulares, smartphones, tablets) fez surgir um novo termo que destaca o uso dessas tecnologias móveis no contexto da saúde: *mHealth* ou Saúde Móvel.

Números da *International Telecommunication Union* atestam que, até maio de 2015, tínhamos cerca de 7 bilhões de telefones celulares no mundo[1]. Alguns desses aparelhos possuem alta capacidade de processamento, de qualidade de imagem e de possibilidade de acesso a multirredes, configurando-se como um computador pessoal e móvel chamado usualmente de *smartphone*. O aumento da venda desse tipo de aparelho condicionou o surgimento de uma nova indústria de *softwares*: as aplicações móveis, mais conhecidas como *apps*. *Apps* são programas aplicativos que executam as mais diversas atividades e são disponibilizados para *download* nos principais sistemas operacionais: Android, IOS e Windows Phone. Dentre as possibilidades, destacam-se os aplicativos dedicados à área da saúde, fazendo surgir o termo saúde móvel (*mHealth*) que se refere, quer às "Práticas médicas e de saúde pública apoiadas por dispositivos móveis, como smartphones, tablets, dispositivos de monitorização de doentes, assistentes pessoais digitais (PDA) e outros dispositivos sem fios"[2], quer às aplicações para o modo de vida e bem-estar, que podem ser ligadas a dispositivos médicos ou sensores (por exemplo, pulseiras ou relógios), bem como sistemas de orientação pessoal, sistemas de informações sobre saúde, sistemas de mensagens que lembram a hora de tomar medicamentos e serviços de telemedicina[3].

A utilização crescente de dispositivos móveis na área da saúde e a possibilidade destes aparelhos recolherem uma grande quantidade de dados pessoais dos usuários – tais como *Electronic Health Records* (EHR), Registro Eletrônico de Saúde, que é um repositório eletrônico de informações em torno da saúde das pessoas e que possibilita um panorama de seus históricos clínicos – têm gerado debates no que se refere à ética, à segurança e a políticas de privacidade e proteção dos dados[4], mobilizando diferentes setores da sociedade: juristas, reguladores de empresas de comunicação, profissionais da saúde e desenvolvedores de tecnologias. A proliferação de *apps* dedicados à área da saúde levanta também a discussão sobre a fiabilidade das informações, a efetividade nas ações de promoção da saúde e o uso indevido dos dados pessoais dos usuários, principalmente por empresas privadas. Por isso, o tema tem merecido reflexões sociais e políticas sobre este novo contexto de endereçar programas de saúde para usuários utilizando esses dados fornecidos por dispositivos móveis[5]. Outras pesquisas focam no desenvolvimento e aprimoramento de técnicas, ferramentas e instrumentos para a segurança dos dados pessoais[6].

É um fato que a *mHealth* está em franco crescimento e que tem um claro potencial para aumentar significativamente a qualidade e a eficiência dos cuidados de saúde[7]. Contudo, pesquisas sobre as políticas de regulação são necessárias, conforme lacuna constatada por vários pesquisadores, tais como Martínes Pérez *et al.*[8], que ressaltam que as leis sobre privacidade e segurança de dados aplicadas à saúde móvel foram aprovadas há muitos anos (por exemplo, 1995 para a Diretiva 95/46/CE da União Europeia[9] e 1996 para a *Health Insurance Portability and Accountability Act* nos EUA). Essas normas ainda estão focadas na saúde eletrônica (*eHealth*), e a sua compreensão foi estendida hoje para a *mHeatlh*, o que as torna muito gerais e, em alguns casos, desatualizadas quanto às necessidades de regulação atuais. Os autores ainda chamam a atenção para a necessidade de mais discussão sobre o tema diante de uma área que está em constante evolução e com novas ferramentas sendo incorporadas[8].

Na verdade, a diversidade de atores que intervêm na *mHealth*, a possibilidade de acesso a grandes volumes de dados armazenados nos *smartphones* ou gerados por estes, a frequente falta de conhecimentos jurídicos dos vários intervenientes no processo, a falta de transparência no tratamento dos dados pessoais relativos à saúde, a falta de conhecimento por parte dos usuários de como os seus dados são utilizados, os

mecanismos de consentimento deficientes, as medidas de segurança insuficientes, a tendência para a maximização dos dados e a amplitude com que as finalidades são interpretadas no tratamento de dados pessoais são algumas das questões que geram frequentes desafios à proteção de dados. Consequentemente, ainda há uma desconfiança em grande parte de usuários na hora de instalar aplicações *mHealth* por preocupações com as práticas de privacidade a que estariam sujeitos os seus dados pessoais de saúde[10].

Para que a *mHealth* desenvolva todo o seu potencial econômico e social, essas fragilidades devem ser consideradas e superadas de maneira que o direito à proteção de dados dos (potenciais) usuários fique garantido. Importa não obviar que muitos dos dados pessoais recolhidos neste contexto são dados relativos à saúde. Dados que são particularmente sensíveis e que requerem uma proteção jurídica elevada.

No Brasil, o direito à proteção de dados aparece como uma extensão do direito à privacidade protegido no artigo 5, inciso X da Constituição Federal Brasileira de 1988[10] e no artigo 21 do Código Civil de 2002[11] (lei 10.406/2002). Este direito ainda não tem uma lei geral, mas é protegido por meio de diferentes normas legislativas do 'Código de Defesa do Consumidor' e do 'Marco Civil da Internet'[12]. Após anos de discussão, uma lei geral de proteção de dados pessoais nos parece urgente. Com o objetivo de contribuir para uma reflexão sobre os desafios de um marco jurídico brasileiro que proteja adequadamente os dados relativos à saúde, este artigo analisa os aspetos jurídicos mais relevantes para que a proteção efetiva dos dados pessoais no contexto específico da *mHealth* seja uma realidade. Como as aplicações *mHealth* são atualmente as grandes protagonistas da saúde móvel, serão alvo do presente estudo.

Esta análise terá como ponto de partida as regras da União Europeia (UE) sobre proteção de dados pessoais – reconhecidas como sendo atualmente as mais elaboradas sobre a matéria – mas, também, considerará os padrões e as melhores práticas internacionais. Levando em conta o objetivo proposto, este estudo começa com uma descrição do quadro jurídico da UE aplicável aos dados pessoais no contexto *mHealth*. O segundo aspecto a ser considerado é a identificação dos tipos de dados tratados na *mHealth*. Em seguida, ganham destaque as regras específicas da proteção dos dados relativos à saúde. Nesta parte, a análise do consentimento do titular dos dados adquire o maior protagonismo. Na quarta e última parte deste artigo, analisa-se como os princípios gerais da proteção de dados são aplicados no contexto específico da *mHealth*. O artigo finaliza com umas breves conclusões.

Quadro jurídico geral aplicável aos dados pessoais no contexto da saúde móvel: aspectos fundamentais

Existe uma certa homogeneidade no teor essencial das regras sobre dados pessoais presentes nos instrumentos internacionais que visam a sua proteção. Na verdade, grande parte destes documentos influenciaram-se mutuamente quanto ao seu conteúdo. Por exemplo, se pensarmos no instrumento de direito derivado que estabelece o regime geral sobre a proteção de dados da UE – que atualmente ainda é a Diretiva 95/46/CE – constatamos que se baseia na Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Convenção 108) adotada em 1981 pelo Conselho da Europa que, por sua vez, se inspira nas linhas diretrizes da Organização para a Cooperação e Desenvolvimento Económico desenvolvidas nas *Guidelines governing the protection of privacy and transborder flows of personal data* (1980, revisão de 2013), no artigo 8 da Convenção Europeia dos Direitos do Homem (1950) e nos vários instrumentos de proteção dos direitos humanos adotados sob a *aegis* das Nações Unidas.

Esta homogeneidade no essencial explica-se porque as regras sobre dados pessoais têm como objetivo último assegurar a proteção dos direitos e liberdades fundamentais e, na prática, dos direitos fundamentais ao respeito pela vida privada e à proteção de dados pessoais da pessoa natural. Em muitos destes instrumentos internacionais, o direito à proteção de dados pessoais é reconhecido como uma extensão do direito à privacidade. Pelo contrário, no direito da UE, este direito ganhou um estatuto autônomo.

A Carta dos Direitos Fundamentais da UE, além de garantir no seu artigo 7 o respeito pela vida privada e familiar, reconhece no artigo 8 o direito fundamental à proteção de dados pessoais. Este artigo especifica que os dados pessoais devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Além disso, o artigo 8 n. 2 consagra o direito de todas as pessoas a aceder aos dados coligidos que lhes digam respeito e, se necessário, de obter a sua respetiva retificação. O número 3 do mesmo artigo estabelece que o cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade nacional independente.

Na jurisprudência do Tribunal de Justiça da União Europeia (TJUE), a diferença entre privacidade e proteção de dados ainda não está totalmente clarificada. Contudo, concordamos com Hustinx[13] quando sublinha que:

Privacy and data protection – more precisely: the right to respect for private life and the right to the protection of personal data – have important connections. […] However, there are also crucial differences. The concept of 'data protection' was developed in order to provide structural legal protection to individuals against the inappropriate use of information technology for processing information relating to them, regardless of whether that processing would be within the scope of the right to respect for private life or not.

As normas de direito derivado da UE, que detalham as regras relativas à proteção de dados pessoais, encontram-se maioritariamente na Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995[9]*, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à* 'livre circulação desses dados' (diretiva proteção de dados). Os objetivos principais dessa diretiva são dois: assegurar a livre circulação de dados pessoais entre os Estados-Membros; e proteger as liberdades e direitos fundamentais das pessoas singulares, nomeadamente o direito fundamental à proteção de dados. Aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como aos tratamentos por meios não automatizados contidos num ficheiro ou a ele destinados. O âmbito material desta Diretiva é limitado às questões do mercado único, e a sua aplicação territorial vai além dos 28 Estados-Membros da UE incluindo, também, os Estados que formam parte do Espaço Económico Europeu (EEE): Islândia, Liechtenstein e Noruega.

Atualmente, no contexto da *mHealth,* importa conjugar a Diretiva 95/46/CE[9] com as disposições da Diretiva Privacidade Eletrônica relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas que se aplica a qualquer aplicação instalada/usada por usuários na UE.

Importa ter em atenção que a Diretiva 95/46/CE[9] é aplicável até 25 de maio de 2018. A partir dessa data é substituída pelo Regulamento (UE) 2016/*679* do *Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a* Diretiva 95/46/CE[11] (Regulamento Geral sobre a Proteção de Dados). Quer dizer, a partir de maio de 2018, o Regulamento Geral sobre a Proteção de Dados será diretamente aplicável em todos os Estados-Membros da UE.

No Regulamento Geral sobre a Proteção de Dados[11] são introduzidos novos princípios e normas aplicáveis à saúde móvel. Destacam-se as seguintes novidades: Artigo 4 al. 13) relativa aos dados genéticos; Artigo 4 (al) alínea 15) que contém uma definição de 'dados relativos à saúde'; Artigo 22 que regula as 'Decisões individuais automatizadas, incluindo definição de perfis'; Artigo 35 'Avaliação de impacto sobre a proteção de dados'; e, Artigo 9 relativa ao 'Tratamento de categorias especiais de dados pessoais'.

Identificação do tipo de dados tratados no contexto da saúde móvel

Através de sensores e aplicações móveis, a saúde móvel permite a aquisição de um importante número de dados. Em princípio, os dados tratados na *mHealth* são dados pessoais porque contêm informações relativas a uma pessoa singular (natural) identificada ou identificável. Além disso, é frequente que os dados tratados neste contexto sejam dados pessoais relativos à saúde. Nas próximas páginas vamos desenvolver os conceitos de dados pessoais e relativos à saúde.

Neste artigo utilizamos o conceito de dados pessoais presente no artigo 2 a) da Diretiva 95/46/CE[9] e que identifica 'dados pessoais' com 'qualquer informação relativa a uma pessoa singular identificada ou identificável'. A expressão "qualquer informação" abrange informações objetivas (tais como o nome da pessoa, um número de identificação ou um elemento específico da sua identidade física) e também opiniões e avaliações subjetivas (tais como a avaliação realizada por uma instituição bancária sobre fiabilidade de um requerente de empréstimo). Este conceito inclui, assim, dados que fornecem qualquer tipo de informação de uma pessoa singular (natural), quer seja verdadeira ou falsa, e que pode estar disponível em qualquer formato: uma fotografia, um número de telefone, dados bancários, dados genéticos, dados biométricos etc.

A informação deve ser relativa a uma pessoa singular (natural) 'identificada' ou 'identificável'. Uma pessoa singular é 'identificável' quando, apesar da pessoa ainda não ter sido identificada, é possível fazê-lo por meio de pesquisas adicionais. A identificação é normalmente obtida através de informações especiais muitas vezes designadas por identificadores que podem ser, nomeadamente, dados de localização, identificadores por via electrónica ou um ou mais elementos específicos da identidade física, fisiológica, psíquica, económica, cultural ou social da pessoa.

Com os termos 'diretamente' ou 'indiretamente' identificável faz-se referência ao fenômeno das combinações únicas: quando uma pessoa pode ser identificada por meio de informações combináveis (independentemente destas informações estarem ou não disponíveis para o responsável pelo tratamento). É o que acontece quando se utilizam pseudônimos. Nestes casos, substitui-se um atributo de um registo por outro através, por exemplo, da cifragem com chave secreta, da função *hash*, da utilização de dispositivos de autentificação etc. Contudo, nestes casos a identidade da pessoa não se perde e pode ser identificada novamente, de acordo com o Grupo de Trabalho (GT) do Artigo 29 do Parecer 05/2014 sobre técnicas de anonimização – WP 216 de abril de 2014. p. 42[12]

Importa sublinhar que muitos dos tipos de dados armazenados num dispositivo inteligente, ou por este gerados, são considerados dados pessoais. Por exemplo: a localização geográfica, os contactos, a identidade do titular dos dados, os registos de chamadas telefônicas, SMS ou mensagens instantâneas, a agenda, a identidade do telefone, os identificadores únicos dos dispositivos e dos clientes, os dados sobre cartões de crédito e pagamento, o histórico de navegação, o correio eletrónico, as imagens e vídeos etc, segundo Parecer 2/2013 do GT do Artigo 29.º, sobre as aplicações em dispositivos inteligentes – WP 202 de fevereiro de 2013. p. 31. Desses dados armazenados pode extrair-se uma grande quantidade de informação sobre o titular dos dados. Por exemplo, sobre a sua vida intelectual (p.e. através do acesso a sítios de Internet específicos), relações (p.e. através da lista de contactos combinada com as listas de chamadas e mensagens) ou hábitos (p.e. através da sua localização geográfica combinada com a sua agenda)[14].

Em muitos casos, os dados tratados no contexto da saúde móvel estão relacionados ou revelam o estado de saúde física ou psíquica dos indivíduos. Estes dados, pela sua natureza, são considerados 'dados sensíveis' por serem mais suscetíveis de representar um risco para o seu titular. São dados que revelam aspectos geralmente considerados íntimos. Consequentemente, estão sujeitos a regras de proteção jurídica reforçada providenciando uma segurança mais elevada ao titular desses dados.

Atualmente, a nível do direito derivado da UE, não há uma definição de 'dados relativos à saúde' de uma pessoa. No caso *Bodil Lindqvist*, o TJUE no Acórdão de 6.11.2003 – Processo C-101/01 – fez uma

interpretação ampla desta expressão ao incluir nela as "informações relativas a todos os aspectos, quer físicos quer psíquicos, da saúde de uma pessoa"[13]. O Regulamento Geral sobre a Proteção de Dados[11] – que visa substituir a atual Diretiva 95/46/CE[9] – vai ao encontro desta interpretação do TJUE ao detalhar no artigo 4 al. 15) a definição de dados relativos à saúde do seguinte modo: "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde"[11]. No considerando 35 do mesmo Regulamento são pormenorizados, numa lista considerada não taxativa, os dados que se devem incluir como dados pessoais relativos à saúde:

Deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular dos dados que revelem informaçãoes sobre a sua saúde física e mental no passado, no presente ou no futuro. O que precede inclui informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação, conforme referido na Diretiva 2011/24/EU do Parlamento Europeu e do Conselho, a essa pessoa singular; qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico ou estado fisiológico ou biomédico do titular dos dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico in vitro.[11]

No entanto, apesar de todos estes elementos, discernir no caso concreto quais dados são relativos à saúde ainda requer uma cuidadosa avaliação. Neste julgamento, a noção do que constitui um dado relativo à saúde deve ser interpretada de forma ampla[15].

Em relação aos dados recolhidos pelas *apps* para o modo de vida e bem-estar – que têm como objetivo principal manter ou incentivar comportamentos saudáveis, o bem-estar e a qualidade de vida dos usuários – entende-se que são dados relativos à saúde quando são tratados num contexto médico ou quando a informação sobre a saúde de um indivíduo pode ser razoavelmente inferida por esses dados. Fazer esta distinção requer, mais uma vez, uma cuidadosa avaliação feita pelo responsável pelo tratamento à situação.

As regras específicas de proteção dos dados pessoais relativos à saúde: o consentimento

Os dados relativos à saúde estão sujeitos, não só às regras gerais em matéria de proteção de dados pessoais mas, também, às regras que concedem uma proteção com garantias específicas aos dados sensíveis objeto de tratamento.

Neste sentido, há uma proibição geral de tratamento de dados pessoais relativos à saúde consagrada no n.º 1 do artigo 8 da Diretiva 95/46/CE[9]. Não obstante, devido à importância que o conhecimento deste tipo de informação pode adquirir, esta proibição está sujeita a várias derrogações. A diretiva de proteção de dados estabelece derrogações obrigatórias nos n. 2 e 3 do artigo 8 e uma isenção facultativa no n. 4 do mesmo artigo. São elas: a) consentimento explícito; b) para atender interesses vitais da pessoa em causa; c) quando está em causa o tratamento de dados (médicos) por profissionais da saúde; d) isenções devidas a um interesse público importante. Estas derrogações são taxativas e devem ser interpretadas de forma restrita. No caso da saúde móvel, o consentimento explícito do usuário é, atualmente, o principal fundamento legal para o tratamento de dados relativos à saúde. Por isso mesmo, nas próximas linhas vamos ver com mais detalhes os requisitos deste consentimento.

Em conformidade com o artigo 8 n.º 2 al. a) da Diretiva 95/46/CE[9], a proibição de tratamento de dados sensíveis "não se aplica quando a pessoa em causa tiver dado o seu consentimento explícito para esse tratamento"[9]. Segundo a definição de 'consentimento' presente na alínea h) do artigo 2 da mesma diretiva,

o consentimento válido deve ser uma "manifestação de vontade, livre, específica e informada"[9]. O consentimento entende-se para "livre", quando é uma decisão voluntária, tomada por uma pessoa na posse de todas as suas faculdades e sem coerção. O consentimento para "específico" diz respeito a uma situação delimitada e concreta. Significa que o consentimento tem de estar relacionado com o tratamento de um determinado item de dados ou de uma categoria limitada de dados. Há consentimento para "informado" quando a pessoa em causa faz uma apreciação e compreensão dos factos e implicações do seu consentimento. Por isso mesmo, de acordo com o GT do Artigo 29.º no "Documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde electrónicos (SER)" de WP 131 de fevereiro de 2007 e p.23[14] o usuário deve dispor de informações exatas e detalhadas de forma compreensível e clara.

Além disso, o consentimento para o tratamento de dados sensíveis deve ser 'explícito'. Entende-se que esta palavra pretende sublinhar que deve ser um consentimento ativo mediante uma declaração ou um ato positivo inequívoco. Entende-se que deve ser dado por escrito. Pressupõe, também, que o consentimento deve ser dado para finalidades determinadas, explícitas e legítimas e só é válido no tratamento de dados para esses fins[16].

Quando falamos de consentimento no contexto da saúde móvel, importa conjugar este artigo 8 da Diretiva Proteção de Dados com o artigo 5, n. 3 da Diretiva Privacidade Eletrônica[9]. Este preceito estabelece uma norma específica ao estipular que quem pretenda armazenar informações ou aceder a informações armazenadas em dispositivos inteligentes de usuários no EEE deve ter o consentimento prévio do usuário. Quer dizer, no caso das aplicações *mHealth* o consentimento deve ser dado com anterioridade à sua instalação e à colocação e recolha de quaisquer dados pessoais.

Importa também chamar a atenção para a distinção entre este consentimento, exigido para colocar ou ler informações armazenadas no dispositivo, e o consentimento necessário para o tratamento dos diferentes tipos de dados pessoais tais como os dados relativos à saúde. Cada um destes consentimentos tem a sua própria base jurídica e, em ambos os casos, tem de ser acorde com a definição constante do artigo 2, al. h) da Diretiva Proteção de Dados[9].

Há várias outras circunstâncias que exigem um consentimento diferenciado e específico do utilizador. É o caso, por exemplo, da publicidade comportamental ou quando os dados pessoais do utilizador vão ser transferidos para um país terceiro (que não forma parte do Espaço Econômico Europeu – EEE) que não esteja coberto por uma decisão de adequação e, como tal, não beneficie da livre transferência de dados.

Na prática, é possível juntar os vários consentimentos desde que o utilizador seja informado claramente do objeto do seu consentimento. Contudo, consideramos que o consentimento diferenciado entre os vários tipos de dados é a melhor prática. O consentimento considera-se diferenciado quando as pessoas podem controlar (especificamente) as funções de tratamento de dados pessoais oferecidas pela aplicação que pretendem ativar. Importa ainda sublinhar que, segundo a Agência dos Direitos fundamentais da União Europeia, apesar de não estar expressamente mencionado no direito derivado, entende-se que os usuários têm de ter a possibilidade de revogar, a todo o tempo, o seu consentimento de forma simples e eficaz (2014).

Princípios gerais da proteção de dados pessoais aplicados à saúde móvel

O tratamento de dados pessoais referentes à saúde deve sempre respeitar os princípios gerais de proteção de dados estabelecidos nos Artigos 6 e 7 da Directiva 95/46/CE. Nomeadamente, os princípios relativos à qualidade dos dados e os princípios relativos à legitimidade do tratamento de dados. Alguns desses princípios adquirem uma importância primordial no contexto da *mHealth*.

Princípio da utilização limitada e princípio da minimização dos dados

O 'princípio da utilização' 'limitada' ou 'princípio da finalidade' estabelece que os dados pessoais devem ser recolhidos para finalidades 'determinadas', 'explícitas' e 'legítimas'. Consequentemente é proibido o tratamento posterior incompatível com as finalidades da aquisição inicial dos dados (para isso exige-se outra base jurídica). Também se entende que as transferências de dados para terceiros constituem uma nova finalidade e, portanto, exigem outra base legal.

Quer dizer, as finalidades do tratamento de dados devem estar claramente definidas e ser compreensíveis para um utilizador médio (sem conhecimentos técnicos ou jurídicos especializados). Este princípio é fundamental para que os usuários possam confiar nas aplicações *mHealth* e demanda aos criadores de aplicativos que definam especificamente e visivelmente as finalidades do tratamento de dados antes das operações de tratamento terem início. Finalidades que devem ser leais e lícitas.

O princípio da utilização limitada está intrinsecamente ligado ao 'princípio da minimização dos dados' ou 'princípio da qualidade dos dados'. Este princípio determina que os dados pessoais recolhidos sejam pertinentes e não excessivos relativamente às finalidades para que são recolhidos. Quer dizer, os criadores de aplicações têm de escrutinar quais os dados que são absolutamente necessários para a funcionalidade pretendida de forma a evitar o tratamento de dados desnecessário. A estrita aplicação deste princípio é particularmente importante quando estão em causa dados sensíveis tais como os relativos à saúde. Generalizar a recolha de dados relativos à saúde é aumentar a possibilidade desses dados serem utilizados na criação de perfis potencialmente discriminatórios. Este princípio requer, igualmente, que os dados pessoais sejam exatos e atualizados.

Princípios de direito de acesso do titular dos dados e da retenção dos dados

O princípio do direito de acesso do titular dos dados consagra que os usuários dos aplicativos devem poder exercer os seus direitos de acesso, retificação e apagamento, e de oposição ao tratamento de dados. Consequentemente, os aplicativos têm de informar os seus usuários, de forma clara e visível, sobre a existência destes mecanismos de acesso e correção. Além disso, deve ser sempre dada aos usuários a possibilidade de revogarem o seu consentimento de forma simples e linear, por meio de mecanismos de fácil acesso. Tem de ser possível desinstalar os aplicativos e, dessa forma, eliminar todos os dados pessoais, inclusivamente os que se encontram armazenados nos servidores do responsável ou responsáveis pelo tratamento.

O princípio da retenção de dados está consagrado na alínea e) do artigo 6 n. 1 da Diretiva Proteção de Dados. Como regra geral, depois de o utilizador ter desinstalado a aplicação, o criador da aplicação perde toda a legitimidade para continuar a tratar os dados pessoais relacionados com aquele utilizador e, por conseguinte, deve eliminar todos os dados. Se o criador da aplicação desejar manter determinados dados deve solicitar o consentimento inequívoco do utilizador durante o processo de desinstalação.

Princípio da privacidade e obrigações ligadas à segurança dos dados pessoais

Segundo o artigo 17 da Diretiva 95/46/CE[9], os responsáveis pelo tratamento de dados e os subcontratantes têm a obrigação de aplicar medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a divulgação não autorizada dos dados. Proteger a confidencialidade dos dados relativos à saúde é um objetivo fundamental que deve determinar quais as medidas de segurança a se adoptar[15].

Cumprir com essas obrigações em matéria de segurança requer, por parte dos responsáveis pelo tratamento, uma avaliação constante dos riscos, não só atuais mas também futuros, que envolvam a proteção de dados. Requer, igualmente, uma avaliação contínua das medidas de atenuação dos riscos implementadas. Estas medidas devem assegurar um nível de segurança adequado aos riscos que o tratamento apresenta

e, também, em relação à natureza dos dados a proteger. Isto leva a que na fase da criação das aplicações se deve classificar os dados que vão ser tratados de acordo com a sua sensibilidade e aplicar os controlos de privacidade de acordo com este critério. Deste modo, dada a natureza sensível dos dados de saúde, as soluções de saúde móvel deverão conter medidas de segurança reforçadas que minimizem os riscos de segurança, tais como a cifragem dos dados dos usuários e mecanismos apropriados de autenticação e outros itens conforme recomendado pela European Network and Information Security Agency (Enisa) [18].

Três princípios que se destacam como importantes complementos a estas medidas de segurança são o 'princípio da minimização' dos dados (já referido) e os 'princípios da privacidade desde a conceção' e da 'privacidade por defeito'.

O princípio da *privacidade desde a conceção* exige que os fabricantes de um dispositivo ou de uma aplicação incorporem a proteção de dados desde o início da sua conceção. O princípio da 'privacidade por defeito' exige que o responsável pelo tratamento aplique mecanismos que garantam, por defeito, que apenas são tratados os dados pessoais necessários para cada finalidade específica do tratamento. Consequentemente, os dados pessoais só podem ser recolhidos ou conservados durante o tempo mínimo necessário para essas finalidades. Além disso, esses mecanismos devem assegurar que, por defeito, os dados pessoais não sejam disponibilizados a um número indeterminado de pessoas singulares.

Requisitos de informação: princípio da transparência

Como já foi referido neste artigo, os responsáveis pelo tratamento de dados devem disponibilizar a sua política de privacidade antes da aplicação ser instalada pelo usuário. Exige-se que essa informação seja de fácil acesso e compreensão e formulada numa linguagem simples.

No contexto das aplicações *mHealth*, segundo o GT do Artigo 29.º Parecer 2/2013[16] sobre as aplicações em dispositivos inteligentes, WP 202 de fev. e p.31, o responsável pelo tratamento tem de informar necessariamente os (potenciais) usuários sobre: a sua identidade e dados de contato; da existência da operação de tratamento de dados; das categorias exatas de dados pessoais que irá recolher e tratar; das finalidades exatas do tratamento; do período de conservação dos dados; se vão ser divulgados a terceiros; o modo como os usuários poderão exercer os seus direitos de acesso, de retificação e de apagamento; e do direito de apresentar queixa.

Também se devem incluir informações sobre se os dados vão ser a transferidos para países terceiros (países fora do EEE). Devido à frequente utilização da computação em nuvem na *mHealth* é bastante comum que o tratamento de dados pessoais ocorra fora do espaço da EEE, muitas vezes, sem conhecimento dos usuários europeus, ficando esses dados frequentemente sob a alçada de responsáveis de tratamento localizados fora de países cobertos por uma decisão de adequação que permita a livre circulação de dados. Nestes casos as transferências devem ter em conta os requisitos estabelecidos nos artigos 25 (Princípios) e 26 (Derrogações) da Directiva Proteção de Dados[9].

Por último, as melhores práticas internacionais incentivam a que o criador de aplicações estabeleça mecanismos que permitam uma distinção clara entre informações obrigatórias e opcionais. Deste modo, o usuário tem a oportunidade de limitar o tratamento dos seus dados relativos à saúde ao recusar o acesso a informações opcionais por meio de alternativas.

Como já dissemos, as informações básicas sobre o tratamento de dados têm de estar disponíveis aos potenciais usuários antes da instalação da aplicação (por intermédio da loja de aplicativos). Em segundo lugar, estas informações relevantes devem estar igualmente acessíveis após a instalação. Além disso, recomendações do California Department of Justice[19] (Departamento de Justiça da California) incluem que os responsáveis pelo tratamento tenham a obrigação de manter os titulares dos dados informados sobre o modo como os dados estão sendo utilizados.

Considerações finais

Por meio de sensores e aplicativos móveis, a saúde móvel permite a aquisição de um importante número de dados. Em princípio, os dados tratados no contexto da *mHealth* são pessoais, porque contêm informações relativas a uma pessoa singular identificada ou identificável. Além disso, é frequente que os dados tratados na *mHealth* estejam relacionados ou revelem o estado de saúde física ou psíquica dos indivíduos. Estes dados relativos à saúde são considerados dados sensíveis pela sua suscetibilidade de pôr em causa as liberdades fundamentais ou o direito à vida privada do seu titular. Consequentemente, esta categoria especial de dados está sujeita a regras de proteção jurídica específicas e que providenciam uma proteção mais elevada ao titular desses dados. No caso da saúde móvel, o consentimento explícito do usuário é o principal fundamento legal para o tratamento de dados pessoais de saúde. No entanto, constata-se que é difícil para os usuários da saúde móvel estarem adequadamente informados do uso que se faz dos seus dados pessoais e, por isso, muitas vezes não estão em posição de dar um consentimento informado nem de ter o controlo desse uso. O problema está na assimetria das informações atualmente existente entre os operadores da indústria *mHealth* e os seus usuários. Por um lado, operadores de mercado têm interesse em explorar todas as possibilidades dos dados recolhidos para novas iniciativas comerciais. Por outro lado, os usuários ainda têm escasso conhecimento das dinâmicas comerciais que utilizam os seus dados pessoais e de quais são os seus direitos enquanto usuários de aplicativos *mHealth*.

Estas fragilidades da *mHealth* impedem que esta desenvolva todo o seu potencial de melhora na gestão e prestação dos cuidados de saúde por meio de soluções inovadoras. Para que a sociedade possa usufruir plenamente dos benefícios da saúde móvel é fundamental que as tecnologias utilizadas ganhem a confiança dos potenciais usuários no que respeita à forma como os seus dados são usados. Entendemos que, para ganhar essa confiança é preciso minimizar surpresas em relação às práticas de privacidade inesperadas. Entendemos que uma efetiva proteção dos dados pessoais no contexto brasileiro passará fundamentalmente por uma série de pressupostos que condensámos em três eixos: responsabilidade (de todos os atores envolvidos na *mHealth*), transparência (por parte dos responsáveis do tratamento) e controle (dos usuários).

'Responsabilidade': É importante que todos os atores envolvidos na indústria da saúde móvel estejam conscientes das suas responsabilidades, que apliquem de uma forma consistente as regras sobre a proteção de dados e que tenham em conta os padrões e as melhores práticas internacionais. Os princípios da utilização limitada, da minimização de dados, da privacidade desde a conceção e da privacidade por defeito são alguns dos princípios fundamentais para a efetiva proteção dos dados pessoais.

'Transparência': É fundamental que os responsáveis pelo tratamento façam um esforço para tornar mais transparente a maneira como lidam, compartilham e reutilizam os dados pessoais, assim como a finalidade para que são recolhidos. Mais transparência por parte dos responsáveis pelo tratamento permite que os usuários adquiram mais informações sobre as finalidades e a maneira como os dados são tratados de modo a que possam dar um consentimento válido ao tratamento dos seus dados pessoais, incluindo os relativos à saúde.

'Controle': Deve haver uma maior preocupação de consciencializar/informar as pessoas dos seus direitos enquanto usuários de aplicações. Em especial, do seu direito de acesso, retificação, apagamento e de oposição ao tratamento de dados. Além disso, deve ser dado aos utilizadores um maior controle de como vão ser tratados os seus dados pessoais. Por exemplo, por meio da possibilidade do consentimento diferenciado onde as pessoas podem controlar especificamente as funções de tratamento de dados pessoais oferecidas pela aplicação que pretendem ativar.

Referências

1. ITU. The World in 2014 - ICT Facts and Figures [Internet]. International Telecommunication Union. 2014. Available from: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf

2. World Health Organization. mHealth: New horizons for health through mobile technologies. Observatory [Internet]. 2011;3(June):112. Available from: http://www.who.int/goe/publications/goe_mhealth_web.pdf

3. Comissão Europeia. Livro verde sobre a saúde móvel [Internet]. Bruxelas; 2014. Available from: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52014DC0219

4. Green H. Strategies for safeguarding security of mobile computing. Healthc Financ Manage [Internet]. 2013 Feb;67(2):88–90, 92, 94. Available from: http://www.ncbi.nlm.nih.gov/pubmed/23413675

5. Lupton D. M-health and health promotion: The digital cyborg and surveillance society. Soc Theory Heal [Internet]. 2012 Aug 27;10(3):229–44. Available from: http://dx.doi.org/10.1057/sth.2012.6

6. Ren J, Wu G, Yao L. A sensitive data aggregation scheme for body sensor networks based on data hiding. Pers Ubiquitous Comput [Internet]. 2013 Oct 29;17(7):1317–29. Available from: http://link.springer.com/10.1007/s10916-014-0143-9

7. Comissão Europeia. Plano de Ação para a saúde em linha, 2012-2020 - Cuidados de saúde inovadores para o século XXI [Internet]. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao comité económico e social europeu e ao comité das regiões. Bruxelas; 2012. Available from: http://ec.europa.eu/health/ehealth/docs/com_2012_736_pt.pdf

8. Martínez-Pérez B, de la Torre-Díez I, López-Coronado M. Privacy and Security in Mobile Health Apps: A Review and Recommendations. J Med Syst. 2014;39(1).

9. Parlamento Europeu - Conselho da União Europeia. Directiva 95/46/CE do Parlamento Europeu e do Conselho: relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados [Internet]. Luxembourg: Jornal Oficial das Comunidades Europeias; 1995. p. 281/31-281/39. Available from: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_pt.pdf

10. Boehm E. Mobile Healthcare's Slow Adoption Curve. Forrester Research inc. 2011.

11. Parlamento Europeu e do Conselho. Regulamento (UE) 2016/679: relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) [Internet]. Luxembourg: Jornal Oficial das Comunidades Europeias; 2016. p. 119-1-87. Available from: http://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:32016R0679

12. Grupo de Trabalho de Proteção de Dados do Artigo 29o da União Europeia. Parecer 05/2014 sobre técnicas de anonimização [Internet]. Bruxelas: (Direitos Fundamentais e Cidadania da União) da Comissão Europeia; 2014. p. 42. Available from: http://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf

13. Grass R, Skouris V. Acórdão do Tribunal de Justiça - Processo C-101/01 [Internet]. Luxembourg: Curia Europa; 2003. p. 39. Available from: http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d2dc30dd28296b2724ac4b0895cf91c3f2a490df.e34KaxiLc3qMb40Rch0SaxuSaxb0?docid=48382&pageIndex=0&doclang=PT&dir=&occ=first&part=1&cid=161864

14. Grupo de Trabalho de Proteção de Dados do Artigo 29o da União Europeia. Documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde electrónicos (RSE). Bruxelas: (Direitos Fundamentais e Cidadania da União) da Comissão Europeia; 2007. p. 23.

15. Agência dos Direitos Fundamentais da União Europeia, Conselho da Europa. Manual da Legislação Europeia sobre Proteção de Dados. 2014.

16. Grupo de Trabalho de Proteção de Dados do Artigo 29o da União Europeia. Parecer 2/2013 sobre as aplicações em dispositivos inteligentes [Internet]. Bruxelas: (Direitos Fundamentais e Cidadania da União) da Comissão Europeia; 2013. p. 31. Available from: http://www.gpdp.gov.mo/uploadfile/2014/0505/20140505062209480.pdf