The doctor just poked you: os novos desafios da Ehealth

Autor(es): Raposo, Vera Lúcia

Publicado por: Faculdade de Direito da Universidade de Coimbra

URL persistente: URI:<http://hdl.handle.net/10316.2/39859>

DOI: DOI:https://doi.org/10.14195/0870-4260_57-3_11

Accessed : 26-Apr-2023 04:14:58

A navegação consulta e descarregamento dos títulos inseridos nas Bibliotecas Digitais UC Digitalis, UC Pombalina e UC Impactum, pressupõem a aceitação plena e sem reservas dos Termos e Condições de Uso destas Bibliotecas Digitais, disponíveis em <https://digitalis.uc.pt/pt-pt/termos>.

Conforme exposto nos referidos Termos e Condições de Uso, o descarregamento de títulos de acesso restrito requer uma licença válida de autorização devendo o utilizador aceder ao(s) documento(s) a partir de um endereço de IP da instituição detentora da supramencionada licença.

Ao utilizador é apenas permitido o descarregamento para uso pessoal, pelo que o emprego do(s) título(s) descarregado(s) para outro fim, designadamente comercial, carece de autorização do respetivo autor ou editor da obra.

Na medida em que todas as obras da UC Digitalis se encontram protegidas pelo Código do Direito de Autor e Direitos Conexos e demais legislação aplicável, toda a cópia, parcial ou total, deste documento, nos casos em que é legalmente admitida, deverá conter ou fazer-se acompanhar por este aviso.

UNIVERSIDADE DE COIMBRA
FACULDADE DE DIREITO

BOLETIM DE CIÊNCIAS ECONÓMICAS

HOMENAGEM AO PROF. DOUTOR ANTÓNIO JOSÉ AVELÃS NUNES

VOLUME LVII Tomo III

2 0 1 4

Organizadores:

LUÍS PEDRO CUNHA
JOSÉ MANUEL QUELHAS
TERESA ALMEIDA

COIMBRA

THE DOCTOR JUST POKED YOU (OS NOVOS DESAFIOS DA E-HEALTH)

A *e-health* expressa, basicamente, a prestação de cuidados de saúde, e de outros serviços relacionados com a saúde, à distância, recorrendo à digitalização de imagens e a versões electrónicas de instrumentos médicos de uso corrente, transmitidos para outro ponto do país, e mesmo do planeta, mediante vários meios de comunicação, nomeadamente o telefone, o correio electrónico, *web sites*, videoconferência, aplicações de *smartphones*, entre outros ¹.

Para além de ser uma diferente forma de praticar medicina, a *e-health* apresenta-se igualmente como um negócio em expansão. Estima-se que o seu valor a nível mundial ascenda a 69 biliões de euros, representando a Europa 1/3 desse valor, isto é, cerca de 20 biliões ².

¹ Neste contexto há quem individualize, dentro da *e-health*, a cybermedicina, como uma sua modalidade particular, caracterizada pelo uso do *e-mail* ou de salas de chat e desprovido de qualquer réstia de contacto pessoal entre os participantes, logo, susceptível de maior cuidado (Shira D. WEINER, “Mouse-To-Mouse Resuscitation...”, p. 114 ss.). Outras vezes a *e-health* aparece referida como telemedicina, sendo esta até a designação usual entre nós, se bem que mais usada para referenciar a transmissão de exames de diagnóstico ou a realização de consultas à distância, aliás, as primeiras formas de *e-health* existentes.

Sendo certo que estas diferenciações se revelam pertinentes, no presente estudo referir-nos-emos à *e-health* como conceito genérico, incluindo qualquer uma das referidas realidade.

² EUROPEAN COMMISSION, *Commission Staff Working Document...*, p. 4.

As mais-valias da *e-health* não deixam de impressionar³. Por exemplo, permite vigiar os sinais vitais de pacientes crónicos desde a sua própria casa, o que, para além de possibilitar a redução dos custos hospitalares, aumenta certamente a qualidade de vida do paciente. Além do mais, o envio de exames mediante as novas tecnologias de comunicação acelera os processos de tratamento, por vezes salvando vidas. A isto acresce que as consultas médicas realizadas à distância permitem que pacientes em locais remotos possam ter acesso a cuidados de saúde de especialistas; além de que diminui o tempo e o gasto da deslocação do médico, aliás, nem sempre possível. Por outro lado, facilita igualmente a formação de profissionais médicos que, por exemplo, poderão ser assistidos à distância por outro médico na realização de intervenções cirúrgicas.

Contudo, embora encerre incontestavelmente muitas virtualidades, a telemedicina deve ser cuidadosamente ponderada e levada a efeito, dado que implica também alguns perigos que cumpre acautelar. Nesta análise abordaremos apenas três das muitas questões que carecem de reflexão: a telemedicina praticada entre diferentes Estados-Membros da União Europeia (UE); a privacidade e a protecção de dados sensíveis do paciente; e o recurso às tecnologias de informação para prestação de serviços de saúde.

1. Prática médica transfronteiriça

1.1. A livre prestação de serviços médicos no espaço europeu

Uma das notas marcantes do mercado único é a livre prestação de serviços (artigo 56.º do Tratado de Funciona-

³ Rashid BASHSHUR, “Telemedicine...”, p. 310.

mento da União Europeia), liberdade na qual se incluem os serviços de saúde ⁴, independentemente da natureza do serviço e do facto de ser ou não retribuído ⁵, pelo que a telemedicina se encontra igualmente abrangida. Esta liberdade assiste àqueles que pretendem receber o serviço (os pacientes), mas também àqueles que o pretendem prestar (os médicos e as instituições de saúde).

Daqui decorre que um Estado-Membro não pode impor impedimentos à prestação de serviços por outros cidadãos ou empresas europeias aos seus nacionais e, por outro lado, pelos seus nacionais a outros cidadãos ou empresas europeias, excepto quando tais limitações se fundem em razões de interesse público, que, no caso dos serviços de saúde, poderão relacionar-se com a saúde pública ⁶.

O regime delineado nos tratados a este respeito foi em 2011 densificado pela Directiva n.º 2011/24/UE ⁷, cujas principais linhas orientadoras são as seguintes: (a) o paciente tem direito a ser informado quanto ao preço e condições do serviço com vista ao respectivo consentimento informado (artigo 4.º/2 da Directiva n.º 2011/24/UE); (b) não existirá qualquer discriminação em razão da nacionalidade na pres-

⁴ Decisão do Tribunal de Justiça da União Europeia (TJUE) de 31 de Janeiro de 1984, nos casos 286/82 e 26/83, *Luisi and Carbone*.

⁵ Decisões do TJUE de 28 Abril de 1998, caso C-158/96 *Kohll*; de 12 de Julho de 2001, caso C-368/98, *Vanbraekel*; de 13 de Maio de 2003, caso C-385/99, *Müller-Fauré and Van Riet*; de 16 de Maio de 2006, caso C-372/04, *Watts*.

⁶ Decisões do TJUE de 2 de Março de 2011, caso C-108/91 *Ker-Optika*; de 4 de Dezembro de 1986, caso 205/84, *Commission v Germany*; de 26 de Fevereiro de 1991, caso C-180/89, *Commission v Italy*; e de 20 de Maio de 1992, caso C-106/91, *Ramrath*.

⁷ Directiva n.º 2011/24/UE do Parlamento Europeu e do Conselho, de 9 de Março de 2011, relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços.

tação do serviço (artigo 4.º/3/4 da Directiva n.º 2011/24/UE); (c) a prestação do serviço de saúde deve pautar-se pela legislação vigente no local onde é prestado, o que, no caso da telemedicina, aponta para a legislação do local de estabelecimento do prestador (artigo 4.º/1 da Directiva n.º 2011/24/UE); (d) o Estado de nacionalidade do paciente deverá reembolsá-lo das quantias despendidas se e na medida em que o acto médico em causa seja igualmente reembolsável nesse seu Estado de nacionalidade ⁸ (artigo 7.º e ss. da Directiva n.º 2011/24/UE), sendo que esta disposição se aplica igualmente à prática médica realizada por meios electrónicos, como o esclarece o ponto 26 da Directiva ⁹.

Este regime carece de ser concatenado com o disposto na Directiva n.º 2000/31/CE ¹⁰, que estabelece o quadro legal europeu em matéria de serviços de informação e comunicação prestados e recebidos por meios electrónicos (*wire*, rádios, meios ópticos e outros mecanismos electromagnéti-

⁸ A decisão de quais os actos médicos reembolsáveis cabe a cada um dos Estados-Membros, com base na sua própria política de saúde.

⁹ O direito ao reembolso dos custos relativos a cuidados de saúde prestados noutro Estado-Membro por parte do regime obrigatório de segurança social dos doentes, enquanto pessoas seguradas, foi reconhecido pelo TJUE em diversos acórdãos como forma de assegurar a concretização da livre circulação dentro do espaço europeu. O Tribunal considerou que as disposições do Tratado sobre a livre prestação de serviços incluem a liberdade de deslocação dos destinatários dos cuidados de saúde, incluindo as pessoas que necessitam de tratamento médico, a outro Estado-Membro, para aí receberem esses cuidados. O mesmo se aplica aos destinatários dos cuidados de saúde que procuram receber esses cuidados noutro Estado-Membro por outras formas, nomeadamente através da prestação de serviços de saúde por via electrónica.

¹⁰ Directiva n.º 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno (Directiva sobre comércio electrónico).

cos), mediante remuneração, com base num pedido prévio do consumidor do serviço ¹¹. Entre os princípios básicos desta Directiva n.º 2000/31/CE contam-se o princípio do país de origem e o princípio da informação. O primeiro estabelece que a lei aplicável a estes serviços será a vigente no país de estabelecimento do prestador. O segundo que este prestador deve fornecer informação constante, directa e clara sobre a sua identidade e contactos e, no caso de profissões reguladas (como os médicos), igualmente sobre o seu título e registo profissional.

1.2. Lei e jurisdição aplicáveis

Ao que ficou dito acresce ainda a possível dificuldade em termos de exercício da prática médica transfronteiriça, em termos de determinação da lei e da jurisdição aplicáveis. Por exemplo, as autoridades competentes do país A poderão não aceitar que um médico do país B, não devidamente registado no país A, aí exerça actos médicos sobre pacientes ¹². Por conseguinte, urge esclarecer com rigor a localização jurídica do acto médico praticado à distância e, consequentemente, qual a legislação aplicável, sobretudo em sede de competência profissional e responsabilidade civil e criminal derivada do acto praticado, assim como a jurisdição competente para dirimir eventuais litígios ¹³.

¹¹ Da análise cumulativa destes requisitos resulta que não se encontram abrangidos por este regime os serviços que recorram a meios electrónicos, mas que se desenrolam na presença física de prestador e consumidor, bem como aqueles que, embora prestados à distância, não recorram a serviços de telecomunicação *on line*.

¹² Anika D. CLIFTON, “Licensure, Reimbursement...”, p. 9.

¹³ Um especial agradecimento ao Doutor Alexandre Libório Dias PEREIRA, meu colega na Faculdade de Direito da Universidade de Coim-

Qualquer destas questões pressupõe a prévia localização do acto médico prestado à distância. Como de seguida veremos, tudo indica que os serviços prestados pela internet se consideram localizados no local onde fisicamente se encontra o prestador, logo, sujeitos às normas jurídicas aí aplicáveis.

1.2.1. Legislação aplicável

No particular contexto da União Europeia surge uma questão específica: será que quando o paciente se encontra num Estado-Membro distinto daquele onde se encontra o prestador de cuidados de saúde se aplica a Directiva relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços?

Esta Directiva revela-se uma importante ferramenta neste ensejo. A Directiva consagra de forma cabal a liberdade de receber serviços médicos num outro Estado-Membro que não o Estado de origem, bem como o direito a ser ressarcido pelos mesmos, desde que aquela prestação médica confira direito a ressarcimento quando prestada no Estado de origem do receptor, mediante disposições que igualmente se aplicam aos serviços prestados por telemedicina. De acordo com o artigo 4.º/1/a da Directiva n.º 2011/24/UE, estes serviços regular-se-ão pelo regime jurídico do Estado no qual são prestados, independentemente da nacionalidade do seu receptor, sendo que no caso específico da telemedicina se consideram prestados no local onde se encontre estabelecido o

bra, pela disponibilização da sua apresentação “Patient Safety in Telemedicine”, no âmbito da Conferência da European Association of Health Law, que teve lugar em Coimbra nos dias 9 a 10 de Outubro de 2013. Veja-se ainda EUROPEAN COMMISSION, *Commission Staff Working Document...*, p. 7 ss.

médico prestador ¹⁴. Tal como já referimos, este regime está em sintonia com o da Directiva n.º 2000/31/CE, sobre e-comércio, que estipula igualmente a aplicação da lei do prestador do serviço.

Contudo, se a prestação de cuidados de saúde se fundar num contrato podem as partes convencionar a lei aplicável ao mesmo. Esta solução resulta do regime do Regulamento n.º 593/2008 ¹⁵, aplicável às relações contratuais, que consagra como regra a aplicação do regime escolhido pelas partes. No silêncio destas, a relação regular-se-á pela lei do Estado onde o prestador tem a sua residência habitual, desde que se trate de relações entre um paciente e um profissional de saúde (artigo 4.º/1/b do Regulamento n.º 593/2008). Se porventura uma das partes for um consumidor (no nosso caso, o paciente) há que distinguir as situações em que o profissional de saúde dirige a sua actividade para o Estado-Membro onde o paciente tem a sua residência habitual, aplicando-se em tal caso a lei desse Estado (artigo 6.º do Regulamento n.º 593/2008); daqueles outros em que o profissional de saúde não dirige a sua actividade especificamente para aquele Estado, sendo que então a lei aplicável será a do Estado no qual este prestador tem a sua residência habitual (artigo 4.º/1/b do Regulamento n.º 593/2008). Ao invés, tratando-se de relações não contratuais, aplicar-se-á a lei do Estado onde o dano ocorreu,

¹⁴ Artigo 3.º/d da Directiva n.º 2011/24/EU — “Estado-Membro de tratamento», o Estado-Membro em cujo território os cuidados de saúde são efectivamente prestados ao doente. No caso da telemedicina, considera-se que os cuidados de saúde são prestados no Estado-Membro em que o prestador dos cuidados de saúde está estabelecido”.

¹⁵ Regulamento (CE) n.º 593/2008 do Parlamento Europeu e do Conselho, de 17 de Junho de 2008, sobre a lei aplicável às obrigações contratuais (Roma I).

ou seja, do local onde o paciente se encontrava quando foi destinatário daquele acto médico praticado à distância (artigo 4.º/1 do Regulamento n.º 593/2008).

1.2.2. Jurisdição competente

Quanto à jurisdição competente, tenha-se em conta o Regulamento n.º 44/2001 ¹⁶, de acordo com o qual as partes podem previamente convencionar qual o tribunal que resolverá eventuais litígios (artigo 23.º do Regulamento n.º 44/2001), embora com algumas limitações fundadas na protecção do consumidor (artigo 17.º do Regulamento n.º 44/2001). Na falta de convenção prévia o litígio será dirimido no tribunal da nacionalidade do réu ou, caso não possua nacionalidade de um Estado-Membro, onde se encontre domiciliado (artigo 2.º do Regulamento n.º 44/2001).

Porém, esta regra geral contém algumas excepções. Assim, tratando-se de responsabilidade civil extracontratual será competente o tribunal do Estado-Membro onde o dano ocorreu que, no caso da telemedicina, será o local onde o paciente se encontrava quando o acto médico foi praticado. Já no caso da responsabilidade civil contratual cumpre distinguir as relações entre pacientes e profissionais de saúde das relações destes últimos entre si. Neste segundo caso será competente o tribunal onde, de acordo com o contrato, o serviço será prestado (artigo 5.º/1/b do Regulamento n.º 44/2001). Diferentemente, quando o paciente seja parte contratual, há uma distinção a fazer: se a actividade do profissional for dirigida ao Estado-Membro onde aquele residia,

¹⁶ Regulamento (CE) n.º 44/2001 do Conselho, de 22 de Dezembro de 2000, relativo à competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial.

pode o paciente escolher se acciona o médico no tribunal do domicílio deste ou no tribunal do seu próprio domicílio (artigos 15.º/1/c e 16.º do Regulamento n.º 44/2001); se a actividade do profissional medico não se dirigir ao Estado-Membro de residência do paciente será competente o tribunal onde, segundo o contrato, a prestação é fornecida (artigo 5.º/1/b do Regulamento n.º 44/2001), o que, no caso da telemedicina, aponta para o Estado onde o paciente se encontrava quando recebeu o acto médico.

Esta distinção suscita a questão de saber quando é que a actividade do profissional de saúde prestada mediante a internet se dirige aos cidadãos de outro Estado-Membro. Segundo o TJUE, assim será quando seja notório que o prestador procura oportunidades de negócio nesse Estado ¹⁷, o que se pode deduzir do facto de comunicar na língua desse outro Estado, referir preços na moeda daquele ou usar números telefónicos com código internacional.

1.3. Acreditação profissional

Sendo a medicina uma profissão altamente regulamentada, aos respectivos profissionais é exigido o registo numa entidade pública encarregue de exercer poderes disciplinares e regulamentares sobre os mesmos, entre nós, a Ordem dos Médicos. As regras que disciplinam os requisitos para o exercício destas profissões e para o respectivo registo profissional caem na exclusiva competência dos Estados-Membros. Nem sequer é preciso recorrer ao reconhecimento das qualificações dos profissionais de saúde — Directiva n.º 2005/36/CE —, na

¹⁷ Decisões do TJUE de 7 de Dezembro de 2010, casos C-144/09, *Hotel Alpenhof GesmbH v. Oliver Heller* e C-585/08, *Peter Pammer v. Reederei Karl Schlüter GmbH & Co KG Hotel Alpenhof GesmbH v. Oliver Heller*.

medida em que na verdade não existe deslocação física, ao passo que a referida Directiva apenas se aplica nessas situações ¹⁸.

2. Privacidade e protecção de dados

2.1. Os riscos da telemedicina em matéria de privacidade

A privacidade do paciente encontra-se especialmente ameaçada quando a sua imagem e as suas palavras são transmitidas à distância e/ou quando se transmitem dados sensíveis acerca de si ¹⁹. À medida que aumenta o leque de sujeitos que pode aceder a tais dados também o paciente perde controlo sobre esse acesso. Neste contexto é crucial que médicos e instituições de saúde implementem protocolos de acesso aos dados e outros mecanismos de segurança destinados a evitar que semelhante informação caia em mãos de pessoas não autorizadas, especialmente por via de ataques cibernéticos.

Mas, e por outro lado, estas cautelas não devem ir tão longe que impeçam os profissionais de saúde envolvidos de aceder à informação constante do processo clínico do paciente — o qual, não sendo um processo clínico electrónico (PCE), deverá ser de alguma forma informatizado ou, pelo mesmo, digitalizado — e de nele registar os actos praticados, como expressamente comina o Código Deontológico da Ordem dos Médicos.

¹⁸ Artigo 5.º/2 da Directiva n.º 2005/36/CE do Parlamento Europeu e do Conselho, de 7 de Setembro de 2005, relativa ao reconhecimento das qualificações profissionais.

¹⁹ HEALTH TELEMATICS UNIT, *Telehealth...*; Javier SANCHÉZ-CARO, Fernando ABELLÁN, *Telemedicina...*; R.T. SANT'ANNA, A.K. CARDOSO, J.R.M. SANT'ANNA, "Aspectos Éticos...", p. 103/110.

Porém, e porque a telemedicina opera usualmente com processos clínicos electrónicos, abre-se assim a porta a novos riscos e, concomitantemente, novas responsabilidades ²⁰. As normas a ter em consideração são, no plano europeu, a Directiva n.º 95/46/CE ²¹ e o artigo 8.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE); no plano interno, a Lei n.º 67/98 ²².

Da concatenação destas normas resulta que os dados de saúde, como dados especialmente sensíveis que são, reclamam uma especial protecção. Assim, os dados de saúde apenas podem ser recolhidos para propósitos específicos, explícitos e legítimos, bem como deverão revelar-se adequados ao fim em vista.

Algumas das maiores causas de vulnerabilidade no âmbito do uso de *e-health* no contexto hospitalar prendem-se com a falta de segurança das *wirelesses*. Referimo-nos a problemas tais como deficiente criptografia; falhas no processo para separar as redes internas das redes externas; falta de autenticação de usuário; incapacidade para identificar dispositivos intrusos na rede sem fios; inexistência de inventários dos equipamentos e dos

²⁰ Detalhadamente a este respeito *vide* o nosso “O Fim da “Letra de Médico”: Problemas Suscitados pelo Processo Clínico Electrónico em Sede de Responsabilidade Médica”, *Lex Medicinæ*, ano 10, n.º 19, 2013, pelo que não trataremos desta questão aqui.

²¹ Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

²² Lei n.º 67/98, de 26 de Outubro, Lei da Protecção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados).

dispositivos de computador autorizado para aceder à rede hospitalar²³.

2.2. Obrigações destinadas a protecção da privacidade

Sob o responsável pelo tratamento dos dados recaem obrigações várias, nomeadamente, a tomada de medidas técnicas e procedimentais para assegurar aos dados um nível de segurança adequado, com vista a evitar a sua destruição ilegítima ou o acesso indevido, a perda acidental e a alteração não autorizada. Deve igualmente providenciar medidas de informação, de autorização de acesso aos dados e de rectificação e complementação dos mesmos²⁴. Para este efeito poderão revelar-se úteis a encriptação de dados e o recurso a redes fechadas. Outro mecanismo interessante é o uso da assinatura electrónica, uma ferramenta útil para efeitos de manter a confidencialidade, a integridade e a autenticidade dos dados de saúde transmitidos²⁵. A transferência de dados sensíveis para países fora da União Europeia apenas será legítima mediante a garantia de um adequado nível de protecção dos dados por parte desses países ou, caso assim não suceda, apenas em circunstâncias delimitadas e sob apertados requisitos²⁶.

Aplicando este regime à *e-health* conclui-se que todas as entidades que processam os dados, independentemente do país em que estejam, têm que obedecer ao regime geral europeu nesta matéria e, cada uma delas, às especificidades dos respectivos regimes nacionais. No que em particular respeita a *sites*

²³ Peter McLAUGHLIN, “The Proliferation...”, p. 3.

²⁴ Artigo 12.º ss. da Directiva n.º 95/46/CE; Artigo 10.º ss. da Lei n.º 67/98.

²⁵ Javier SANCHÉZ-CARO, Fernando ABELLÁN, *Telemedicina...*, p. 64.

²⁶ Artigo 25.º ss. da Directiva n.º 95/46/CE; Artigos 19 ss. da Lei n.º 67/98.

e *apps* tem-se inclusivamente falado em *privacy by design* ²⁷, precisamente para expressar a ligação entre a construção destes instrumentos da sociedade de informação e as preocupações relacionadas com a privacidade, e que opera essencialmente mediante *privacy-enhancing technologies* (PET's).

A maioria das obrigações em matéria de protecção de dados cabe ao designado “responsável pelo tratamento”. Porém, outras entidades poderão colaborar no processamento dos dados, tais como os fornecedores de armazenamento na *cloud* ²⁸ ou os fornecedores de serviços de internet que hos-

²⁷ Trata-se de um conceito desenvolvido nos anos 90 do século passado pela Dra. Ann CAVOUKIAN, da Ontario's Information and Privacy Commission, e que se pode descrever da seguinte forma, segundo palavras da própria:

“*Privacy by Design* refers to the philosophy and approach of embedding privacy into the design specifications of various technologies. This may be achieved by building the principles of Fair Information Practices (FIPs) into the design, operation and management of information processing technologies and systems. This approach originally had information technology as its primary area of application, but I have since expanded its scope to two other areas. In total, the three areas of application are: (1) information technology; (2) business practices; and (3) physical design and infrastructures.” (Ann CAVOUKIAN, “Privacy by Design”)

²⁸ GRUPO DE TRABALHO PARA A PROTEÇÃO DE DADOS INSTITUÍDO PELO ARTIGO 29.º, “Parecer 05/2012...”, p. 25:

“Os prestadores de serviços de computação em nuvem devem informar os seus clientes de todos os aspectos relevantes (relativos a protecção de dados) dos seus serviços durante as negociações de contratos. Os clientes devem, em especial, ser informados sobre todos os subcontratantes que contribuem para a prestação dos serviços de computação em nuvem e sobre todos os locais em que os dados podem ser armazenados ou tratados pelo prestador de serviços e/ou pelos seus subcontratantes (nomeadamente, se alguns ou todos os

pedam o conteúdo, e que são considerados subcontratantes dos serviços para este efeito (embora possa suceder que o responsável pelo tratamento chame a si todo o processo). A responsabilidade por falhas no tratamento dos dados caberá *prima facie* àquele primeiro — que deve igualmente ter o cuidado de escolher um subcontratante que forneça garantias adequadas de segurança e fiabilidade ²⁹ —, sem prejuízo de

“as obrigações e responsabilidades decorrentes da legislação em matéria de protecção de dados deverem ser claramente definidas e não ser dispersas ao longo de toda a cadeia da externalização ou de subcontratação, a fim de assegurar o controlo efectivo das actividades de tratamento e a atribuição de responsabilidades claras” ³⁰.

A quantidade de dados recolhidos deverá pautar-se por um princípio de proporcionalidade. Ou seja, por um lado têm que ser recolhidos dados suficientes para fornecer o serviço de forma eficaz, contudo, e por outro lado, não se devem recolher mais dados do que os necessários para o funcionamento eficiente do serviço ³¹.

locais se situarem fora do Espaço Económico Europeu (EEE)). Deve ser facultada ao cliente informação pertinente sobre as medidas técnicas e organizativas aplicadas pelo prestador de serviços; o cliente deve, por questão de boas práticas, informar as pessoas em causa sobre o prestador de serviços de computação em nuvem e todos os seus subcontratantes (se aplicável), bem como sobre os locais em que os dados podem ser armazenados ou tratados pelo prestador de serviços e/ou pelos seus subcontratantes”.

²⁹ Artigo 17.º/2 da Directiva n.º 95/46/CE; Artigo 14.º/2 da Lei n.º 67/98.

³⁰ GRUPO DE TRABALHO PARA A PROTEÇÃO DE DADOS INSTITUÍDO PELO ARTIGO 29.º, “Parecer 05/2012...”, p. 12.

³¹ ARTICLE 29 DATA PROTECTION WORKING PARTY 00461, “Opinion 02/2013...”, p. 17, 27.

2.3. A necessidade de regulamentação específica

Este regime sobre protecção de dados revela-se bastante restritivo, nomeadamente, mediante a regra da proibição do tratamento de dados de saúde sem o consentimento do paciente. A isto acresce que a autoridade nacional nesta matéria, a Comissão Nacional de Protecção de Dados, tem-se pautando por requisitos muito exigentes (porventura demasiado) quando se trata de avaliar o consentimento do titular dos dados (expresso, livre, esclarecido, específico). Embora o regime legal existente admita igualmente casos excepcionais em que o tratamento de dados pode ser levado a efeito sem o referido consentimento —

“quando for necessário para efeitos de medicina preventiva, de diagnóstico médico, de prestação de cuidados ou tratamentos médicos ou de gestão de serviços de saúde, desde que o tratamento desses dados seja efetuado por um profissional de saúde obrigado a sigilo ou por outra pessoa sujeita igualmente a segredo profissional, seja notificado à CNPD, nos termos do artigo 27.º, e sejam garantidas medidas adequadas de segurança da informação” (artigo 7.º/4 da Lei n.º 67/98)

— ainda assim as restrições são muitas, sobretudo no plano da entidade de fiscalização. Em função desta constatação tem-se recomendado a criação de uma nova directiva ou de um código de conduta (a serem elaboradas, por exemplo, pelo ARTICLE 29 DATA PROTECTION WORKING PARTY) que, sem perder a linha orientadora de protecção dos dados de saúde e do seu titular, procure simultaneamente harmonizar tal protecção com as exigências da prestação de cuidados de saúde por vias electrónicas³². Esta iniciativa caminha em paralelo

³² EUROPEAN COMMISSION, “Legally E-Health”, p. 22, 23.

com a preocupação revelada pela União Europeia no sentido de conformar os serviços de telemedicina à sociedade de informação ³³.

A ausência de legislação adequada poderá criar ao início uma situação mais permissiva para os operadores económicos deste mercado, mas a médio e longo prazo gerará mais entraves do que aqueles que evita, porque é de supor que os tribunais e as autoridades nacionais de controlo tenderão a assumir o papel de vigilante que o legislador deveria ter chamado a si e, porventura, de forma ainda mais rigorosa. Embora tendencialmente a análise do caso concreto seja mais prudente do que a previsão geral e abstracta da lei, certo é que a prática demonstra que estas autoridades têm adoptado posições extremamente restritivas e exigentes, pelo que uma base legal poderia erguer alguns limites ao seu poder de apreciação, assim como conceder uma mais ampla margem de manobra aos prestadores de serviços.

Por outro lado, a ausência de lei reguladora pode ainda revelar-se perigosa para os Estados nacionais, como o demonstra a decisão do Tribunal Europeu dos Direitos do Homem (TEDH) no caso *I v. Finland*, onde o Estado finlandês foi condenado por falta de mecanismos legais e judiciais na ordem jurídica nacional que permitissem proteger adequadamente os dados de saúde da queixosa, com base no artigo 8.º da Convenção Europeia dos Direitos do Homem (CEDH) ³⁴.

³³ EUROPEAN COMMISSION, “Online Services...”.

³⁴ *I v. Finland*, 17/07/2008:

“The Court notes that the mere fact that the domestic legislation provided the applicant with an opportunity to claim compensation for damages caused by an alleged unlawful disclosure of personal data was not sufficient to protect her private life. What is required in this connection is practical and effective protection to

2.4. O consentimento do titular dos dados

A questão é que na *e-health* o consentimento para tratamento de dados de saúde assume por vezes um carácter menos explícito do que o normal consentimento, sobretudo quando se trate do uso de um serviço disponibilizado por um *site*. Nestes casos a informação que antecede o consentimento — e que funciona como seu requisito de legitimidade — é usualmente disponibilizada no próprio *site*, pedindo-se ao utilizador do mesmo que vá “baixando” a extensa informação que lhe é fornecida e que no final seleccione o já famoso “I accept”/”Eu aceito”, ao qual se segue o envio dos dados pedidos.

Porém, este sistema apresenta alguns problemas: primeiro, não existe a possibilidade de esclarecer qualquer dúvida resultante da informação providenciada; segundo, tão-pouco existe a possibilidade de uma aceitação parcial e do consequente envio parcial de dados (aqueles que o utilizador entendesse enviar). Por outro lado, esta informação, e correlativo consentimento, valem para o inicial tratamento de dados, mas muitas vezes o processo não é repetido face a futuros tratamentos de dados ou quando o prestador do serviço muda a sua política de privacidade ³⁵.

Problemas semelhantes se suscitam quanto às *apps* para *smart devices*, um domínio onde se tem considerado que a mera

excludes any possibility of unauthorized access occurring in the first place. Such protection was not given here. The Court cannot but conclude that at the relevant time the State failed in its positive obligation under Article 8 § 1 of the Convention to ensure respect for the applicant's private life”.

³⁵ Dando conta destes problemas, Paul DE HERT, et al., “Privacy in e-Health...”, p. 3.

instalação da aplicação, ou mesmo a aceitação da respectiva política de privacidade, são insusceptíveis de funcionar como consentimento suficiente para este efeito. É necessário que o propósito para o qual estão a dar o consentimento esteja explicitamente referenciado no ecrã e que fique claro que o utilizador compreendeu efectivamente a informação disponibilizada ³⁶.

Uma vez que são necessários vários consentimentos poder-se-ia pensar em usar uma única fórmula para a sua obtenção conjunta. Contudo, este mecanismo — que sem dúvida tornaria o processo mais expedito — nem sempre é possível (por exemplo, o consentimento para o tratamento de dados de saúde não vale, igualmente, para a obtenção de dados de localização), o que, por sua vez, causa o problema inverso de sobrecarregar o utilizador com vários pedidos de consentimento e causar interferências excessivas na utilização do serviço ³⁷.

3. O recurso às tecnologias de informação para prestação de serviços de saúde

3.1. Sites de informação médica

Tratando-se de serviços médicos providenciados mediante uma página web impõem-se alguns requisitos adicionais ³⁸.

Desde logo, o respectivo responsável (pessoa ou organização) deve estar plenamente identificado (nome, endereço físico, endereço electrónico, formas de contactar o serviço), bem como

³⁶ ARTICLE 29 DATA PROTECTION WORKING PARTY 00461, “Opinion 02/2013...”, p. 15.

³⁷ Emily HAY, Jan DHONT, “Getting a Clean Bill...”, p. 6.

³⁸ COMITÉ PERMANENTE DE MÉDICOS EUROPEOS, *Directrices...*; EUROPEAN COMMISSION, “eEurope 2002...”.

os objectivos e propósitos do serviço e o tipo de audiência a que se dirige, sendo que, caso se dirija a diferentes públicos, poder-se-ão criar distintos níveis de acesso. A mesma informação (nome, direcção, informação para contactos), mas agora em relação ao organismo que concedeu a autorização para exercer a medicina, deve igualmente constar do *site*.

A informação veiculada pelos *sites* de *e-health* deve ser acurada, fidedigna e actualizada (com indicação da data da última actualização), transmitida numa linguagem perceptível ao tipo de audiência esperada. Deve igualmente referir as fontes da informação providenciada e os critérios utilizados para seleccionar e avaliar a informação. As pessoas e instituições que tenham contribuído com informação para o *site* devem igualmente ser indicadas, bem como as respectivas credenciais.

Os *sites* que providenciem informações de saúde devem indicar expressamente se se trata apenas de um site educacional ou para venda de produtos ou serviços, bem como se existe algum interesse financeiro relevante nas indicações que fornecem. Caso o *site* seja financiado por fontes externas, devem estas ser indicadas.

Um ponto que nunca pode ser descurado é a privacidade. Assim, as políticas de segurança e confidencialidade devem ser explicadas, de forma expressa e clara, incluindo as opções “*opt-in*” (necessidade de consentimento expreso) no que respeita ao armazenamento de dados pessoais.

O *site* poderá remeter para outros sites e outros serviços, podendo sempre apresentar um *disclaimer* no sentido de excluir qualquer responsabilidade em relação aos danos por aqueles outros causados. Contudo, e na medida do possível, deve abster-se de remeter para *sites* pouco fidedignos nesta matéria.

Um aspecto a ter em conta na construção de *sites* onde o médico presta serviços (ou, ao menos, os publicita) prende-se com a forma como anuncia os seus serviços. Desde logo, não

deve garantir o sucesso dos actos que pratica, caso contrário, estará a assumir perante potenciais clientes uma obrigação de resultado ³⁹, o que, por sua vez, dará origem a uma presunção de culpa caso advenha algum dano da sua actividade, com a agravante de que as presunções de culpa na nossa jurisprudência dão frequentemente azo a presunção de causalidade e até de ilicitude ⁴⁰.

Outro potencial foco de conflito diz respeito à responsabilidade pela informação disponibilizada (à comunidade em geral, a comunidades específicas, a pacientes devidamente registados ou apenas a profissionais de saúde). De facto, a *web* propicia a divulgação de informação, não só em termos de quantidade e acessibilidade ⁴¹, mas também de custos ⁴². Em contrapartida, acarreta novas dificuldades, tais como o respeito pelos direitos de propriedade intelectual e a triagem de informação fidedigna,

De acordo com a Directiva sobre comércio electrónico a responsabilidade por tais informações cabe essencialmente a quem as providencia, e não ao detentor do *site* que hospeda o serviço e que, nesta medida, funciona apenas como inter-

³⁹ Vera Lúcia RAPOSO, *Do Ato Médico...*, p. 96 ss.

⁴⁰ Vera Lúcia RAPOSO, *Do Ato Médico...*, p. 62 ss., 136/138.

⁴¹ A maior acessibilidade de informação por parte do paciente funcionará como uma fonte adicional de escrutínio à actividade médica, permitindo àquele detectar casos de negligência que, de outra forma, passariam incólumes ou, pelo menos, seriam detectados mais tarde.

Contudo, esta maior acessibilidade apresenta também um *dark side*, na medida em que, e atendendo às incorreções da informação facultada pelos mais diversos e duvidosos *sites*, os pacientes não estarão necessariamente mais esclarecidos, simplesmente se considerarão mais esclarecidos, quantas vezes incorrendo em erros graves e pretendendo mesmo discutir com o seu médico complexas questões clínicas de igual para igual, o que inclusivamente fomenta a litigância injustificada.

⁴² Nicolas P. TERRY, “Cyber-Malpractice...”, p. 330.

mediário ⁴³. Este último apenas responderá “se tiver conhecimento de actividade ou informação cuja ilicitude for manifesta e não retirar ou impossibilitar logo o acesso a essa informação”, exigindo-se que “tenha ou deva ter consciência do carácter ilícito da informação” ⁴⁴. Contudo, não impende sobre este qualquer obrigação geral de vigilância sobre as informações que transmite ou armazene, nem o dever de procurar activamente eventuais ilicitudes ⁴⁵.

O mero facto de o *site* incluir um *disclaimer* onde os autores da informação afastam qualquer responsabilidade por eventuais danos derivados da informação facultada, e recusam que a sua intervenção possa substituir uma consulta médica, não parece suficiente para, em termos efectivos, excluir essa responsabilidade ⁴⁶. É certo que o artigo 485.º do Código

⁴³ A questão da responsabilidade pela informação tem sido amplamente discutida pelos tribunais no que respeita ao conteúdo de livros e material similar. A orientação geral que decorre destas decisões é que a responsabilidade do autor depende de circunstâncias várias — tais como a natureza da publicação, o público-alvo, a determinação da causalidade, a previsibilidade do dano —, ao passo que a responsabilidade do editor é, em princípio, afastada. Cfr. Nicolas P. TERRY, “Cyber-Malpractice...”, p. 353.

⁴⁴ Artigo 14.º da Directiva n.º 2000/31/CEE; Artigos 16.º/1/2 do Decreto-Lei n.º 7/2004, de 7 de Janeiro, alterado pelo Decreto-Lei n.º 62/2009, de 10 de Março e pela Lei n.º 46/2012 de 29 de Agosto. Em termo gerais *vide* Sofia de Vasconcelos CASIMIRO, *Responsabilidade Civil...*

⁴⁵ Artigo 15/1.º da Directiva n.º 2000/31/CEE; Artigo 12.º do Decreto-Lei n.º 7/2004.

⁴⁶ Veja-se um possível exemplo de um *disclaimer* desta natureza:

“The contents of the WebMD Site, such as text, graphics, images, and other material contained on the WebMD Site ("Content") are for informational purposes only. The Content is not intended to be a substitute for professional medical advice, diagnosis, or treatment. Always seek the advice of your physician or other qualified health provider with any questions you may have regarding a medical condition. Never disregard professional medical advice or delay

Civil (CC) exclui a responsabilidade por conselhos, recomendações ou informações ⁴⁷, mas quando um *site* se apresenta a si mesmo como fornecedor de informação de saúde fidedigna é duvidoso que semelhante *disclaimer* seja bastante para afastar a responsabilidade, sobretudo em casos de negligência grosseira na informação comunicada ⁴⁸, sem prejuízo de semelhante cautela ser uma precaução importante e, segundo nos parece, poder efectivamente afastar a responsabilidade em caso de negligência leve no conteúdo da infor-

in seeking it because of something you have read on the WebMD Site! If you think you may have a medical emergency, call your doctor or 911 immediately. WebMD does not recommend or endorse any specific tests, physicians, products, procedures, opinions, or other information that may be mentioned on the Site. Reliance on any information provided by WebMD, WebMD employees, others appearing on the Site at the invitation of WebMD, or other visitors to the Site is solely at your own risk. The Site may contain health — or medical-related materials that are sexually explicit. If you find these materials offensive, you may not want to use our Site. The Site and the Content are provided on an "as is" basis (<<http://www.webmd.com/about-webmd-policies/additional-info?ss=fr>>).

⁴⁷ “1. Os simples conselhos, recomendações ou informações não responsabilizam quem os dá, ainda que haja negligência da sua parte.

2. A obrigação de indemnizar existe, porém, quando se tenha assumido a responsabilidade pelos danos, quando havia o dever jurídico de dar conselho, recomendação ou informação e se tenha procedido com negligência ou intenção de prejudicar, ou quando o procedimento do agente constitua facto punível.”

⁴⁸ Afastando a responsabilidade daquele que fornece a informação, ao que parece quaisquer que sejam as circunstâncias e o grau de culpa do agente, e inclusivamente invocando *the right to free speech* do *1st Amendment*, Paul SPRADLEY, “Telemedicine...”, p. 326, 327. Segundo o autor, “[c]ertain recourse may exist where a provider is willfully attempting to deceive users or solicit money, but even in those cases, medical malpractice is an unlikely fit” (p. 326). Contudo, o que aqui advogamos não é propriamente um processo por responsabilidade médica, mas sim por informação errónea.

mação disponibilizada ou na forma da sua comunicação. Será sobretudo útil para reforçar a ideia de que aquela informação não dispensa a intervenção de um médico pois

“[i]f a patient reasonably believes that the service she is receiving will eliminate the need for traditional face-to-face medical treatment then the practitioner will probably be subjected to malpractice liability”⁴⁹.

3.2. Comunicação electrónica entre médico e paciente

O correio electrónico é uma ferramenta útil para as comunicações à distância, inclusivamente no âmbito da prestação de cuidados de saúde. Porém, o médico deve ter particulares cautelas com a forma como comunica com o seu paciente⁵⁰ (ainda que se revele um meio de comunicação mais seguro e fidedigno do que mecanismos de mensagens instantâneos, tais como o “*What’s up*” ou o “*Skype*”), especialmente porque a perenidade das coisas escritas é muito superior à de meras conversas orais (sublinhe-se mesmo que os *e-mails* nunca desaparecem completamente e podem ser facilmente recuperados mediante uma auditoria⁵¹). Deve igualmente confirmar que a sua apólice de responsabilidade civil cobre danos resultantes de conselhos e prescrições realizados por *e-mail*. Por outro lado, ao correio electrónico andam associados perigos tais como as interrupções de fornecimento de serviço, ataques por *hackers* e outras falhas de segurança, destruição de dados ocasionadas por falhas técnicas ou vírus e mal entendidos resultantes da ausência de *feedback* imediato do interlocutor.

⁴⁹ Paul SPRADLEY, “Telemedicine...”, p. 327.

⁵⁰ COMITÉ PERMANENTE DE MÉDICOS EUROPEOS, *Directrices...*; Vera Lúcia RAPOSO, “O Fim da “Letra De Médico”...”.

⁵¹ Vera Lúcia RAPOSO, “O Fim da “Letra De Médico”...”.

O médico nunca deve utilizar o *e-mail* como substituto das conversas pessoais com o paciente, mas apenas recorrer a ele quando o assunto em causa não exija esse encontro pessoal. A oportunidade do uso do *e-mail* deve inclusivamente ficar previamente agendada com o paciente, estipulando-se que não deverá ser usado para futilidades nem para assuntos urgentes e/ou graves. Ainda quando o correio electrónico se revele útil, seguro e eficaz — comunicação de resultados laboratoriais; seguimento de uma doença crónica ou de tratamento prologado; medidas de promoção da saúde; questões administrativas, como a marcação de uma consulta — algumas regras devem ser cumpridas, muitas delas resultantes de *guidelines* criadas por organismos internacionais ⁵²:

- (a) Antes de iniciar a comunicação por *e-mail* o médico deve informar o paciente de todos os aspectos relevantes, nomeadamente os perigos que esta forma de comunicação poderá acarretar para a privacidade daquele;
- (b) Deve igualmente confirmar que possui o equipamento necessário para este tipo de comunicação, especialmente uma rede segura, bem como *hardwares* e *softwares* que cumpram os necessários requisitos;
- (c) O endereço de *e-mail* utilizado, quer pelo paciente, quer pelo médico, deve ser sempre o mesmo;
- (d) A linguagem deve ser clara e acessível a um leigo (como em regra o é o paciente), mas simultaneamente rigorosa e restrita ao assunto em discussão;
- (e) Os *e-mails* devem ser todos enviados em “*reply*” ao *e-mail* original, de forma a manter um *track* da conversa que permita perceber na íntegra cada um dos conteúdos;

⁵² Estas resultam, no geral, da American Medical Informatics Association, do eRisk Working Group for Healthcare e da American Medical Association (*apud* Sharon HOFFMAN, Andy PODGURSKI, “E-Health Hazards...”, p. 1573).

- (f) Os *e-mails* devem ser enviados com confirmação de entrega e de leitura por parte do destinatário;
- (g) O tempo de resposta deve ser previamente estipulado com o paciente;
- (h) O médico deve incluir em cada *e-mail* a sua identificação e a forma como o paciente pode chegar ao seu contacto directo e, paralelamente, o paciente deve-se identificar de forma completa no *e-mail*, bem como ao assunto em causa;
- (i) Todos os *e-mails* (enviados e recebidos) devem ser arquivados de forma ordenada no processo clínico do paciente.

3.3. *Apps para smartphones relacionadas com a saúde*

Existem hoje disponíveis no mercado inúmeras *apps* (aplicações) relacionadas com a saúde ⁵³, por exemplo, para monitorizar determinados sintomas, receber resultados laboratoriais, enviar dados para um médico distante ou renovar prescrições de medicamentos, quando usadas por pacientes; ou para obter informação médica de cariz técnico, no caso dos profissionais de saúde.

A norte-americana Food and Drugs Administration (FDA) já se pronunciou sobre estas aplicações, estendendo a algumas delas o regime dos dispositivos médicos ⁵⁴. A FDA opera com o conceito de aplicações médicas móveis (*mobile medical apps*), isto é, *apps* que, atendendo à sua fun-

⁵³ Estima-se que, a nível mundial, 500 milhões de utilizadores de *smartphones* usem *apps* relacionadas com a saúde e que em 2018 passemos para perto de 2 milhões (<<http://www.research2guidance.com/500m-people-will-be-using-healthcare-mobile-applications-in-2015/>>, 06/11/2013).

⁵⁴ Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff, at <<http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf>> (28/06/2013).

ção, podem ser consideradas dispositivos médicos ⁵⁵. A intenção da FDA é regular apenas aquelas *mobile medical apps* que assumam um risco alto (classe III) ou mesmo moderado (classe II), excluindo assim aquelas que envolvam um risco mínimo para os usuários. Nesta última categoria incluem-se aquelas que auxiliem o utente a gerir a sua doença ou condição, sem fornecer sugestões de tratamento específico; que lhe disponibilizem ferramentas simples para organizar e controlar os seus dados de saúde, ou informações de saúde genéricas; que lhe permitam comunicar ao médico informações relativas à sua saúde; ou possibilitem a interação com o respectivo processo clínico ⁵⁶.

Porém, a correspondente europeia da FDA, a European Medicines Agency (EMA), apenas dispõe de competências em sede de fármacos, pelo que não pode esclarecer sobre esta matéria. Tão-pouco a nossa autoridade nacional, o Infarmed (que tem efectivamente competências para medicamentos e dispositivos médicos) manifestou alguma posição nesse sentido. Aliás, no contexto europeu tem sido essencialmente o ARTICLE 29 DATA PROTECTION WORKING PARTY a tratar das aplicações para *smartphones*, logo, de uma perspetiva exclusiva de privaci-

⁵⁵ “Mobile apps that transform a mobile platform into a regulated medical device and therefore are mobile medical apps: These mobile apps use a mobile platform’s built-in features such as light, vibrations, camera, or other similar sources to perform medical device functions (e.g., mobile medical apps that are used by a licensed practitioner to diagnose or treat a disease). Possible product codes:Varies depending on the intended use and function of the mobile medical app; see additional examples below” (<<http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/MobileMedicalApplications/ucm368743.htm>>, 29/11/2013).

⁵⁶ A FDA também esclarece que não regula a venda destas aplicações, nem considera as entidades que as vendem (Tunes Apps Store ou Google Play Store) como fabricantes de dispositivos médicos.

dade. Mas, e tal como vimos suceder nos EUA, não está excluído que alguma destas *apps* sejam dispositivos médicos, tendo em conta a definição que desta categoria é feita na Directiva europeia⁵⁷ e na lei nacional⁵⁸.

O que ficou dito a propósito das tecnologias de informação e privacidade vale para as *apps*, embora com algumas especificidades. Atendendo ao seu modo de funcionamento assume particular relevo o já referido princípio da proporcionalidade na recolha de dados. Ou seja, se a tutela da privacidade exige dados de geolocalização deve-se evitar contínuas recolhas desses dados, a não ser que sejam absolutamente necessários para o funcionamento da aplicação; ou se a *app* se sincroniza com o calendário do utilizador ou com o seu livro de endereço devem ser tomadas medidas para não usar mais dados do que os absolutamente necessários⁵⁹.

⁵⁷ Artigo 1.º/2/a da Directiva 93/42/CEE do Conselho de 14 de Junho de 1993 relativa aos dispositivos médicos:

“Dispositivo médico: qualquer instrumento, aparelho, equipamento, *software*, material ou outro artigo, utilizado isoladamente ou em combinação, incluindo o *software* destinado pelo seu fabricante a ser utilizado especificamente para fins de diagnóstico e/ou terapêuticos e que seja necessário para o bom funcionamento do dispositivo médico, destinado pelo fabricante a ser utilizado em seres humanos para efeitos de: diagnóstico, prevenção, controlo, tratamento ou atenuação de uma doença; diagnóstico, controlo, tratamento, atenuação ou compensação de uma lesão ou de uma deficiência, estudo, substituição ou alteração da anatomia ou de um processo fisiológico; controlo da concepção, cujo principal efeito pretendido no corpo humano não seja alcançado por meios farmacológicos, imunológicos ou metabólicos, embora a sua função possa ser apoiada por esses meios”.

⁵⁸ Artigo 3.º/t do Decreto-Lei n.º 145/2009 de 17 de Junho, que repete a definição anterior.

⁵⁹ Emily HAY, Jan DHONT, “Getting a Clean Bill...”, p. 4.

4. Apreciações finais

Num mundo que já se fala num “ATM model of medical care”⁶⁰ urge que profissionais de saúde e profissionais jurídicos repensem a prestação de cuidados de saúde mediante novas tecnologias. Adivinha-se uma realidade onde o paciente poderá *twittar* sobre a sua condições de saúde, onde grupos de *Facebook* discutirão sobre estados clínicos e o *Skype* estará ao serviço das consultas médicas.

A tecnologia mudou o nosso mundo e a prática médica foi uma das mais alteradas. O que antes tinha lugar na privacidade de um consultório médico pode hoje desenrolar-se numa sala de chat ou numa página de *Facebook*⁶¹, o que terá os seus benefícios, mas tem também muitos inconvenientes. A melhor forma de os evitar é criar um quadro legal que, à partida, defina os direitos e deveres de cada uma das partes envolvidas.

Pode ser que num futuro (mais ou menos) próximo seja boa prática médica que o médico *poke* o seu paciente. Nos dias de hoje é ainda duvidoso.

Bibliografia

ARTICLE 29 DATA PROTECTION WORKING PARTY — “Opinion 02/2013 on Apps on Smart Devices” 00461/13/EN WP 202, Adopted on 27 February 2013, at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf> (02/01/2014).

CASIMIRO, Sofia de Vasconcelos — *Responsabilidade Civil pelo Conteúdo da Informação Transmitida pela Internet*, Almedina, Coimbra, 2000.

CAVOUKIAN, Ann — “Privacy by Design”, at <<http://www.ipc.on.ca/images/Resources/privacybydesign.pdf>> (06/11/2013).

⁶⁰ Nicolas P. TERRY, “Structural and Legal...”.

⁶¹ <<http://online.wsj.com/news/articles/SB10001424127887324900204578283900262408308#!>> (04/11/2013).

- CLIFTON, Anika D. — “Licensure, Reimbursement and Liability in Telemedicine: An Academic Perspective”, *Annals of Health Law — Advance Directive*, 18, fall 2008
- COMITÉ PERMANENTE DE MÉDICOS EUROPEOS (CPME) — *Directrices del CPME Sobre Telemedicina*, at <<https://www.cgcom.es/sites/default/files/Directrices%20sobre%20telemedicina%202002%20Boletín%2096.pdf>> (31/10/2013).
- DE HERT, Paul, et al. — “Privacy in e-Health Put to Practice: The Concept of Concierge as a Physical and Technical Interface”, in *Third European Conference on Health Law — Book of Proceedings*, 2011.
- EUROPEAN COMMISSION — “eEurope 2002: Quality Criteria for Health related Websites”, *Journal of Medical Internet Research*, 4(3):e15, 2002 at <<http://www.jmir.org/2002/3/e15/>> (30/09/2013).
- “Legally E-Health”, Contract #30-CE-0041734 /00-55, at <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=3149> (05/12/2013).
- “Online Services, Including e-Commerce, in the Single Market-Commission Staff Working Document (Accompanying the Document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions): A Coherent Framework to Boost Confidence in the Digital Single Market of e-Commerce and Other Online Services”, SEC(2011) 1641 final, Brussels, 11.1.2012.
- EUROPEAN COMMISSION — *Commission Staff Working Document on the Applicability of the Existing EU Legal Framework to Telemedicine Services — Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions — e-health Action Plan 2012-2020 — Innovative Healthcare For The 21st Century*, SWD(2012) 414 final, Brussels, 6.12.2012.
- GRUPO DE TRABALHO PARA A PROTEÇÃO DE DADOS INSTITUÍDO PELO ARTIGO 29.º — “Parecer 05/2012 relativo à Computação em Nuvem”, 01037/12/EN WP 196, adoptado a 1 de Julho de 2012, at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_pt.pdf (06/01/2014).
- HAY, Emily; DHONT, Jan — “Getting a Clean Bill of Health for Privacy in Your Mobile App”, Data Privacy Department, Lorenz Brussels, *International Lawyers*, at <http://www.lorenz-law.com/wp-content/uploads/Article_Getting-a-Clean-Bill-of-Health-for-Privacy-in-Your-Mobile-App.pdf> (05/12/2013).

- HEALTH TELEMATICS UNIT — *Telehealth and e-Health Policy Considerations for Alberta*, Health Telematics Unit, University of Calgary for Alberta Health and Wellness, August 2004 (Version 2), at <<http://www.fp.ucalgary.ca/telehealth/Team%20Members/Publications/Alberta%20e-Health%20Policy%20Report-Ver2-FIN%20FIN.pdf>> (15/10/2013).
- HILDEBRAND, Paul — “Telemedicine Risk Management — White Paper”, at <http://lovell.com/wp-content/uploads/2013/01/White-Paper-Telemedicine.pdf> (10/01/2014).
- HOFFMAN, Sharona; PODGURSKI, Andy — “E-Health Hazards: Provider Liability and Electronic Health Record Systems”, *Berkeley Technology Law Journal*, 24(4), 2009.
- MCLAUGHLIN, Peter — “The Proliferation of Mobile Devices and Apps for Health Care: Promises and Risks”, *Privacy & Security Law Report*, 10, PVLR 26, 2011.
- PEREIRA, Alexandre Libório Dias — “Patient Safety in Telemedicine”, no âmbito da Conferencia da European Association of Health Law, Coimbra, 9/10 de Outubro de 2013.
- RAPOSO, Vera Lúcia — *Do Ato Médico ao Problema Jurídico (Breves Notas sobre o Acolhimento da Responsabilidade Médica Civil e Profissional na Jurisprudência Nacional)*, Almedina, Coimbra, 2013.
- “O Fim da “Letra De Médico”: Problemas Suscitados pelo Processo Clínico Electrónico em Sede de Responsabilidade Médica”, a publicar na revista *Lex Medicinæ*.
- SANCHÉZ-CARO, Javier; ABELLÁN, Fernando — *Telemedicina y Protección de Datos Sanitarios*, Acesoramiento en Derecho Sanitario, Adesa, Granada, 2002.
- SANT’ANNA, R.T.; CARDOSO, A.K.; SANT’ANNA, J.R.M. — “Aspectos Éticos e Legais da Telemedicina Aplicados a Dispositivos de Estimulação Cardíaca Artificial”, *Reblampa*, 18(3), 2005.
- TERRY, Nicolas P. — “Cyber-Malpractice: Legal Exposure for Cybermedicine”, *American Journal of Law & Medicine*, 25, 1999.
- “Structural and Legal Implications of E-Health”, *Journal of Health Law*, 33(4), 2000.
- WEINER, Shira D. — “Mouse-To-Mouse Resuscitation: Cybermedicine and the Need for Federal Regulation”, *Cardozo Law Review*, 23, 2002.

Resumo: O fenómeno designado por *e-health* pretende expressar as diversas formas de cuidados de saúde prestados à distância. Inclui, obviamente, a tradicional telemedicina, muitos vezes praticada além fronteiras,

com todos os problemas que daí derivam, mesmo no âmbito de um espaço que se supõe ser um mercado único e sem fronteiras, como sucede com a União Europeia. Mas o termo *e-health* inclui também outros mecanismos mais recentes e complexos, como por exemplo os *sites* de informação médica e de conselhos médicos, mas também as diversas aplicações de cariz médico para *smartphones*. Serão estes os temas a ser desenvolvidos no presente estudo, tendo como base a ideia de que aquilo que o futuro nos reserva é muito mais do que o que presente auspica.

Palavras-chave: *e-health*; cuidados médicos transfronteiriços; *websites*; aplicações médicas; privacidade.

The doctor just poked you (E-health new challenges)

Abstract: The phenomenon designated as e-health aims to express the various forms of at distance health care. It includes, of course, the traditional telemedicine, frequently practiced across borders, with all the problems that derive therefrom, even within a space that is supposed to be a single and borderless market, as happens with the European Union. But the term e-health also includes more recent and complex mechanisms, such as websites of medical information and medical advice, but also the various medical applications for smartphones. These are the topics to be developed in the present study, having for base the idea that the future holds much more than what the present foresees.

Keywords: e-health; cross border healthcare; websites; medical apps; privacy.

Vera Lúcia Raposo

Faculdade de Direito da Universidade de Coimbra
Faculdade de Direito da Universidade de Macau