CONSELHO NACIONAL DE ÉTICA PARA AS CIÊNCIAS DA VIDA

CONSELHO NACIONAL DE ÉTICA PARA AS CIÊNCIAS DA VIDA

ACESSO AOS DADOS DE SAÚDE
DOCUMENTO DE TRABALHO

Grupo de Trabalho:

Daniel Torres Gonçalves (Coord.), Carlos Maurício Barbosa, Sérgio Deodato, Sandra Horta e Silva.

NOTA PRÉVIA: *Documento de apoio à reflexão sobre o tema do "acesso aos dados em saúde", da responsabilidade dos seus autores, como tal não votado pelo plenário do CNECV. Elaborado em 2016 e atualizado em 2017.*

INTRODUÇÃO

O Conselho Nacional de Ética para as Ciências da Vida (CNECV), reconhecendo a pertinência do tema, decidiu, por sua iniciativa, refletir sobre o acesso à informação de saúde. Sabendo a multiplicidade de vertentes relevantes para análise sobre a informação em saúde, e sem prejuízo de ulteriores análises sobre este assunto, pretende-se com o presente enquadrar especificamente o tema do acesso a tal informação.

A. DO ENQUADRAMENTO JURÍDICO

1. O ACESSO À INFORMAÇÃO DE SAÚDE NA CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA

A intimidade da vida privada dos cidadãos é objeto de tutela jurídica, nomeadamente ao nível Constitucional. A intimidade da vida privada é protegida pela Constituição da República Portuguesa, adiante designada CRP, através do artigo 26.º, n.º1.[1] Pela sua natureza, a informação de saúde faz parte dos bens tutelados por tal disposição.

Sendo a informação de saúde protegida pela tutela oferecida à intimidade da vida privada, o acesso a tal informação deverá ser limitado. Devemos, assim, incluir na proteção da esfera da intimidade da vida privada dos cidadãos, os seus dados de saúde, que, por alguma razão, se encontrem registados numa plataforma informática de uma organização de saúde.

A Constituição da República Portuguesa, adiante designada CRP, apresenta um conjunto de provisões relevantes para o acesso à informação de saúde. Cabe, neste ponto, referir duas vertentes tratadas pela CRP.

Em primeiro lugar, a proteção dos dados pessoais informatizados encontra-se consagrada no artigo 35º da Constituição da República Portuguesa, devendo ser analisada numa dupla perspetiva. Numa perspetiva positiva, a referida disposição garante ao cidadão o livre acesso e a possibilidade de supervisionar o uso da informação que lhe diz respeito.[2] Por

[1] "A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação".

[2] Artigo 35º nº 1 da CRP: *"Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam."*

outro lado, numa perspetiva negativa, a disposição proíbe o acesso e a utilização dos seus dados pessoais por terceiros[3].

O direito de acesso vai além do direito a conhecer os dados e corrigi-los se for o caso; abrangendo, igualmente, o conhecimento da finalidade do seu tratamento, por forma a garantir a inexistência de abuso e/ou manipulação dos mesmos.

O nº 2 do artigo 35º da CRP impôs ao legislador a definição de "dados pessoais"[4], o que veio a ocorrer somente com a Lei n.º 10/91, de 27 de abril, por força da Convenção 108 do Conselho da Europa sobre a proteção das pessoas relativamente ao tratamento automatizado de dados pessoais, adotada em Estrasburgo em 28 de Janeiro de 1981[5].

Em segundo lugar, a CRP vem tratar particularmente do ponto relativo à informação constante de documentos da Administração Pública. Consagrando o princípio da administração aberta,[6] o artigo 268.º, n.º 2, da CRP consagra que *"Os cidadãos têm também o direito de acesso aos arquivos e registos administrativos, sem prejuízo do disposto na lei em matérias relativas à segurança interna e externa, à investigação criminal e à intimidade das pessoas"*.

2. O ACESSO À INFORMAÇÃO DE SAÚDE NA LEGISLAÇÃO ORDINÁRIA

Surgindo como uma concretização do artigo 26.º, n.º1, da CRP, o Código Civil, no seu artigo 80.º, prevê o direito à reserva sobre a intimidade da vida privada.[7] Este direito é aplicável a um conjunto alargado de realidade, entre as quais se encontrará a informação de saúde. Existe, contudo, larga legislação especificamente direcionada para este tipo de informação.

A Carta dos Direitos e Deveres dos Doentes (CDDD), elaborada pela Direcção-Geral da Saúde e divulgada em Março de 1997 reconhece o direito de acesso à informação sobre dados de saúde por parte do titular e está subjacente a toda a legislação produzida em Portugal sobre a matéria.

O regime de acesso a dados relativos à saúde encontra-se plasmado essencialmente em quatro diplomas:

---

[3] Artigo 35º nº 4 da CRP: *"É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei."*

[4] Artigo 35º nº 2 da CRP: *"A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente."*

[5] Este diploma veio a ser revogado pela Lei n.º 67/98, de 26 de Outubro, alterado pela Lei n.º 41/2004, de 18 de agosto.

[6] Este princípio é concretizado no artigo 17.º do Código do Procedimento Administrativo, onde se dispõe que "Todas as pessoas têm o direito de acesso aos arquivos e registos administrativos, **mesmo quando nenhum procedimento que lhes diga diretamente respeito** esteja em curso, sem prejuízo do disposto na lei em matérias relativas à segurança interna e externa, à investigação criminal, ao sigilo fiscal e à privacidade das pessoas" (sublinhado nosso).

[7] "Todos devem guardar reserva quanto à intimidade da vida privada de outrem".

- 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 (Regulamento Geral sobre a Proteção de Dados, adiante RGPD);

- Lei da Proteção de dados pessoais: Lei n.º 67/98, de 26/10,[8] doravante designada por LPD, ainda em vigor em tudo o que não contrarie o RGPD;

- Lei que regula a informação genética pessoal e informação de saúde: Lei n.º 12/2005, de 26 de Janeiro;

- Regime de acesso à informação administrativa, aprovado pela Lei n.º26/2016, de 22 de agosto.

A LPD dá-nos uma perspetiva generalista do que constituem dados pessoais: *"qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ('titular dos dados'); é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social"* - artigo 3º alínea a) da LPD.

Depois, conforme decorre do artigo 2º da Lei 12/2015, de 26 de Janeiro, são dados relativos à saúde "*todo o tipo de informação directa ou indirectamente ligada à saúde, presente ou futura, de uma pessoa, quer se encontre com vida ou tenha falecido, e a sua história clínica e familiar."* Importa, ainda, referir que os dados relativos à saúde englobam os dados relativos à vida sexual e os dados genéticos.

2.1. NATUREZA PÚBLICA OU PRIVADA DA ENTIDADE DETENTORA DA INFORMAÇÃO DE SAÚDE

As regras relativas ao acesso à informação de saúde variam consoante a natureza da entidade detentora dessa informação. Na verdade, no nosso ordenamento jurídico, vigoram simultaneamente dois regimes distintos, cuja aplicação varia consoante a natureza pública ou privada das entidades detentoras da informação de saúde:

- O regime que regula a proteção de dados pessoais e, em particular, a informação genética pessoal e informação de saúde;

- O regime de acesso aos documentos administrativos detidos por entidades integradas no Serviço Nacional de Saúde.

[8] A Lei n.º 67/98, de 26 de Outubro resultou da transposição para a ordem jurídica nacional da Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, entretanto revogada pelo RGPD.

A referida dualidade é extensível às entidades fiscalizadoras. De facto, a aplicação dos referidos regimes é fiscalizada por duas entidades administrativas independentes. Por um lado, o primeiro regime, tem como entidade competente a CNPD - Comissão Nacional de Protecção de Dados. Por outro, a CADA - Comissão de Acesso aos Documentos Administrativos é competente relativamente aos documentos administrativos.

O RGPD *"aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados".*[9] O RGPD, como a LPD, faz incluir os dados de saúde na categoria de dados pessoais sensíveis, os quais são objeto de uma proteção acrescida. Salvo raras exceções, não podem ser objeto de tratamento; e, a sê-lo, obedecem sempre a um regime específico próprio.[10]

Por seu turno, o Regime de acesso à informação administrativa regula o acesso à mesma informação de saúde, mas quando os dados se encontram inseridos em documentos administrativos.[11] Os documentos administrativos que integrem dados de saúde são considerados documentos nominativos por conterem dados pessoais – artigo 3º nº 1 do Regime.

Nos termos da alínea c) do n.º 1 do artigo 30.º do Regime,, compete à CADA *"Emitir parecer sobre o acesso aos documentos administrativos"* e, segundo a alínea d) da mesma disposição, compete à mesma entidade *"Emitir parecer sobre a comunicação de documentos entre serviços e organismos da Administração, a pedido da entidade requerida ou da interessada, a não ser que se anteveja risco de interconexão de dados, caso em que a questão é submetida à apreciação da Comissão Nacional de Protecção de Dados".*[12]

Por último, convém referir que é entendimento da CADA que o acesso pelo titular ou por terceiro é regido pelo Regime, anteriormente pela LADA, mesmo que as informações de saúde constem numa base de dados. [13]

Em conclusão, da leitura atenta da CRP e da legislação ordinária resulta que o RGPD e a LPD assentam no princípio geral de proibição ou limitação de acesso aos dados por terceiros, excecionando os casos de permissão a um acesso condicionado aos dados de

[9] Artigo 4.º
[10] Artigo 9.º do RGPD.
[11] Nos termos do artigo 1.º, n.º3, da Lei n.º26/2016, de 22 de agosto, *"O acesso a informação e a documentos nominativos, nomeadamente quando incluam dados de saúde, produzidos ou detidos pelos órgãos ou entidades referidos no artigo 4.º, quando efetuado pelo titular dos dados, por terceiro autorizado pelo titular ou por quem demonstre ser titular de um interesse direto, pessoal, legítimo e constitucionalmente protegido na informação, rege -se pela presente lei, sem prejuízo do regime legal de proteção de dados pessoais"*.
[12] Na alínea i) do artigo 3º da LPD vem definida a interconexão de dados pessoais como a *"forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de um ficheiro ou ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade"*.
[13] Parecer nº274/2007 de 2007.11.14 e Parecer n.º 131/2011 de 2011.04.12

saúde. Contrariamente, a LADA estrutura-se no respeito pelo princípio do livre acesso aos documentos administrativos, excecionando os casos de restrição de acesso à informação de saúde.

Existem dúvidas, jurídicas e éticas, sobre a dualidade de regimes que assenta sobre a natureza da entidade que detém a informação de saúde. Sobre esta dualidade de regimes, pronunciou-se o Provedor de Justiça alertando *"para a necessidade de assegurar a uniformização e coerência dos regimes legais em causa e garantir que não estão legitimados dois níveis diferentes de proteção de dados pessoais referentes à saúde."*[14] Ademais, numa exposição apresentada pelo Provedor de Justiça à Assembleia da República é sugerido a este órgão *"a ponderação das razões que aconselham à intervenção legislativa pertinente, de modo a garantir:*

a) a clarificação dos motivos que justificam a existência de dois regimes legais de protecção de dados de saúde, unicamente baseados na natureza pública ou privada das entidades que detêm;

b) a delimitação expressa e inequívoca dos respectivos âmbitos materiais de apreciação;

c) a confirmação de que a situação descrita em circunstância alguma tolera níveis diferentes de protecção de dados pessoais referentes à saúde, em caso de dúvida desencadeando-se as medidas consideradas adequadas à superação da situação." [15]

Sobre este ponto, apontamos sérias reservas sobre a existência de fundamentos éticos que sustentem a diferença de regimes apontada, reconhecendo que as recentes alterações legislativas vieram mitigar o alcance prático de tais diferenças.

3. REGIME JURÍDICO 3.1. O ACESSO PELO TITULAR DA INFORMAÇÃO

O acesso à informação de saúde é emanação do princípio ético da autonomia, traduzido na participação informada dos cidadãos na decisão sobre aspetos relacionados com a sua saúde. Face a tal princípio, em regra, o cidadão tem o direito a aceder a toda a informação constante do seu processo clínico - n.º 2 do artigo 3.º da Lei n.º 12/2005.[16]

As exceções, igualmente plasmadas na lei, comportam duas situações. A primeira respeita às anotações pessoais do médico. É o que resulta do disposto na alínea a) do n.º 2 do artigo 3.º do Regime de acesso à informação administrativa ao determinar que não se consideram documentos administrativos *"As notas pessoais, esboços, apontamentos,*

[14] "Direitos fundamentais na prática do Provedor de Justiça" José de Faria Costa, Provedor de Justiça Conferência Tribunais e Direitos Humanos: Direitos fundamentais na jurisprudência do STJ e na prática da Provedoria, realizada no Centro de Estudos Judiciários em 11 de Julho de 2014

[15] http://www.provedor-jus.pt/archive/doc/6472_09AR.pdf

[16] *"O titular da informação de saúde tem o direito de, querendo, tomar conhecimento de todo o processo clínico que lhe diga respeito, salvo circunstâncias excepcionais devidamente justificadas e em que seja inequivocamente demonstrado que isso lhe possa ser prejudicial, ou de o fazer comunicar a quem seja por si indicado."*

comunicações eletrónicas pessoais e outros registos de natureza semelhante, qualquer que seja o seu suporte".

A segunda exceção respeita ao privilégio terapêutico e vem contemplada no n.º 2 do artigo 3.º da Lei n.º 12/2005[17].

É de notar que, até recentemente, existiu uma diferença entre os regimes aplicáveis às entidades públicas e privadas relativamente à intermediação por médico. Por efeito de diferentes diplomas legais, os regimes encontraram uma uniformização na não exigência da intermediação médica.

Em sede de documentos na posse de entidades públicas, *"O acesso à informação de saúde por parte do seu titular, ou de terceiros com o seu consentimento ou nos termos da lei, é exercido por intermédio de médico se o titular da informação o solicitar"* - artigo 7.º do Regime de acesso à informação administrativa. Isto significa que ficará na disponibilidade do requerente a determinação da existência de intermediação por um médico no acesso aos dados de saúde.

Quanto aos documentos na posse de entidades privadas, o acesso faz-se, ao abrigo do regime ainda em vigor, necessariamente através de intermediação médica, conforme dispõe o n.º 5 do artigo 11.º da LPD: *"O direito de acesso à informação relativa a dados de saúde, incluindo os dados genéticos, é exercido por intermédio de médico escolhido pelo titular dos dados".*[18] Note-se que no mesmo sentido ia o n.º3 do artigo 3.º da Lei n.º 12/2005: *"O acesso à informação de saúde por parte do seu titular, ou de terceiros com o seu consentimento, é feito através de médico, com habilitação própria, escolhido pelo titular da informação".*

Também o mencionado artigo 3.º, n.º3 da Lei n.º12/2005, foi alterado pela Lei n.º26/2016, de 22 de agosto, deixando de prever ao requisito da intermediação: *"O acesso à informação de saúde por parte do seu titular, ou de terceiros com o seu consentimento ou nos termos da lei, é exercido por intermédio de médico, com habilitação própria, se o titular da informação o solicitar*".

Verificamos, assim, que a mediação no acesso à informação de saúde deixou de ser obrigatória em todos os casos. Nos casos em que é impossível conhecer esta vontade e havendo autorização prévia para que um terceiro possa aceder ao processo clínico, a mediação por médico é obrigatória, como determina o nº 4 do artigo 3.º da Lei nº 12/2005 de 26 de janeiro, alterada pela Lei nº 26/2016 de 22 de agosto.

No entanto, importa analisar na perspetiva ética, qual o papel das organizações de saúde e qual o agir dos profissionais de saúde quando lhes for solicitado esse acesso à informação de saúde, pelo seu titular. Para tal, devemos aprofundar um pouco a reflexão acerca da

[17] Idem.
[18] Note-se que o RGPD não prevê este regime, mas é admissível que tal seja mantido, nos termos do artigo 9.º, n.º4.

natureza da informação de saúde e de quais devem ser os cuidados a ter na sua transmissão.

A informação de saúde integra um conjunto de dados relativos à vida da pessoa, nomeadamente no que diz respeito à sua situação de saúde-doença e à sua história clínica. Contém informação codificada pela linguagem dos profissionais de saúde e pode conter muitos registos sobre situações que a ética da saúde tem apelidado de "más notícias".

Estas duas razões – informação que pode ser de difícil entendimento para a pessoa e registos que podem configurar uma notícia nova e má – costumam ser apontadas como causas justificativas para a existência de uma mediação na transmissão da informação de saúde. Ou seja, perante a previsibilidade de incompreensão da informação registada e/ou perante a possibilidade do processo clínico conter informações más que não são conhecidas do seu titular, a transmissão mediada por um profissional de saúde, pode constituir uma forma de atenuar os danos causados pelo acesso a essas informações.

A ser assim, trata-se de um direito para a pessoa e de um dever dos profissionais de saúde, que as organizações de saúde devem respeitar. Ou seja, a transmissão de informação ao próprio, não deve ser entendido como um mero ato administrativo, mas deve configurar-se como uma ação terapêutica, porquanto pretende evitar danos de saúde que podem ser causados pela incerteza ou pela dureza da informação registada. É deste modo que o profissional de saúde assume como dever, chamar a si, a transmissão da informação contida no processo clínico, como que estendendo a sua intervenção terapêutica perante a pessoa que assistiu

O facto desta mediação não ser obrigatória nos termos da lei atual, não deve, contudo, afastar estas obrigações institucionais e estes deveres dos profissionais de saúde. Às organização de saúde compete informar da possibilidade desta mediação e os profissionais de saúde devem manter-se disponíveis para o fazer. Só uma pessoa que tenha plena consciência de que poderá ter acesso à sua informação de saúde de forma mediada por um profissional de saúde, poderá decidir livremente se a dispensa.

3.2. O ACESSO POR TERCEIROS

Em princípio, terceiros não poderão aceder à informação de saúde, salvo os casos previstos no n.º 5 do artigo 6.º da LADA:

- Terceiro com autorização do titular;

- Terceiro com interesse direto, pessoal e legítimo.[19]

[19] *"O interesse é directo quando incide imediatamente e não de uma forma meramente reflexa sobre a esfera de direitos ou interesses legalmente protegidos do recorrente, é pessoal quando lhe diga respeito e não a terceiros e é legítimo quando se conforma com cânones de direito objectivo"* - Parecer da CADA n.º 59/2003

Igualmente, nos termos do RGPD e da LPD vigora o princípio da proibição de acesso, sendo apenas admissível nos casos previstos no artigo 9.º, n.º2, do RGPD, nomeadamente:

- Existindo consentimento explícito para finalidade ou finalidades específicas - alínea a);

- Quando for indispensável ao cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social - alínea b);

- Para proteção de interesses vitais do titular dos dados ou de uma outra pessoa - alínea c);

- Defesa de um direito em processo judicial - alínea f);

- Motivos de interesse público importante ou interesse público no domínio da saúde pública - alíneas g) e i);

- Quando for indispensável ara efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social - alínea h).

3.2.1. O ACESSO POR PROFISSIONAIS DE SAÚDE

O acesso aos dados de saúde por profissionais de saúde merece um tratamento especial por parte da legislação. Sendo tal acesso necessário à prestação dos serviços por parte daqueles profissionais, compreende-se que o mesmo seja facilitado.

Vai neste sentido o acima mencionado artigo 9.º, n.º2, alínea h), do RGPD, tal como o artigo 7.º, n.º4 da LPD, bem como o artigo 5.º, n.º5 da Lei n.º12/2005.[20] Todas as disposições remetem para o acesso aos dados de saúde por parte do *"profissional sujeito à obrigação de sigilo"*.[21] A título de exemplo, refira-se que médicos, enfermeiros e farmacêuticos se encontram obrigados a tal sigilo.

O Código Deontológico dos Médicos consagra o segredo médico como *"condição essencial ao relacionamento médico-doente"*,[22] que se impõe em *"todas as circunstâncias"*.[23] O segredo médico deve incidir particularmente sobre as informações que constem do

[20] *"O processo clínico só pode ser consultado por médico incumbido da realização de prestações de saúde a favor da pessoa a que respeita ou, sob a supervisão daquele, por outro profissional de saúde obrigado a sigilo e na medida do estritamente necessário à realização das mesmas (…)"*.
[21] Artigo 9.º, n.º3, do RGPD.
[22] Artigo 29.º do novo Código Deontológico dos Médicos – anterior artigo 85.º
[23] Artigo 30.º do novo Código Deontológico dos Médicos – anterior artigo 86.º

processo clínico do doente.[24] O médico está, ainda, impedido de enviar doentes para *"entidade não vinculada ao segredo médico"*.[25]

Também o Código Deontológico dos Enfermeiros consagra o dever de sigilo, obrigando os profissionais a *"guardar segredo profissional sobre o que toma conhecimento no exercício da sua profissão"*, bem como como a *"partilhar informação pertinente só com aqueles que estão implicados no plano terapêutico"*.[26]

Por fim, os farmacêuticos são obrigados também ao *"sigilo profissional relativo a todos os factos de que tenham conhecimento no exercício da sua profissão, com exceção das situações previstas na lei"*, dever este que *"subsiste após a cessação da atividade profissional*".[27] Neste sentido, os farmacêuticos devem comportar-se por forma a "*evitar que terceiros se apercebam das informações respeitantes à situação clínica do doente"*, abstendo-se de "*mencionar ou comentar factos que possam violar a privacidade do doente"*.

A este respeito podemos considerar como princípio que oriente a ação dos profissionais de saúde, o da inclusão no plano terapêutico, segundo o qual o acesso aos dados de saúde de uma pessoa só deve ser possível por aqueles que se encontrem implicados no plano terapêutico dessa pessoa, ficando obrigados ao dever de sigilo.

3.2.2. O ACESSO NO ÂMBITO DA INVESTIGAÇÃO CLÍNICA

Outra situação em que a lei prevê o acesso por terceiros a dados de saúde prende-se com a investigação clínica. Neste âmbito, um conjunto de sujeitos podem, mediante a verificação de certos pressupostos, aceder a dados de saúde dos participantes nos estudos clínicos.

A Lei da Investigação Clínica, Lei n.º21/2014, de 16 de abril, consagra a possibilidade de diversos sujeitos terem acesso a dados de saúde. Tais sujeitos poderão ser promotores,[28] investigadores,[29] monitores ou auditores. Todos os sujeitos ficam adstritos ao dever de confidencialidade.[30]

---

[24] Artigo 31.º do novo Código Deontológico dos Médicos – anterior artigo 87.º: *"Os médicos que trabalhem em unidades de saúde estão obrigados, singular e colectivamente, a guardar segredo médico quanto às informações que constem do processo individual do doente"*.

[25] Artigo 30.º do novo Código Deontológico dos Médicos – anterior artigo 86.º

[26] Artigo 85.º

[27] Artigo 85.º do Estatuto da Ordem dos Farmacêuticos, aprovado pela Lei nº 131/2015, de 4 de setembro.

[28] Artigo 9.º, n.º5: *"Os profissionais que acedem aos dados pessoais nos termos dos números anteriores devem garantir a confidencialidade da informação pessoal dos participantes no estudo clínico"*.

[29] Artigo 10.º, alínea c): *"Incumbe ao investigador, designadamente: Garantir a confidencialidade na preparação, realização e conclusão do estudo clínico, bem como das informações respeitantes aos participantes no estudo clínico"*.

[30] Artigo 51.º, n.º1: *"As informações transmitidas no âmbito da presente lei são confidenciais, ficando todos os que delas tenham conhecimento sujeitos a dever de sigilo, sem prejuízo da divulgação das informações necessárias à salvaguarda da saúde pública"*.

Também o Decreto-Lei n.º102/2007, de 2 de abril, relativo aos princípios e diretrizes de boas práticas clínicas no que respeita aos medicamentos experimentais para uso humano, bem como os requisitos especiais aplicáveis às autorizações de fabrico ou importação desses produtos, admite o acesso aos dados de saúde por parte de promotores e investigadores[31] e, ainda, auditores.[32] O diploma dispõe que *"A informação relativa ao ensaio clínico deve ser registada, tratada e arquivada, de modo a permitir a sua notificação, interpretação e verificação,* ***sem prejuízo da confidencialidade dos registos*** *referentes aos participantes nos ensaios"* (negrito nosso), remetendo, ainda, para a LPD.[33]

4. PDS-PLATAFORMA DE DADOS DA SAÚDE

4.1. PROCESSO FÍSICO E PROCESSO DIGITAL

A digitalização do processo clínico comporta desafios à análise da proteção dos dados de saúde. A existência de um processo clínico digital, a par ou em substituição do processo físico, vem ampliar ou redefinir problemas existentes. Tal sucede, nomeadamente, com o controlo sobre os acessos à informação e com a rastreabilidade desses mesmos acessos. Ao mesmo tempo, a referida digitalização apresenta novos problemas, como a facilidade de difusão e replicação da informação, bem como vem permitir que tais operações ocorram, praticamente, sem qualquer custo.

A análise feita acima pode considerar-se extensível ao acesso a informação clínica quer esta conste de processo físico, quer conste de processo digital. Contudo, as particularidades deste último, tornam pertinente uma análise que se prenda aos seus pontos específicos.

No contexto português, o acesso a dados de saúde por meios digitais sofreu um grande acréscimo, qualitativo e quantitativo, com a criação da Plataforma de Dados da Saúde, lançada em 2012.

4.2. A PLATAFORMA DE DADOS DA SAÚDE

A Plataforma de Dados da Saúde (adiante PDS) é uma plataforma informática que permite o registo e a partilha de informação clínica entre o utente, os profissionais de Saúde e as entidades prestadoras de serviços de saúde. A plataforma foi desenvolvida com o objetivo de melhorar a eficiência, eficácia e qualidade dos cuidados prestados e promover o envolvimento dos utentes e sua participação ativa na prestação daqueles cuidados.

[31] Artigo 10.º.
[32] Artigo 19.º, n.º3: *"O processo permanente do ensaio constitui a base para a auditoria a efectuar pelo auditor independente do promotor e para a inspecção a efectuar pelo INFARMED e demais autoridades competentes"*.
[33] Artigo 6.º

A PDS foi desenvolvida pela Comissão para a Informatização Clínica (adiante CIC) e pelos Serviços Partilhados do Ministério da Saúde (adiante SPMS).A CIC havia sido criada pelo Despacho n.º16519/2011, de 6 de dezembro, tendo como competências delinear a orientação estratégica na área da informatização clínica do Serviço Nacional de Saúde. Entre os vários projetos a implementar, encontramos a PDS. Por seu turno, os SPMS foram criados pelo Decreto-Lei n.º19/2010, de 22 de março, tendo como missão a prestação de serviços partilhados, nomeadamente na área das tecnologias de informação e comunicação às entidades com atividade específica na área da saúde.

A PDS, na sua primeira fase, foi autorizada pela Comissão Nacional de Proteção de Dados (adiante CNPD) através da Autorização n.º3742/2012, de 30 de abril.[34] A PDS é constituída por quatro portais:

- O **Portal do Utente**, lançado em maio de 2012, possibilita a consulta do histórico de saúde do utente, pelo próprio e pelos profissionais de saúde, permite o agendamento de consultas e o pedido de prescrição de medicação crónica, bem como a consulta do tempo de espera para intervenções cirúrgicas.

O registo no Portal do Utente possui dois níveis de autenticação: através do número de utente e através de autenticação com o Cartão de Cidadão.

O Portal do utente é composto por duas áreas: a de informação geral, com acesso aberto, e a área autenticada, que necessita de registo.

Mediante a autorização do utente, a sua informação clínica pode ser partilhada com os profissionais de saúde nacionais e estrangeiros.

O utente poderá controlar os acessos aos seus dados, através da consulta do histórico de acessos.

- O **Portal do Profissional**, lançado em junho de 2012, permite aos profissionais de saúde o acesso à informação clínica do doente. O PDS – Portal do Profissional destina-se a ser utilizado, consultado e gerido pelos próprios profissionais de saúde do SNS e, progressivamente, pelos profissionais do setor privado.

Numa outra perspetiva vamos encontrar a PDS Live que constitui uma plataforma de telemedicina que permite ligar dois profissionais de saúde do SNS ou utente e médico em contacto direto, através de chat áudio e vídeo, viabilizando a realização de uma teleconsulta com partilha de imagens e outros documentos.

A PDS Live está disponível a qualquer profissional que aceda ao PDS – Portal Profissional, e que possua uma webcam e microfone.

- O **Portal Internacional** permite a partilha de informações de saúde transfronteiriças, por intermédio do *Smart Open Services for European Patients* (adiante epSOS), cuja participação de Portugal é feita através da PDS. Os profissionais de saúde

[34] https://www.cnpd.pt/bin/decisoes/aut/10_3742_2012.pdf

estrangeiros de um país aderente ao projeto epSOS podem, desta forma, aceder à informação do utente.

O Portal Internacional tem por objetivo disponibilizar serviços transfronteiriços que permitam assegurar cuidados de saúde eficientes e seguros aos cidadãos europeus quando viajam pela Europa[35].

- O **Portal institucional** contém informação anonimizada disponibilizada para estudos estatísticos desenvolvidos por instituições de saúde. Têm acesso ao Portal as organizações centrais, como a Direção Geral da Saúde ou a Administração Central do Sistema de Saúde. Este portal foi alvo de autorização da CNPD através da autorização n.º940/2013, de 5 de fevereiro de 2013.[36]

As características da PDS procuram assegurar que a partilha da informação constitua um método seguro para o efeito. Nomeadamente, através de limitações ao nível do acesso a dados pelos profissionais de saúde sem os poderem alterar ou apagar, bem como através do registo da sua consulta num histórico de acessos. Contudo, há que reconhecer que este sistema apresenta riscos de segurança.

Em primeiro lugar, como qualquer outro sistema informático, a PDS apresenta riscos de utilização abusiva, acessos indevidos ou fugas de dados. Em segundo lugar, a implementação prática da PDS enfrenta alguns desafios à segurança dos dados pessoais. A título de exemplo, a utilização generalizada, pelos profissionais de saúde, de passwords alheias dificulta a eficácia de um sistema de rastreabilidade dos acessos. Por outro lado, tais passwords são utilizadas por quem não tem autorização para aceder à plataforma – veja-se o exemplo dos departamentos de informática e dos farmacêuticos.

B. DAS QUESTÕES ÉTICAS

1. DA IMPORTÂNCIA DOS DADOS DE SAÚDE

Os dados em saúde consubstanciam um recurso valioso em saúde, nomeadamente desempenhando papel fundamental na melhoria da prática médica e da eficiência dos serviços de saúde, bem como permitem gerar conhecimento, impulsando a inovação.[37]

O acesso a dados em saúde capacita os profissionais de saúde a colaborarem no processo terapêutico dos doentes de forma mais eficiente e efetiva no âmbito das suas atribuições e competências técnico-científicas. Na verdade, o acesso à informação, em condições previamente definidas e autorizadas pelo titular dos dados e sem condicionalismos

[35] Diretiva 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, JO 2011 L 88
[36] https://www.cnpd.pt/bin/decisoes/aut/10_940_2013.pdf
[37] Nuffield Council on Bioethics - The Collection, linking and use of data in biomedical research and health care: ethical issues, ch.2

circunstanciais (ex. limitações dos Sistemas de Informação), possibilita, entre outros aspetos, promover o contacto entre os profissionais de saúde nos casos em que seja necessário complementar informação para a decisão ou validação clínica e retirar pressão sobre os cuidados de saúde, em particular secundários (Centros de Exame, p. ex.) e terciários (Hospitais e Cuidados Continuados, p. ex.).

Por outro lado, os sistemas de tratamento automatizado de dados (registos eletrónicos) do cidadão relativos ao estado de saúde que revelem informações sobre a sua saúde física ou mental no passado e no presente – como por exemplo os dados de registos médicos com informações como diagnósticos, resultados de exames e quaisquer intervenções ou tratamentos realizados – possibilitam uma intervenção no âmbito da saúde e da segurança do cidadão e proteção da saúde pública através da partilha consentida com os profissionais de saúde que, pela natureza das suas funções, desempenham atividades de cariz assistencial.

Os dados em saúde – historial, diagnósticos, investigação e tratamentos – no seu formato digital aumentam o acesso a cuidados de saúde através da partilha de informação que assegura uma continuidade na transição entre cuidados e um suporte mais robusto e integrado no processo de decisão clínica, promovendo a qualidade dos cuidados e diminuindo os custos associados.

O valor dos dados em saúde, que depende da possibilidade em serem acedidos e da sua partilha, espelha-se no seu valor ético. De facto, a partilha de dados de saúde, que respeite um conjunto de princípios, nomeadamente transparência, integridade, clareza, segurança e respeito pela privacidade poderá resultar em benefícios para a comunidade e por isso deverá ser defendido o seu valor ético.[38]

2. DO VALOR DA PRIVACIDADE

Ao mesmo tempo que se analisa o valor dos dados em saúde, é igualmente vital avaliar o **valor da privacidade**, que é fundamental para os indivíduos e grupos no estabelecimento e manutenção da sua identidade e relação com os outros.[39] Apesar da dificuldade de encontrar uma definição de privacidade, tal não coloca em causa o valor desta.[40]

Não obstantes a lei atribui ao titular dos dados um conjunto de direitos - como o direito de acesso, retificação e eliminação, em algumas circunstâncias, a lei concede também a terceiros o direito de acesso. Neste caso, o interesse do terceiro protegido deve ser medido em relação aos interesses do titular dos dados. No âmbito dos sistemas de tratamento automatizado de dados, os desafios técnicos que se impõem são muito relevantes. Na

[38] Health Parliament Portugal - Recomendações para o futuro da Saúde, Ética em Saúde.

[39] Nuffield Council on Bioethics - The Collection, linking and use of data in biomedical research and health care: ethical issues, ch.3.1. (Proposition 9).

[40] 'The lack of a word translatable as "privacy" is entirely plausible; the absence of concern for it is not' - James B. Rule, Privacy in Peril (Oxford University Press, 2007), 3.

verdade, o confronto da privacidade com sistemas de tratamento automatizado de dados, como os referidos acima utilizados no tratamento de dados em saúde, traz desafios próprios, atendendo, nomeadamente às vicissitudes daqueles sistemas - como a capacidade de tratamento, a perenidade dos dados e a facilidade da sua difusão. Tal significa, por exemplo, que, perante tais sistemas, se torna materialmente impossível controlar o fluxo de informação.[41] Ou seja, torna-se impossível ao titular dos dados pessoais manter o controlo sobre os dados pessoais submetidos àquele tratamento.

Sucede que, o controlo do fluxo de informação é fundamental para a proteção da privacidade.[42] Na verdade, pode argumentar-se que, desde que a disseminação de informações pessoais respeite as expectativas do seu titular, a sua privacidade será respeitada.[43] Só ao ser capaz de decidir que informação partilhar, com quem e quando, o indivíduo verá a sua privacidade protegida.[44]

Esta situação deverá conduzir à necessidade da afirmação ética da existência da liberdade do indivíduo face às tecnologias de informação.[45] A privacidade deve ser afirmada como um bem a proteger que excede a mera composição física e moral do indivíduo. Nos direitos atribuídos pela lei, em particular através do artigo 35.º da Constituição da República Portuguesa, encontra-se a *autodeterminação informacional.*[46] Este direito atribui ao titular dos dados o controlo sobre os seus dados pessoais, podendo definir quais informações estarão disponíveis para quem e em que momento.[47] Esta abordagem permite que o titular seja considerado como sujeito de direito e não meramente um objeto da informação em causa.[48]

[41] Von Hannover v. Alemanha (Tribunal Europeu dos Direitos do Homem (3.ª Secção), 2004).

[42] Boyd, Danah. «Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence». Convergence: The International Journal of Research into New Media Technologies 14, n. 1 (2008): 13–20, p.18

[43] Nissenbaum, Helen. Privacy in context: Technology, policy, and the integrity of social life. Stanford Law & Politics, 2010, pp.159, 186.

[44] 'Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. (…) [P]rivacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve' - Westin, Alan F. Privacy and Freedom. Atheneum, 1967, p.7.

[45] Vittorio Frosini and Jorge Guerrero R, Informática Y Derecho, 1988 *Apud* Segado, Francisco Fernández. «El régimen jurídico del tratamiento autorizado de los datos de carácter personal en España». Derecho PUCP, n. 51 (2013): 7–48, p.9.

[46] Castro, Catarina Sarmento. Direito da Informática: Privacidade e Dados Pessoais. Almedina, p.33.

[47] Paulo Cardoso Correia da Mota Pinto, 'A Protecção Da Vida Privada E a Constituição', Boletim Da Faculdade de Direito Da Universidade de Coimbra LXXVI (2000): 159.
Ettore Giannantonio et al., La Tutela Dei Dati Personali: Commentario Alla L. 675-1996, vol. 5 (Cedam, 1999), 16. Apud. Castro, Direito da Informática: Privacidade e Dados Pessoais, 27–28.

[48] Canotilho e Moreira, Constituição da República Portuguesa Anotada, I: Comentário ao Artigo 35. parágrafo II.

Enfatizar o papel do controlo sobre a informação como forma de proteção da privacidade confere a este a importância que lhe será devida, colocando a autodeterminação informacional como central na proteção da *projeção vital* do indivíduo.[49]

O direito à privacidade pode ser entendido como um meio para a sociedade, como um todo, salvaguardar a individualidade de cada sujeito. Garantir que cada pessoa possa controlar o fluxo dos seus dados pessoais poderá promover a sua integração na sua sociedade e a interação social. Neste sentido, o direito à privacidade não deve ser visto simplesmente como um direito individual; mas como um verdadeiro direito fundamental.[50]

3. DAS CONSIDERAÇÕES ÉTICAS

O CNECV refletiu, por diversas vezes, sobre o acesso à informação de saúde. São exemplos os seguintes Pareceres e respetivos Relatórios:

- Parecer 37/CNECV/01 acerca do Projecto de Lei Nº 455/VIII "Informação Genética Pessoal", Proposto pelos Deputados do Bloco de Esquerda;
- Parecer 43/CNECV/04 sobre Projecto De Lei N.º 28/IX - Informação Genética Pessoal e Informação de Saúde;
- Parecer 52/CNECV/07 sobre Regime Jurídico da Base de Dados de Perfis de A.D.N.;
- Parecer 57/CNECV/09 sobre o Projecto De Lei N.º 788/X – "Direitos dos Doentes à Informação e ao Consentimento Informado";
- Parecer 60/CNECV/2011 Sobre Informação de Saúde e Registos Informáticos de Saúde
- Parecer 68/CNECV/2012 sobre Projeto de Decreto-Lei que Regulamenta a Lei N.º12/2005, de 26 de Janeiro, no que Respeita A Informação Genética, Bases De Dados Genéticos E Testes Genéticos.

Os temas analisados por este Conselho foram de teor diverso, destacando-se a informação genética. Relativamente ao acesso aos dados de saúde, há a salientar o Parecer 60/CNECV/2011, cujo objeto é parcialmente coincidente com o ora analisado. Sem se pretender repetir o que ali consta, remete-se para aquele Parecer, sem prejuízo de se passar a complementar a análise efetuada. É de referir, em particular, a circunstância de, após a emissão do Parecer 60/CNECV/2011, o contexto ter evoluído consideravelmente, a dois níveis. Por um lado, há a mencionar a evolução tecnológica. Em termos globais, o tema da *big data* tornou-se premente desde 2011. Em termos nacionais, foi desenvolvida a

[49] Orlando de Carvalho, 'Por Uma Teoria Da Pessoa Humana (1999)', in Teoria Geral Do Direito Civil, 3.a ed. (Coimbra: Coimbra Editora, 2012).
[50] Ana Isabel Herrán Ortiz, El Derecho a La Protección de Datos Personales En La Sociedad de La Información (Bilbao, Universidad de Deusto, Cuadernos Deusto de Derechos Humanos, 2002), 13–14.

Plataforma de Dados da Saúde.[51] Por outro lado, ao nível legislativo, o enquadramento legal sofreu diversas alterações, tanto internamente como em termos comunitários.

Tendo, assim, presente o Parecer 60/CNECV/2011, remete-se para as vantagens e riscos ali elencados, que se mantêm atuais, mas que deverão ser complementados outras, nomeadamente, quanto as vantagens: Satisfação dos profissionais clínicos[52] e a capacidade de integração e interoperabilidade, inovação e competitividade, partilha de recursos[53]; e quanto aos riscos: associados ao *Big Data* e ao desenvolvimento da PDS, a medicina personalizada, *Mobile informatics*, apps e aparelhos de registos de dados pessoais,[54] bem como a Impossibilidade técnica de anonimização irreversível.

Em suma, a informação de saúde, que tem sempre origem num indivíduo que merece tutela, quando bem utilizada permite decisões *mais esclarecidas e adequadas.*[55] O equilíbrio entre aquela tutela, face aos riscos identificados, e as vantagens verificadas deve ser objeto de reflexão ética.[56]

Tal reflexão encontra como vetores fundamentais os seguintes:

- A segurança e confidencialidade dos dados de saúde
- O fundamento para o tratamento dos dados pessoais.

3.1. DA SEGURANÇA E CONFIDENCIALIDADE DOS DADOS DE SAÚDE

Parte dos riscos relacionados com o tratamento informático dos dados em saúde relaciona-se com a segurança e confidencialidade. Estes riscos poderão verificar-se por diversas causas.

Em primeiro lugar, os riscos prendem-se com as falhas de segurança, caso em que se mostra fundamental reconhecer que os sistemas informáticos são falíveis.[57] Assim, poderá

[51] O Parecer 60/CNECV/2011 não ignora esta evolução que se anunciava, referindo *"a criação do 'Registo de Saúde Electrónico'"*, apelando a uma *"especial atenção no sentido de se identificarem as questões de natureza ética relevantes à sua criação e funcionamento"* - cfr. ponto 15 do Parecer.

[52] Karimi F., Poo D.C., Tan Y.M. Clinical information systems end user satisfaction: the expectations and needs congruencies effects. J Biomed Inform. 2015 Feb;53:342-54

[53] Audição do Professor Doutor Henrique Martins.

[54] Audições do Professor Doutor Luís Antunes e do Professor Doutor Henrique Martins.

[55] Parecer 60/CNECV/2011 - considerando C.

[56] "As novas tecnologias de informatização da saúde podem, sem dúvida, aumentar a segurança e a privacidade no armazenamento e transmissão dos dados pessoais. (...) Embora sendo consensual que a garantia de privacidade total das informações e dados pessoais em saúde é impossível, deverão existir normas e guias de conduta muito claros que permitam a confiança dos cidadãos na forma como é garantida a confidencialidade e a privacidade dos seus dados de saúde" - Bioética e Políticas Públicas | 2014 - Uma Proposta De Um Modelo De Deliberação Ética Para A Saúde Pública. Ana Sofia Carvalho, p.32

[57] Ainda que possam oferecer potencialmente maior segurança do que os registos em papel cfr. Parecer 60/CNECV/2011, p.4: *"Segurança da informação, em muitos aspectos maior do que a dos registos em papel, incluindo quanto à sua perda, desde que tomadas medidas de segurança disponíveis e actualiza-*

haver fuga de informações, com causas acidentais, como envio erróneo de dados, ou com origem deliberada, como com acessos indevidos ao sistema.[58]

Em segundo lugar, os sistemas informáticos estão sujeitos à utilização indevida por quem tem acesso legítimo ao sistema. A título de exemplo, tal sucede devido à prática da utilização comum de credenciais de acesso, por parte de diferentes profissionais de saúde. Neste particular seria fundamental fomentar uma *cultura institucional no âmbito da proteção dos dados de saúde* pelos profissionais da saúde.[59] Depois, ainda que existam ferramentas tecnológicas com vista a evitar que tais acessos ocorram, muitas vezes elas não são efetivamente utilizadas. Nomeadamente, devido à inatividade das ferramentas que permitem a rastreabilidade[60] e à falta de controlo de acessos por entidades externas.[61] É recomendável que as ferramentas disponíveis sejam utilizadas, para que seja possível avaliar as medidas tecnológicas adicionais que serão necessárias. Seria, ainda, conveniente que o próprio paciente pudesse ter conhecimento de quem acedeu aos seus dados clínicos.

A este propósito, há que questionar se deverá ser alargado o universo de quem pode aceder aos sistemas de acesso aos dados de saúde, em particular à PDS.[62] Tal alargamento deverá ser precedido de uma análise do custo-benefício. Levantam-se, desde já, reservas éticas quanto à integração indiscriminada de profissionais e não profissionais nos acessos à referida Plataforma.

Em terceiro lugar, existem riscos associados à própria conceção dos sistemas informáticos que procedem ao tratamento dos dados de saúde. Encontram-se características na base destes sistemas que dificultam a proteção dos dados independentemente das soluções tecnológicas que lhe estejam subjacentes. Desde logo, é merecedor de censura ética a crescente *fusão entre a informação administrativa e os dados clínicos,* o que implica uma crescente dificuldade em destrinçar dados em saúde dos restantes dados pessoais.[63] Esta realidade, resulta numa maior dificuldade de proteção dos dados em saúde face aos demais. Depois, há sistemas que, por definição, fornecem acesso a dados em saúde, cuja transparência e necessidade há que questionar. Refira-se, em concreto, os dados retidos por empresas de prescrição médica.

---

das".

[58] *"Nem todos os inscritos na PDS saberão que estão inscritos (...) Os dados pedidos na inscrição são tão básicos que qualquer pessoa pode registar outros"* - audição do Professor Doutor Luís Filipe Antunes.

[59] O Dr. Rui Vasconcelos Guimarães mencionou a ausência de uma cultura institucional no âmbito da proteção dos dados de saúde.

[60] Na audição perante o CNECV, o Professor Doutor Luís Filipe Antunes referiu que a rastreabilidade dos acesso é possível através dos *logs,* que "*não estão ativos"*.

[61] O Dr. Rui Vasconcelos Guimarães exemplificou com as empresas de suporte informático.

[62] O Professor Doutor Henrique Martins mencionou que não deveriam ser só médicos e enfermeiros a aceder à PDS, mencionando que o mesmo deveria acontecer com outras categorias de profissionais e não profissionais, exemplificando com farmacêuticos, técnicos de fisioterapia e estudantes de Medicina.

[63] O Professor Doutor Henrique Martins referiu, na audição perante o CNECV, que existe cada vez mais *"a fusão entre a informação administrativa e os dados clínicos"*, exemplificando com o sistema do cheque-dentista, através do qual é possível aceder à informação de que o paciente é portador da patologia VIH-SIDA.

Ainda relativamente à conceção dos sistemas, será de relevo discutir o papel desempenhado pela SPMS no âmbito da gestão dos dados em saúde, atendendo à sua natureza. Na verdade, esta entidade, ainda que de natureza pública, assume-se como uma empresa fornecedora de serviços aos hospitais. Há que refletir, assim, se ela será a mais habilitada para controlar a *cloud* onde estão armazenados os dados em saúde.[64] Neste ponto, poderá ser de avaliar a pertinência da gestão da PDS passar a ser efetuada por entidade exclusivamente administrativa.

Neste âmbito, deverá, ainda, ser fomentado o princípio da *privacy by design,* imbuindo os sistemas de informação de uma arquitetura que vise a proteção dos dados pessoais, em particular no controlo sobre o fluxo de dados em saúde, desde a sua conceção.

3.2. DO FUNDAMENTO E FINALIDADE PARA O TRATAMENTO DOS DADOS PESSOAIS

A validade ética do tratamento dos dados em saúde depende da justificação que lhe esteja subjacente. Esta justificação encontra reflexo jurídico, por um lado, na necessidade da verificação de um fundamento para o tratamento dos dados pessoais,[65] e, por outro, na necessidade da determinação da finalidade do tratamento.[66]

Apresentam-se como fundamentos eticamente válidos para o tratamento de dados em saúde, nomeadamente, a existência do consentimento do titular dos dados, a prossecução do interesse público e os fins de investigação científica.

Em primeiro lugar, quando o fundamento para o tratamento dos dados em saúde se prenda unicamente com o consentimento do titular, este deverá ser informado, explícito e consistir em ato positivo inequívoco.[67] A exigência quanto ao consentimento deve ser reforçada no caso específico dos dados em saúde.[68] É, assim, desejável que, quando o tratamento de dados em saúde se baseie no consentimento, este tenha sido prestado de forma explícita e não tenha consistido num consentimento presumido. Destarte, sempre que possível e não seja aplicável outro fundamento, o tratamento dos dados em saúde, nomeadamente no âmbito da PDS, deve ser precedido da obtenção do consentimento explícito do titular, baseando-se este numa opção de *opt-in,* ainda que tal acarrete *maiores custos e esforço no contacto com os pacientes.*[69] [70]

[64] Audição do Professor Doutor Luís Filipe Antunes, que questionou se uma empresa fornecedora dos hospitais, como é a SPMS, será a mais habilitada para controlar a *cloud* onde estão armazenados os dados de saúde.
[65] Nos termos do artigo 5.º, n.º1, alínea a), e artigo 6.º, ambos do RGPD.
[66] Nos termos do artigo 5.º, n.º1, alínea b) do RGPD
[67] Artigo 4.º, 11) do RGPD
[68] Neste sentido, o artigo 9.º, n.º2, alínea a), do RGPD refere *"consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidade específicas".*
[69] Shen H., Ma J., Privacy Challenges of Genomic Big Data., Adv Exp Med Biol. 2017;1028:139-148.

Nos casos em que o fundamento para o tratamento de dados seja o consentimento do titular, merece reflexão a possibilidade do uso secundário dos dados pessoais,[71] o que é particularmente limitada no caso dos dados em saúde, vista a sua natureza como dados sensíveis. Este uso secundário coloca em causa as expectativas do titular dos dados, bem como cria incerteza quanto ao destino dos dados. Ao mesmo tempo, a utilização de dados pessoais para fins diferentes daqueles para que foram recolhidos poderá dar azo à descontextualização e erros de interpretação. Por outro lado, há que reconhecer que tal uso pode permitir a prossecução de novas finalidades desejáveis, nomeadamente ao nível da investigação científica.[72] Neste sentido, quando vise a prossecução de finalidades desejáveis, não seja possível ou exija um esforço desproporcionado a obtenção de novo consentimento e sejam salvaguardados os direitos dos titulares, será de admitir o uso secundário dos dados.

Em segundo lugar, o tratamento dos dados em saúde poderá justificar-se por motivos de interesse público no domínio da saúde pública, nomeadamente para *"assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos"*.[73] Este fundamento para o tratamento dos dados em saúde poderá justificar, por exemplo, a prescindência da obtenção de consentimentos reiterados do paciente, após o consentimento inicial; bem como a comunicação dos dados entre profissionais de saúde, desde que vinculados pelo sigilo profissional.

Em terceiro lugar, o tratamento dos dados pode ter por base o fundamento relativo aos fins de investigação científica. Considerando a utilidade individual e social desta atividade, justifica-se que ela seja fundamento suficiente para o tratamento de dados em saúde, podendo prescindir-se de consentimento do titular para o efeito. Contudo, neste caso, será fundamental proporcionar garantias para os titulares dos dados em saúde, nomeadamente quanto à utilização exclusivamente da quantidade mínima essencial de dados e, sempre que possível, da sua separação da identidade do titular.[74] É fundamental que só se prescinda do consentimento do titular dos dados em saúde para o seu tratamento quando tal não seja um esforço desproporcional face aos ganhos potenciais da investigação em causa.[75]

---

[70] O Professor Doutor Henrique Martins defendeu a solução do *opt-out* relativamente à PDS, argumentando que a solução do *opt-in* traria maiores custos e esforço no contacto com os pacientes.

[71] O uso secundário dos dados consiste na utilização destes para finalidades diferentes daquelas para que inicialmente foram recolhidos.

[72] D. J. Solove, "A taxonomy of privacy" *in* University of Pennsylvania Law Review, vol.154, 477 - pp.521-522.

[73] Artigo 9.º, n.º2, alínea i) do RGPD.

[74] Conforme prevê o artigo 89.º, n.º1, do RGPD.

[75] European Patients Forum, "The new EU Regulation on the protection of personal data: what does it mean for patients?", p.17

Finalmente, refira-se ainda que, no sentido de promover o controlo sobre os dados em saúde, mostra-se importante que o titular destes possa ver concretizado o seu pedido relativo à eliminação, desde que tal não colida com interesse superior, nomeadamente não coloque em causa a saúde ou o interesse público.[76] Reconhece-se que tal pedido poderá comportar desafios, nomeadamente de ordem técnica. Contudo, estes não deverão sobrepor-se àquela que seja a legítima vontade do titular dos dados. Deverão, assim, sempre que possível, os sistemas de processamento de dados, nomeadamente a PDS, estar dotados de meios para a eliminação dos dados em saúde.[77]•

Audições.

No âmbito da reflexão sobre o tema do acesso aos dados de saúde foram ouvidos, por ordem de intervenção:

Dr. Rui de Vasconcellos Guimarães, Responsável pelo Acesso à Informação (RAI) do Centro Hospitalar de São João, EPE (CHSJ).

Prof. Doutor Luís Antunes, Diretor do Centro de Competências em Cibersegurança e Privacidade da Universidade do Porto (FCUP);

Prof. Doutor Henrique Martins, Presidente do Conselho de Administração da SPMS – Serviços Partilhados do Ministério da Saúde, EPE;

Prof. Doutor Alexandre Quintanilha, Deputado à Assembleia da República, Presidente da Comissão de Ética para a Investigação Clínica (CEIC).

[76] Naquilo que a lei prevê, no artigo 17.º do RGPD, como o direito ao esquecimento.

[77] Em audição, o Professor Doutor Henrique Martins referiu que a SPMS não tem capacidade para apagar todos os dados, mencionando que tal traz riscos para o próprio paciente.