



UNIVERSIDADE CATÓLICA PORTUGUESA

**O Espaço Europeu de  
Dados de Saúde**  
**Uma Análise à sua Proposta de Regulamento**

Nádia Soraia Keta Figueiredo

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2024





UNIVERSIDADE CATÓLICA PORTUGUESA

**O Espaço Europeu de  
Dados de Saúde**  
**Uma Análise à sua Proposta de Regulamento**

Nádia Soraia Keta Figueiredo

Orientadora: Professora Doutora Filipa Urbano  
Calvão

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2024

*A felicidade e a saúde são incompatíveis com a ociosidade.*

*- Aristóteles*

## *Agradecimentos*

Embora a elaboração de uma dissertação seja um processo exaustivo, o apoio constante daqueles que me são mais próximos fez com que conseguisse terminar esta etapa do meu percurso académico de cabeça erguida.

Assim, agradeço em especial à minha família e aos amigos por todo o amor e confiança depositados em mim.

À Universidade Católica Portuguesa do Porto e aos docentes, por toda a formação e experiências académicas.

À minha orientadora, a Professora Dr<sup>a</sup>. Filipa Urbano Calvão, por me ter auxiliado na concretização deste estudo.



## **RESUMO**

Nos últimos anos temos assistido a uma crescente necessidade de regular o registo eletrónico de dados de saúde e a partilha destes dados entre os vários Estados-Membros, de forma a tornar o acesso dos titulares e dos profissionais de saúde a estes dados mais célere e eficaz.

O Parlamento Europeu e o Conselho vieram apresentar uma Proposta de Regulamento que tem em vista a criação de um Espaço Europeu de Dados de Saúde.

Nesta senda, propomo-nos a analisar a Proposta de Regulamento, identificando e criticando os principais problemas que carecem de solução, comparando o proposto com o quadro jurídico vigente no RGPD.

**Palavras-chave:** Espaço Europeu de Dados de Saúde, Proteção de Dados, Utilização Primária; RGPD; Tratamento de Dados Pessoais Sensíveis.



## ***ABSTRACT***

*In recent years we have seen a growing need to regulate the electronic registration of health data and the sharing of this data between the various Member States, in order to make access to this data faster and more effective for data subjects and health professionals.*

*The European Parliament and the Council have presented a Proposal for a Regulation aimed at creating a European Health Data Space.*

*With this in mind, we propose to analyze the Proposal for a Regulation, identifying and criticizing the main problems that need to be resolved, comparing the proposal with the current legal framework of the GDPR.*

***Keywords:*** *European Health Data Space, Data Protection, Primary Use; GDPR; Processing of Sensitive Personal Data.*



# ÍNDICE

<b>Agradecimentos</b> .....	5
<b>RESUMO</b> .....	7
<b>ABSTRACT</b> .....	9
<b>ADVERTÊNCIA</b> .....	13
<b>LISTA DE SIGLAS, ACRÓNIMOS E ABREVIATURAS</b> .....	14
<b>1. INTRODUÇÃO</b> .....	15
<b>2. ENQUADRAMENTO GERAL</b> .....	17
2.1.    A Proposta de Regulamento sobre a Criação de um Espaço Europeu de Dados de Saúde: Motivações e Objetivos.....	17
2.2.    Principais Obstáculos à Criação do EEDS: Uma Visão Geral..	20
2.2.1.    Os Princípios Fundamentais do Tratamento de Dados, em especial: a Licitude.....	24
2.2.2.    As Principais Problemáticas a Regular na Proposta .....	28
<b>3. ANÁLISE DO REGIME PROPOSTO</b> .....	32
3.1.    Disposições Gerais .....	33
3.2.    A Utilização Primária dos Dados de Saúde .....	37
3.3.    Os Sistemas de RSE .....	46
3.4.    Disposições Finais.....	47
<b>4. CONCLUSÃO</b> .....	49
<b>BIBLIOGRAFIA CONSULTADA</b> .....	50



## ADVERTÊNCIA

A nossa investigação para a elaboração desta dissertação terminou a **24 de fevereiro de 2024**, data em que a proposta foi consultada pela última vez. Neste sentido alertamos que não foram tidas em conta quaisquer possíveis alterações à proposta após esta data, nem a futura aprovação e publicação do regime criado.

## LISTA DE SIGLAS, ACRÓNIMOS E ABREVIATURAS

Ac.	Acórdão
Acs.	Acórdãos
Al.	Alínea
Art.	Artigo
Arts	Artigos
CDFUE	Carta dos Direitos Fundamentais da União Europeia
CNPD	Comissão Nacional da Proteção de Dados
Cfr	Conforme
CRP	Constituição da República Portuguesa
Consult.	Consultado
EEDS	Espaço Europeu de Dados de Saúde
n.º	número
op. cit.	<i>opus citatum (da obra citada)</i>
Pág.	Página
Págs.	Páginas
Proc.	Processo
RSE	Registo de Saúde Eletrónico
RGPD	Regulamento Geral de Proteção de Dados
Segs.	Seguintes
TFUE	Tratado sobre o Funcionamento da União Europeia
UE	União Europeia
v.g.	<i>verbi gratia (por exemplo)</i>

# 1. INTRODUÇÃO

Os sistemas de tratamento de dados estão ao serviço do Homem, devendo respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência<sup>1</sup>, e à luz do artigo 35.º da CRP, todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

De acordo com a Recomendação (UE) 2019/243<sup>2</sup>, “[H]á mais de dois milhões de casos anuais registados em que um cidadão residente num Estado-Membro procurou cuidados de saúde noutra Estado-Membro”. Face a isto podemos afirmar que a União Europeia (UE) se tem visto na necessidade de colmatar as dificuldades derivadas da prestação de serviços de saúde entre os diferentes Estados-Membros, sendo um dos principais obstáculos a proteção e o tratamento de dados de saúde. Ao abrigo do programa “Década Digital da Europa”, foram estabelecidas metas digitais para 2030 a alcançar na UE, estando incluída nestas metas, a digitalização dos serviços públicos, e relativamente à saúde, a meta de que todos os cidadãos venham a ter acesso ao seu processo clínico em linha.

Na Recomendação (UE) 2019/243, foi ainda referenciada “a necessidade de os Estados-Membros tornarem os seus sistemas de saúde eletrónicos mais interoperáveis, a fim de conferir aos cidadãos um maior controlo sobre os seus dados de saúde”<sup>3</sup>.

Como podemos ver através destas contribuições, já há algum tempo que a UE tem contemplado colocar em ação um mecanismo de interoperabilidade e partilha de dados de saúde entre os diferentes Estados-Membros, estando cada vez mais perto de o alcançar.

Em 2022, foi apresentada uma Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao Espaço Europeu de Dados de Saúde, com o objetivo de concretizar esta ideologia, e finalmente tomar os passos necessários à evolução e criação de um “sistema europeu de saúde”<sup>4</sup>.

---

<sup>1</sup> Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, Considerando (2).

<sup>2</sup> Recomendação (UE) 2019/243 da Comissão de 6 de fevereiro de 2019 relativa a um formato europeu de intercâmbio de registos de saúde eletrónicos.

<sup>3</sup> Ibidem, Considerando (6).

<sup>4</sup> Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao Espaço Europeu de Dados

Ao longo da nossa investigação propomo-nos a analisar a proposta de regulamento, nomeadamente no que diz respeito à utilização primária de dados de saúde, e fazer a ponte entre os diplomas de proteção de dados já existentes, como o RGPD, assim como outra legislação relevante. Pretendemos perceber de que forma poderão os titulares ter acesso e controlo sobre os seus dados, como será regulado o acesso aos dados por parte dos profissionais de saúde, quais os mecanismos de controlo e de responsabilidade aplicados, e acima de tudo comparar a proposta com os meios de tutela já em curso, verificando de que forma é que estes se contradizem ou complementam.

---

de Saúde, COM/2022/197 final, consult. em 24/Fev/2024,  
<https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52022PC0197> .

## 2. ENQUADRAMENTO GERAL

### 2.1. A Proposta de Regulamento sobre a Criação de um Espaço Europeu de Dados de Saúde: Motivações e Objetivos

No dia 3 de maio de 2022 foi publicada uma Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao Espaço Europeu de Dados de Saúde, cujo objetivo seria regular, precisamente, a criação de um Espaço Europeu de Dados de Saúde (EEDS). Com a evolução da tecnologia, nomeadamente no campo da saúde, tornou-se prática comum nos Estados-Membros fazer um registo eletrónico de dados dos pacientes, o que levanta determinadas questões e problemas que carecem de solução, especialmente ao nível do tratamento de dados pessoais, desde logo a forma como as pessoas singulares podem ter acesso aos seus dados de saúde, quais as entidades que estão autorizadas a aceder a esses dados e para que fins.

A ideia de um sistema que regule estes aspetos não é propriamente inovadora dado que os próprios Estados-Membros já o fazem internamente, mas gerir um sistema deste tipo a nível da União Europeia (UE) pode tornar-se uma tarefa extremamente exaustiva tendo em conta que estamos a tratar de dados pessoais, que, de acordo com o artigo 9.º do Regulamento Geral da Proteção de Dados (RGPD), inserem-se numa categoria especial de dados, correspondendo a dados pessoais mais sensíveis.

Na verdade, a conceção de um espaço europeu da saúde já tem sido idealizada ao longo dos anos, como se pode ver através da Decisão 1786/2002/CE do Parlamento Europeu e do Conselho, de 23 de setembro de 2002<sup>5</sup>, onde, no seu artigo 5.º, já faz referência a uma cooperação entre os Estados-Membros e mecanismos de interoperabilidade de dados de forma a combater ameaças à saúde pública. Porém tal tem sido difícil de concretizar dado que um sistema como este deve assegurar o cumprimento de todas as disposições legais pertinentes em matéria de proteção dos dados pessoais, e ainda a introdução de mecanismos que assegurem a confidencialidade e a segurança desses dados.

Uma grande impulsionadora da criação desta proposta de regulamento foi a crise criada pela pandemia COVID-19. Como sabemos os governos mundiais não estavam preparados para receber uma ameaça como esta pelo que foi necessário “tapar buracos”

---

<sup>5</sup> Decisão n.º 1786/2002/CE do Parlamento Europeu e do Conselho, de 23 de setembro de 2002, que aprova um programa de ação comunitária no domínio da saúde pública (2003-2008).

e criar com caráter urgente, legislação e regulamentos que pudessem ajudar a apaziguar as inseguranças geradas pela doença, assim como combatê-la eficazmente. Deste modo, conseguimos entender como um sistema a nível europeu de registo de dados de saúde poderia ter sido útil para facilitar o acesso, vigilância e acompanhamento dos doentes, servindo também como um mecanismo de contenção.

Uma destas medidas remediadoras foi a adoção do sistema de gestão clínica dos doentes, criado pela Decisão de Execução (UE) 2019/1269 da Comissão<sup>6</sup>, que veio de certo modo permitir e regular a transferência de dados de saúde dentro da União Europeia, relativa a doentes “que se deslocassem entre prestadores de cuidados de saúde e entre Estados-Membros durante o pico da pandemia”<sup>7</sup>. Porém, um mecanismo como aquele que se pretende que seja implementado não se poderá deixar ficar por estas medidas pelo que haverá outros aspetos a ter em consideração e que pretendemos explorar ao longo da nossa análise.

Antes de mais cabe-nos perceber quais as motivações que levaram a que a UE finalmente tomasse este passo e apresentasse uma proposta. Claro que a pandemia e a necessidade de contenção de doenças foram um destes motivos, mas não se basta por aqui.

Creemos que a internacionalização da sociedade foi também uma destas motivações, especialmente ao nível europeu. Podemos verificar que o número de pessoas que se deslocam para o estrangeiro para visitar, estudar, trabalhar ou viver tem crescido de forma exponencial, e nesse sentido mostra-se necessário conseguir garantir que independentemente do Estado-Membro em que se encontrem, seja o seu país de origem ou outro, os vários sistemas de saúde estão preparados para prestar os melhores serviços possíveis.

Ao abrigo do artigo 15.º do RGPD, todos os titulares de dados têm um direito de acesso aos seus dados, porém o Parlamento Europeu entende que a consagração deste direito a nível dos dados de saúde carece de uma proteção maior, sendo necessário tornar o acesso aos dados pelos seus titulares mais célere. As obstruções criadas a este acesso podem ter consequências gravíssimas especialmente em situações de urgência

---

<sup>6</sup> Decisão de Execução (UE) 2019/1269 da Comissão, de 26 de julho de 2019, que altera a Decisão de Execução 2014/287/UE, que define critérios para a criação e avaliação de redes europeias de referência e dos seus membros, bem como para facilitar o intercâmbio de informações e experiências sobre a criação e avaliação das referidas redes (JO L 200 de 29.7.2019, p. 35).

<sup>7</sup> Proposta de Regulamento Do Parlamento Europeu e do Conselho relativo ao Espaço Europeu de Dados de Saúde, de 3 de maio de 2022, Considerando (2).

decorrentes do seu estado de saúde, pelo que a criação de um mecanismo harmonizador dos sistemas de Registo de Saúde Eletrónico (RSE) no espaço europeu ajudaria a evitar situações em que um tratamento médico ficaria comprometido pela falta de informação.

Não podemos deixar de trazer a vantagem associada à redução dos encargos administrativos para os profissionais e instituições de saúde. Tornar os dados interoperáveis entre os vários prestadores de serviços, evitando que os tenham de introduzir manualmente nos seus sistemas eletrónicos, é uma forma de poupar recursos e evitar atos inúteis como a recolha de informação repetida. Sobre este ponto chamamos inclusive a atenção para o considerando 5 da Recomendação (UE) 2019/243 da Comissão de 6 de fevereiro de 2019, que nos diz,

*[U]ma melhor gestão das doenças crónicas na comunidade, a par da redução da duplicação das ações de cuidados de saúde (como os exames), não só tornará os sistemas mais sustentáveis como também melhorará a qualidade de vida global, a qualidade dos cuidados de saúde prestados aos cidadãos e reduzirá os custos associados aos cuidados de saúde para os indivíduos e os agregados familiares.*

No entanto, será necessário haver um alto nível de cooperação entre os vários institutos hospitalares e entre fronteiras, visto que qualquer prestador de serviços deverá poder confiar nos dados presentes no sistema independentemente da entidade que os tenha inserido (leia-se, entre as entidades legitimadas para esse efeito), ou do Estado-Membro de onde provenha a informação. Significa isto que deverá existir um nível de controlo, assim como critérios rigorosos de seleção no que toca à informação introduzida e ao tratamento de dados que seja uniforme para todos os Estados.

Com o regulamento do EEDS, pretende-se que sejam estabelecidas regras mais precisas sobre o tratamento de dados pessoais relativos à saúde, de uma forma mais concreta e aprofundada comparativamente ao RGPD, uniformizando este tratamento por todos os Estados-Membros.

Já é prática em muitos Estados-Membros, como é o caso de Portugal, a existência de sistemas nacionais de saúde que estabelecem uma rede de acesso e partilha de dados entre as diferentes instituições hospitalares e prestadores de cuidados de saúde, sendo que este registo eletrónico contém todo o historial clínico dos pacientes, diagnósticos, ocorrências, prescrições, receitas médicas, alergias, etc... e, encontra-se inserido numa infraestrutura centralizada que liga os vários sistemas de RSE. Tal poderá ocorrer quer através de uma infraestrutura organizada, quer através da criação de espaços de dados de saúde ou plataformas de utentes e/ou profissionais de saúde. Mas o facto é que a

existência de um local de armazenamento e partilha de dados entre profissionais de saúde e utentes já foi concebida de diferentes formas. O que pretende a UE agora é livrar-se desta falta de uniformização, aplicando um sistema obrigatório e coerente por toda a União, que cesse os entraves à livre circulação dos dados no espaço europeu.

## 2.2. Principais Obstáculos à Criação do EEDS: Uma Visão Geral

À luz do artigo 8.º da Diretiva 95/46/CE<sup>8</sup>, já revogada, foi estabelecida a proibição do tratamento de dados relativos à saúde, agora concretizada através do RGPD que os considera uma categoria de dados sensíveis e os sujeita a um regime especial, nos termos do seu artigo 9.º. Ao abrigo desta diretiva e deste artigo o Grupo de Trabalho do artigo 29.<sup>º</sup>, grupo que reunia as autoridades nacionais dos Estados-Membros e que funcionava como órgão consultivo da Comissão Europeia, com vista à proteção das pessoas no que diz respeito ao tratamento de dados pessoais através da análise de questões relativas à aplicação das disposições nacionais tomadas nos termos da diretiva, e com vista a contribuir para a sua aplicação uniforme, tornou pública a sua posição quanto à questão dos registos eletrónicos de dados de saúde. Temos que este grupo foi substituído, com a implementação do RGPD, por um Comité com as mesmas atribuições e dotado de personalidade jurídica. Porém, tal não torna as conclusões e recomendações do Grupo de Trabalho menos relevantes para o estudo da proposta em causa, aliás ajuda-nos a perceber quais eram as principais preocupações da União na implementação deste sistema e de que forma é que a proposta em análise conseguiu contemplar as recomendações realizadas.

Assim, podemos apontar como principais preocupações da União: a autodeterminação informacional dos titulares dos dados; a identificação e autenticação de forma segura dos pacientes e profissionais de saúde aquando do acesso a este sistema; a implementação de uma autorização especial para que se pudesse ler, escrever e registar no sistema RSE; o controlo da utilização do sistema de registo de dados eletrónicos para

---

<sup>8</sup> A Diretiva sobre Proteção de Dados (Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995) procurou harmonizar o tratamento de dados de cada Estado-Membro no seu território, garantir a sua proteção assim como estabelecer a livre circulação de dados pessoais entre os Estados-Membros e desenvolvimento do mercado interno, nomeadamente através dos princípios da transparência e proporcionalidade. Como a diretiva não chegava para garantir a proteção dos dados de forma uniforme por deixar muita liberdade aos Estados-Membros, foi criado o RGPD.

<sup>9</sup> Grupo de Trabalho do Artigo 29º para a Proteção de Dados, Documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde eletrónicos (RSE), 00323/07/PT WP 131, adotado em 15 de fevereiro de 2007.

outros fins; a criação de uma estrutura organizativa de um sistema RSE; a criação de categorias dos dados armazenados, assim como modos de apresentação dos mesmos; a regulação da transferência internacional de registos médicos; a verificação da segurança e transparência dos dados; a gestão da responsabilidade através da criação de sanções e ainda o estabelecimento de mecanismos de controlo para o tratamento de dados nos RSE.

De forma a conseguirmos fazer uma melhor análise destes tópicos será necessário estabelecer alguns conceitos, desde logo o conceito de dados de saúde. Assim, dados de saúde, serão na sua base dados pessoais, na aceção da definição do artigo 4.º do RGPD, isto é, qualquer informação relativa a uma pessoa singular que seja identificada ou identificável. Nestes termos será aquela informação identificada ou identificável, se permitir que se possa identificar, diretamente ou indiretamente, uma pessoa singular através dela, sendo exemplos o nome, o número de identificação, elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social. Quanto à questão da “saúde”, falamos de dados relacionados com a saúde física ou mental da pessoa singular, isto é, todos os dados que estejam incluídos num registo clínico, sejam eles relativos ao estado da pessoa, características genéticas e hereditárias, amostras biológicas, comportamentos, influências ambientais e físicas, a prestação de serviços e cuidados médicos, prescrições e receitas, dados administrativos (como o NIF, NISS ou data de admissão num hospital), fatores sociais e educacionais<sup>10</sup>.

Já um registo de saúde eletrónico será, portanto, um registo médico exaustivo, ou documentação semelhante, relativa ao estado de saúde físico e mental, passado e presente, de um indivíduo, em formato eletrónico e que permita a disponibilidade imediata desses dados para tratamento médico e outros fins estritamente relacionados. Assim, o objetivo do registo seria a compilação de toda a documentação e registos/episódios médicos de um indivíduo, provenientes de diferentes fontes e períodos (idealmente registo de toda a vida do paciente), de forma que todos os profissionais de saúde autorizados pudessem ter acesso a esta informação quando

---

<sup>10</sup> Neste tópico referimos o Acórdão do Tribunal de Justiça da União Europeia do Processo de Reenvio Prejudicial C-101/01, de 06 de novembro de 2003, também conhecido como “Acórdão Lindqvist”, sendo este um dos acórdãos mais importantes a respeito do tema da proteção de dados pessoais na internet. Nesta questão prejudicial, o TJUE decidiu que a expressão “dados relativos à saúde” deveria ser interpretada de forma ampla, de modo a incluir informações relativas a todos os aspetos físicos ou psíquicos da saúde de uma pessoa. Assim, o facto de uma pessoa ter lesionado o pé e estar de licença médica constitui um dado de carácter pessoal relativo à saúde ao abrigo do art. 8.º, n.º 1 da Diretiva 95/46.

necessário. Neste sentido, não só nos referimos aos dados fornecidos pelo titular, como por outras pessoas singulares ou coletivas (ex: profissionais e instituições de saúde). Também estarão aqui incluídos dados que tenham sido recolhidos para fins de utilização secundária, dados inferidos ou derivados como são os diagnósticos, exames e testes médicos, e ainda os dados observados e registados por meios automáticos.

Assim, com um registo atualizado seria possível uma melhor qualidade de tratamento, visto existir mais informação sobre os pacientes; uma melhor relação custo-eficácia dos tratamentos médicos, evitando uma evolução nos défices orçamentais no setor da saúde; e ainda, com um fornecimento de dados para controlo da qualidade, as estatísticas e o planeamento no setor dos cuidados de saúde públicos estaria melhor acondicionado sendo um acréscimo positivo nos orçamentos dos cuidados de saúde públicos.

Apesar de um registo eletrónico conseguir obter uma maior qualidade e segurança no conteúdo das informações pelos documentos e dados ficarem todos num só local, sem risco de se perderem como ocorre com os registos em papel, tratam de dados pessoais sensíveis em grande quantidade e mais facilmente acessíveis a um círculo mais vasto de destinatários, acarretando assim um novo risco de possibilidades de utilização indevida dessas informações. Neste sentido é também de notar que o artigo 17.º da Diretiva 95/46/CE impunha que o tratamento de dados fosse efetuado de forma segura, ou seja as medidas técnicas e organizativas do tratamento deveriam ser adequadas para proteger aqueles dados (protegendo-os tanto do acesso de terceiros, como da sua destruição acidental ou ilícita), artigo este cujo conteúdo podemos encontrar no artigo 32.º do RGPD.

Aliás, um registo eletrónico de dados supõe um suporte digital, no entanto questionamo-nos se será possível conceber um sistema totalmente eletrónico em todos os Estados-Membros, de onde constem todas as informações desde o nascimento de cada cidadão até à atualidade. Queria isto dizer que da parte de cada Estado-Membro teria de haver um enorme esforço de forma a transformar todos os registos em suporte de papel, em registos eletrónicos, o que até poderia ser possível para alguns Estados que já realizam esse processo internamente, mas certamente não seria possível para todos. Para além disso, se o objetivo será potenciar o acesso aos dados, será de esperar que estas mudanças abranjam não só a questão da celeridade como também facilitar a todos os cidadãos o acesso. Pondo em causa o plano português que apresenta uma demografia populacional envelhecida, é importante perceber de que forma estes utentes poderão

aceder aos seus dados sem que tal tarefa se demonstre mais um obstáculo ao invés de uma ponte ou atalho<sup>11</sup>.

Como já referimos um dos objetivos consagrados pela proposta será o acesso imediato dos cidadãos aos seus dados de saúde, porém há que reconhecer que um acesso imediato a este tipo de dados poderá também trazer desvantagens e problemas éticos em si. Falamos de exemplos como a informação sobre estados de saúde críticos; não parece adequado que a comunicação de determinadas doenças, como um cancro incurável, ou uma doença letal deva ser realizada por meios eletrónicos. É necessário assegurar que este tipo de informações são comunicadas aos titulares com a empatia que lhes deverá ser intrínseca, pelo que se entende que nestes casos os próprios profissionais de saúde, ou responsáveis pelo tratamento possam esconder ou mesmo bloquear o acesso a estas informações tendo o interesse do titular sempre em mente.

Ainda relevante nesta questão do acesso pelos titulares será o controlo dos dados. Assim, será que esta proposta pretende contemplar um poder efetivo de controlar os dados? Por controlo efetivo entendemos o poder de controlar quais os dados inseridos no sistema, assim como adicionar ou retirar informações. Temos as nossas dúvidas quanto a este aspeto nomeadamente em termos de legitimidade de acesso, apesar de todos terem o direito à privacidade. Por outro lado, os titulares devem consentir no tratamento de todos os seus dados, mas, no que toca a dados de saúde que envolvem conhecimentos técnicos e especializados aquando da sua aferição e interpretação, é-nos difícil conceber que qualquer cidadão possa alterar/ocultar os seus dados. Tal extensão de poder poderia ser mais penosa do que benéfica, podendo levar a tratamentos médicos incoerentes, ineficazes ou incompletos por falta de informação. Coisa diferente será ter o poder para retificar dados de saúde que se encontrem incorretos, aqui entende-se que seja possível os titulares dos dados mediante a deteção de erros solicitarem que estes sejam retificados de imediato, tendo então um poder de fiscalizar a veracidade dos dados inseridos no sistema.

Chamamos ainda a atenção para o facto de um sistema tão complexo quanto este implicar que sejam gerados e armazenados dados de carácter extremamente sensível, ações que acarretam consequências muito maiores do que aquelas que provavelmente conseguimos perceber à primeira vista. Deixamos como exemplo o facto de que, ao

---

<sup>11</sup> Neste sentido, a Recomendação (UE) 2019/243 da Comissão, relembra a importância deste sistema cumprir com os requisitos de acessibilidade estabelecidos pela Diretiva (UE) 2016/2102 do Parlamento Europeu e do Conselho, para as pessoas com deficiência.

permitir armazenar dados relativos à saúde física, mental e comportamental, a proposta poderia proporcionar uma análise de perfis a um nível bastante específico, sendo possível inclusive prever ações e manipular comportamentos.

### 2.2.1. Os Princípios Fundamentais do Tratamento de Dados, em especial: a Licidade

De forma que possa existir um EEDS é importante que este se consiga reger pelos princípios fundamentais relativos ao tratamento de dados pessoais, previstos no art. 5.º do RGPD. Entendemos que deveríamos elencar alguns destes princípios por considerarmos que têm uma especial relevância para o nosso tema.

O princípio da licitude, como vimos pelo título deste ponto, terá uma apreciação especial no nosso estudo. Está previsto no art. 5.º, n.º 1, al. a) e determina, em sentido estrito, que todo e qualquer tratamento de dados encontre o seu fundamento numa norma permissiva (art. 8.º, n.º 2 da CDFUE), e em sentido amplo, que cumpra com a Lei (RGPD e outros diplomas concretamente aplicáveis).<sup>12</sup>

As condições de licitude do tratamento de dados encontram-se previstas, na sua maioria, no art. 6.º, n.º 1 do RGPD (e, por remissão, nos seus arts. 7.º e 8.º), no entanto também encontramos alguns dos fundamentos de licitude nos arts. 9.º e 10.º.

Estando estabelecido no art. 6.º o regime comum da licitude, o art. 9.º consagra um regime especial para o tratamento de dados pessoais sensíveis, que se justifica pela natureza dos dados e riscos acrescidos associados ao seu tratamento. A principal diferença será o “agravamento dos requisitos legais para o tratamento de dados pessoais”<sup>13</sup>.

O principal fundamento da licitude é o consentimento (previsto no regime comum no art. 6.º, n.º1, al. a) e no regime especial no art. 9.º, n.º 2, al. a)) no entanto, quanto ao tratamento de dados de saúde a obtenção deste consentimento pode não se mostrar uma alternativa muito viável. Desde logo porque para que o consentimento possa ser válido ele tem de, à luz do art. 4.º, n.º 11 e do art. 9.º, n.º 2, al. a), ser declarado de forma livre, específica, informada, inequívoca e explícita e, infelizmente, tem-se constatado um

---

<sup>12</sup> CORDEIRO, A. Barreto Menezes, “Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019” / coord. A. Barreto Menezes Cordeiro, Coimbra, Almedina, 2021, p.102.

<sup>13</sup> Idem, “Direito da proteção de dados: à luz do RGPD e da Lei nº 58/2019”, Coimbra, Almedina, 2020, p.238.

elevado nível de desinformação dos pacientes no que toca ao conhecimento sobre quais os dados de saúde que são recolhidos para efeitos da prestação de cuidados/serviços ou quais as consequências do tratamento destes dados.<sup>14</sup> Só será considerado um consentimento informado, aquele em que o titular tenha conhecimento sobre a identidade do responsável, a finalidade do tratamento, a possibilidade de transferência dos dados pessoais para um país terceiro ou organização internacional, os destinatários das transferências, os direitos do titular dos dados, e as consequências do consentimento<sup>15</sup>, e na maior parte dos casos esta não será a situação. Não consideramos que a culpa desta desinformação recaia na totalidade sobre os pacientes, visto que muita desta informação implica um determinado nível de conhecimento técnico, mas não sendo possível tratar os dados com base no consentimento em todos os casos, haverá que justificar o tratamento com base noutro fundamento.

Fazemos assim uma menção ao art. 9.º, n.º 2, al. c) (correspondente no regime comum ao art. 6.º, n.º 1, al. d)), que refere os interesses vitais do titular ou de terceiro. Este é um fundamento com bastantes restrições e que apenas deverá ser utilizado com base na necessidade de evitar a produção de um dano grave para a vida, saúde ou integridade física do titular ou de terceiro, sendo o seu âmbito de aplicação circunscrito com base no considerando 46 do RGPD. Também só poderá ser utilizado nos casos em que o titular esteja incapacitado de prestar o seu consentimento, de todo, ou em tempo útil. Assim, vistas as restrições a este fundamento entendemos que o tratamento de dados relativos à saúde, para os efeitos do regime em análise, não se poderá fundamentar nesta alínea.

Chegados à alínea h) do art. 9.º, n.º 2, deparamo-nos com um fundamento diretamente relacionado com os dados de saúde, sendo então permitido o tratamento de dados pessoais sensíveis quando tal for necessário para efeitos de: medicina preventiva ou do trabalho; avaliação da capacidade de trabalho do empregado; diagnóstico médico; prestação de cuidados ou tratamentos de saúde ou de ação social; e, gestão de sistemas e serviços de saúde ou de ação social. Significa isto que nas situações em que não seja possível obter o consentimento do titular dos dados, através desta alínea, o tratamento de dados pessoais de saúde será lícito. É ainda feita uma ressalva na parte final da alínea

---

<sup>14</sup> DRUEDAHL, L.C., Kälve mark Sporrang, S., “Patient Perspectives on Data Sharing”, *In: Corrales Compagnucci, M., Minssen, T., Fenwick, M., Aboy, M., Liddell, K. (eds) The Law and Ethics of Data Sharing in Health Sciences. Perspectives in Law, Business and Innovation. Springer, Singapore, 2024.*

<sup>15</sup> GONÇALVES, Anabela Susana de Sousa, “O Consentimento como Fundamento de Licitude para o Tratamento de Dados Pessoais na União Europeia”, 2022, p. 57.

h), dizendo-nos que o tratamento destes dados para fins de cuidados de saúde deve ter como base o Direito da União ou dos Estados-Membros, ou uma relação estabelecida com um profissional de saúde sujeito a uma obrigação de sigilo, nos termos do art. 9.º, n.º 3<sup>16</sup>. O art. 29.º da Lei 58/2019, de 8 de agosto fala especificamente do tratamento de dados de saúde impondo estritos deveres de sigilo a todos os profissionais que estejam envolvidos no tratamento dos dados ao lado do responsável<sup>17</sup>.

Não deixaremos de fazer menção à alínea i) que ao contrário da al. h) que se refere aos interesses individuais do titular no domínio da saúde, visa a proteção de interesses coletivos, nomeadamente a saúde pública. A definição de saúde pública encontra-se prevista no art. 3.º, al. c) do Regulamento (CE) n.º 1338/2008 do Parlamento Europeu e do Conselho de 16 de Dezembro de 2008<sup>18</sup>, sendo constituída por,

*[T]odos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade.*

Assim, ao lado de um motivo de interesse público, qualquer um destes elementos poderia justificar o tratamento de dados de saúde, desde que sujeito ao cumprimento de medidas adequadas e específicas, a fim de defender os direitos e liberdades das pessoas singulares. Esta autorização exclui o tratamento destes dados para outros fins ou por outras entidades, nomeadamente seguradoras ou instituições bancárias.<sup>19</sup>

Vista a questão da licitude, temos ainda alguns princípios sobre os quais gostaríamos de tecer algumas considerações.

O princípio da finalidade (art. 5.º, n.º 1, alínea b) do RGPD), previsto também no art. 8.º, n.º 2 da CDFUE, determina que os dados devem ser recolhidos para finalidades determinadas, explícitas e legítimas. Assim, serão determinadas as finalidades do tratamento que estejam definidas antes do início do processo, estando os seus propósitos devidamente identificados e fundamentados. Serão explícitas se forem conhecidas dos interessados no tratamento, i.e., o titular, autoridades competentes e terceiros.<sup>20</sup>E, serão

---

<sup>16</sup> CORDEIRO, A. Barreto Menezes, Op. cit, p. 250.

<sup>17</sup> Ibidem, p. 239.

<sup>18</sup> Regulamento (CE) n.º 1338/2008 do Parlamento Europeu e do Conselho de 16 de Dezembro de 2008 relativo às estatísticas comunitárias sobre saúde pública e saúde e segurança no trabalho.

<sup>19</sup> RGPD, Considerando (54).

<sup>20</sup>Grupo de Trabalho do Artigo 29º para a Proteção de Dados, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, adopted on 2 April 2013, p. 17.

legítimas as finalidades que cumpram com as disposições legais concretamente aplicáveis. Relacionando este princípio com o regime em análise, temos que a recolha e tratamento de dados relativos à saúde deve cumprir com este princípio, ou seja, as finalidades do tratamento devem cumprir com estes requisitos. Será que um sistema RSE de onde constem os dados de saúde de vários pacientes e consequentemente um EEDS, conseguem cumprir com estas limitações? Cremos que sim, porque mesmo que os dados de um paciente sejam tratados ao abrigo de uma prestação de cuidados específica, não significa que o registo e manutenção desses dados num sistema sejam contrários à finalidade inicial. O princípio permite que os dados sejam objeto de tratamento subsequente se o responsável utilizar os dados para uma finalidade compatível com a originária, e a continuidade da prestação de cuidados de saúde, mesmo que no futuro e relativamente a uma situação distinta parece, a nosso ver, uma finalidade compatível.

De seguida temos o princípio da minimização (art. 5.º, n.º 1, alínea c)), segundo o qual os dados recolhidos devem ser adequados, pertinentes e limitados às finalidades em causa, andando este princípio de mão dada com o princípio da exatidão (art. 5.º, n.º 1, alínea d) do RGPD), que nos diz que os dados deverão estar sempre atualizados, que os dados inúteis deverão ser eliminados e que deverão ser sempre realizadas as necessárias retificações. Consideramos que os dados mantidos num sistema RSE relativos a situações passadas, que não reflitam a saúde atual do paciente, continuam a cumprir com este princípio, pois só assim se conseguirá ver uma figura completa da saúde do titular dos dados.<sup>21</sup>

No princípio da conservação (art. 5.º, n.º 1, alínea e), do RGPD), consta a obrigação de conservação dos dados apenas pelo período necessário para a finalidade com que foram recolhidos.

Temos finalmente de fazer uma referência aos princípios da integridade e confidencialidade (art. 5.º, n.º 1, al.f)) que impõe que os responsáveis pelo tratamento garantam a segurança dos dados contra perdas, destruição ou danificação e ainda contra acessos não autorizados. No artigo 29.º, n.º 1 da Lei 58/2019 está consagrado o princípio *need to know*, que apesar de não ser um dos princípios fundamentais elencados no n.º 5 do RGPD é de enorme relevância no nosso estudo, podendo ser retirado dos princípios da integridade e confidencialidade. Este princípio determina que, “os funcionários,

---

<sup>21</sup> CORDEIRO, A. Barreto Menezes, “Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019” / coord. A. Barreto Menezes Cordeiro, Coimbra, Almedina, 2021, p.106.

prestadores de serviços e demais sujeitos que auxiliam os responsáveis pelo tratamento de dados ou os subcontratantes apenas podem aceder a dados pessoais na medida em que seja necessário para o exercício das suas funções”<sup>22</sup>. Apesar deste princípio estar consagrado no sistema português, entendemos que deverá ser considerado em termos de aplicação do regime pensado para o EEDS, especialmente se tivermos em conta as diferentes categorias de profissionais de saúde que tratam dados pessoais no exercício das suas funções.

## 2.2.2. As Principais Problemáticas a Regular na Proposta

Vista a questão da licitude e dos restantes princípios fundamentais do tratamento dos dados pessoais de saúde, cabe-nos discutir alguns aspetos que consideramos que devem estar devidamente regulados na proposta, de forma que o regime pensado seja o mais seguro e confiável possível para os titulares dos dados, nunca esquecendo que há um quadro jurídico vigente e regulado pelo RGPD para o tratamento de dados sensíveis.

Começamos então por referir que os titulares dos dados têm o direito à autodeterminação informacional. De acordo com este, não é só imposto aos responsáveis pelo tratamento um dever de segredo e segurança, como também é atribuído aos titulares o controlo sobre os seus dados, podendo impor limitações ao seu tratamento, acesso e divulgação.<sup>23</sup> Este direito dá “a cada pessoa o direito de controlar a informação disponível a seu respeito, impedindo-se que a pessoa se transforme em simples objeto de informações.”<sup>24</sup>

Estabelecido este direito, consideramos que deverão existir diferentes graus no seu exercício. Assim, enquanto regra-geral, o acesso aos dados deveria ser regido por um sistema de “*opt-in*”, especialmente no caso de dados com potencial discriminatório (dados relativos a aborto ou psiquiátricos) e “*opt-out*” para aqueles dados menos intrusivos, garantindo assim flexibilidade, mas um nível adequado de proteção. Deste modo os titulares poderiam ter o controlo dos seus dados, restringindo o acesso aos profissionais de saúde.

---

<sup>22</sup> Idem, “Direito da proteção de dados: à luz do RGPD e da Lei nº 58/2019”, Coimbra, Almedina, 2020, p.253.

<sup>23</sup> CASTRO, Catarina Sarmiento e, “40 anos de «Utilização da Informática» - o artigo 35.º da Constituição da República Portuguesa”, 2016, p.51.

<sup>24</sup> CANOTILHO, J.J. Gomes; MOREIRA, Vital – Constituição da República Portuguesa Anotada, Vol. I, cit., p. 550.

Relativamente ao acesso dos profissionais de saúde a estes dados, como vimos o acesso destes será lícito, desde que cumprindo com as finalidades da alínea h) e as que venham a estar previstas no regime do EEDS. No entanto, chamamos a atenção para a necessidade de garantir a segurança na identificação e autenticação das pessoas que terão acesso aos dados de saúde, entendendo nós que mesmo entre os profissionais deverá estar regulado um acesso/partilha seletiva. Os pacientes, em geral, confiam mais nos médicos do que noutros membros das equipas técnicas ou no sistema de saúde em geral, aquando da partilha dos seus dados<sup>25</sup>, pelo que restringir ao máximo o número e a categoria de profissionais que têm este acesso seria bastante benéfico. A questão já foi discutida na Deliberação n.º 984/2018<sup>26</sup> da Comissão Nacional da Proteção de Dados (CNPd), em que se discutia a necessidade dos prestadores de cuidados terem acesso a todo o historial de um paciente dada a tendencial impossibilidade de estratificar informação consoante a finalidade. Em princípio, não se consegue definir *a priori* quais os dados relevantes, em concreto, para uma determinada prestação de cuidados/serviços.<sup>27</sup> Concordamos com esta afirmação até determinado ponto, mas também entendemos que com a evolução tecnológica e o poderio existente na criação do regime em análise, não seria inadequado acreditar que esta avaliação casuística da informação fosse concretizável.

De todo o modo, mesmo não sendo possível adaptar a informação disponível aos profissionais consoante a prestação de cuidados, com certeza será possível estabelecer um sistema de categorização, que defina critérios de credencialização de forma a não permitir que qualquer médico, de qualquer especialidade, a qualquer altura possa aceder aos dados dos titulares de um determinado centro hospitalar, e ainda evitar que outros profissionais como técnicos ou farmacêuticos tenham um acesso desproporcional face às suas funções.<sup>28</sup> Caso estas restrições não sejam devidamente estabelecidas corre-se o risco de tornar “irrelevante o núcleo essencial do direito fundamental à proteção de dados pessoais”<sup>29</sup>, assim como violar os princípios da minimização e da integridade e confidencialidade.

---

<sup>25</sup> KIM J, Kim H, Bell E et al., Patient perspectives about decisions to share medical data and biospecimens for research. *JAMA Netw Open* 2(8):e199550, 2019;  
SANYER O, Butler JM, Fortenberry K et al., Information sharing via electronic health records in team-based care: the patient perspective. 2021, *Fam Pract* 38(4):468–472, 2021.

<sup>26</sup> Deliberação n.º 984/2018 da Comissão Nacional da Proteção de Dados, Processo n.º 9932/2018, de 9 de outubro de 2018.

<sup>27</sup> *Ibidem*, p. 6.

<sup>28</sup> *Ibidem*, p. 6.

<sup>29</sup> *Ibidem*, p. 7.

Num sistema de registo de dados eletrónicos, será necessária a implementação de uma estrutura organizativa, pelo que consideramos três possibilidades a adotar.

A primeira opção seria um RSE como sistema que dá acesso aos registos médicos mantidos pelo profissional de saúde, que tem a obrigação de manter registos sobre o tratamento dos seus pacientes, o designado “armazenamento descentralizado”. A segunda opção passaria por um sistema uniforme de armazenamento, para o qual os profissionais de saúde teriam de transferir a sua documentação, o “armazenamento centralizado”. Por último, teríamos uma terceira alternativa, permitindo que o titular dos dados controlasse os seus próprios registos médicos, decidindo inclusive o que seria inserido no processo clínico<sup>30</sup>.

Começando pela terceira opção parece-nos que um sistema previsto nestes moldes não permitiria que a qualidade da informação fosse assegurada, ficando esta comprometida por não possuir a mesma exatidão e exatidão exigida para este tipo de conteúdo. Quanto ao armazenamento descentralizado, apesar da criação de caminhos de pesquisa, dado que a estrutura atual de armazenamento da documentação permaneceria inalterada, caso a qualidade do sistema de pesquisa não seja a melhor, a localização dos dados dos doentes poderia tornar-se uma tarefa complicada. Já o armazenamento centralizado, iria idealmente permitir uma maior segurança técnica e disponibilização a todo o tempo dos dados, no entanto tal implicaria a existência de um controlador único para todo o sistema, distinto dos profissionais/instituições de saúde que transmitem a sua documentação ao sistema central. Ora não sendo os profissionais de saúde os responsáveis por este tratamento, temos que o requisito da obrigação de sigilo poderia também ser comprometido, deixando os titulares menos confiantes no sistema.

O objetivo do EEDS seria ser uma compilação de todos os dados de saúde registados ao longo de toda a vida dos titulares. No entanto, para evitar que um ficheiro de saúde seja um documento extremamente exaustivo, que torne complicada a leitura da informação, seria importante a criação de diferentes categorias conforme a relevância dos dados para o estado de saúde do titular, de forma que não seja comprometido o sucesso do tratamento.

Questionamos ainda, qual o período de conservação destas informações. Apesar de existirem dados que são relevantes para toda a vida do titular, seja o caso das alergias,

---

<sup>30</sup> Grupo de Trabalho do Artigo 29º para a Proteção de Dados, Documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde eletrónicos (RSE), 00323/07/PT WP 131, adotado em 15 de fevereiro de 2007, p. 17.

com certeza haverá informação que só tem relevância para aquela prestação de cuidados de saúde específica. Entendemos que informações como a medicação ou as prescrições médicas e o boletim de vacinação devem ser informações facilmente acessíveis por parte dos titulares, tal como a um conjunto alargado de serviços de saúde, já quanto a outras categorias de dados mais sensíveis, o acesso dos profissionais poderia depender de consentimento prestado por parte do paciente, como seria por exemplo a informação sobre tratamentos psiquiátricos, existência de DST's, informações sobre a sujeição a uma interrupção voluntária da gravidez, etc (...).

Como é claro, a interoperabilidade dos dados e a transferência destes entre os diferentes Estados-Membros será um dos elementos-chave de um sistema de RSE ao nível europeu, dado que permitiria melhorar os meios de diagnóstico e de tratamento, inclusive através do acesso a conhecimentos médicos especializados disponíveis noutros países.

Podemos concordar que muitas vezes a busca por conselhos médicos não exige que a identidade do paciente seja revelada, pelo que também seria interessante pensar na possibilidade desses dados poderem ser transferidos para países fora da UE ou EEE, anonimamente. Se os dados transferidos não forem suscetíveis de identificar o titular, não estaremos a falar de dados pessoais e o RGPD não será aplicável, pelo que fazer com que o formato dos dados seja interoperável nesses casos também é um aspeto a ter em conta.

Contudo, o tratamento de dados pessoais relativos à saúde deve ser sempre feito em países da UE, precisamente para garantir o cumprimento do quadro jurídico em matéria de proteção de dados e as regras do RGPD. No EEDS, o nível de segurança da proteção dos dados terá de ser elevadíssimo e o acesso de pessoas não autorizadas deve ser praticamente impossível e impedido. O acesso ao sistema pelos próprios profissionais deverá ser limitado e eficiente, devendo ser criadas obrigações ou condições que impeçam a alteração ou perda de dados injustificadas, assim como o tratamento e acesso não autorizados.<sup>31</sup> O uso de cifragem deverá ser contemplado não só para a transferência como para o armazenamento dos dados pessoais.

Para que esta segurança seja garantida será então necessário que exista um sistema fiável de identificação e autenticação eletrónicas, que os registos dos dados sejam constantemente atualizados, verificando-se todos os acessos e respetivas solicitações,

---

<sup>31</sup> Por exemplo, através da implementação de Privacy enhancing technologies (PETs) - ou, tecnologias de reforço da privacidade a ser aplicadas para promover a proteção dos dados pessoais.

que exista um registo exaustivo de todas as etapas de processamento que tiveram lugar (pedidos de acesso, leituras e introdução de dados), mecanismos de recuperação e de cópias de segurança para proteger o conteúdo do sistema, garantindo que não exista alteração de dados durante estes processos, clareza nas instruções de utilização do sistema pelo pessoal autorizado, distinção das funções e acessos das diferentes categorias de pessoas e ainda auditorias externas e internas regulares em matéria de proteção.<sup>32</sup>

Entendemos que a implementação do EEDS traga consigo uma grande pressão e tanto a opinião pública, como as pessoas singulares, de forma a confiarem no sistema exigirão um elevado nível de transparência no que respeita ao seu conteúdo e funcionamento. Por isto mesmo, os responsáveis pelo sistema deverão manter contacto e notificar as autoridades de controlo da proteção de dados, assim como assegurar que todas as comunicações feitas relativas a este mecanismo sejam de fácil acesso e compreensão.

Fica ainda a questão da responsabilidade, quem será responsável por eventuais violações de privacidade causadas pelo armazenamento destes dados, por exemplo a utilização dos dados para outros fins ou por pessoas não autorizadas? Para averiguar questões de responsabilidade será necessário que os próprios Estados-Membros realizem estudos aprofundados e avaliações de impacto antes de aplicarem este regime, focados em direito civil e direito médico.

Perante os cenários de risco inerentes a um regime como este, ficará a tarefa de instaurar mecanismos de controlo eficazes. Assim, os litígios que surjam à luz do sistema deverão estar sujeitos a um processo de arbitragem especial, não havendo entraves para que os titulares dos dados lhes possam recorrer. Também, havendo vários responsáveis pelo tratamento, compreende-se a necessidade da criação de uma entidade ou instituição especial que consiga vir responder às dificuldades que o acesso ao sistema possa causar, entre outras complicações que venham a surgir.

### **3. ANÁLISE DO REGIME PROPOSTO**

Passando agora à análise da proposta, gostaríamos de deixar referenciado mais uma vez que na nossa investigação não pretendemos fazer uma análise exaustiva de todo

---

<sup>32</sup>Ibidem, p. 20.

o regime proposto, sendo que tal seria impossível dada a extensão do nosso trabalho. Contudo selecionamos algumas das normas e capítulos da proposta que entendemos serem relevantes para a análise das questões feitas ao longo das últimas páginas, planeando expor agora o seu conteúdo, relacioná-lo com o RGPD e outros diplomas relevantes no tema da proteção de dados, assim como verificar se, face aos problemas suscitados, esta proposta consegue responder adequadamente, ou se, na nossa humilde opinião, carece de uma melhor concretização.

Desde logo é importante referir que o RGPD não é o único diploma que pode entrar em conflito com a proposta, sendo que há outros diplomas tais como o Regulamento (UE) 2018/1725<sup>33</sup> e a Diretiva 2002/58/CE<sup>34</sup>, que concretizam os direitos fundamentais previstos nos arts. 7.º e 8.º da CDFUE e no art.16.º do TFUE. Deste modo torna-se imperativo evitar que a proposta possa colocar direta ou indiretamente estes direitos adquiridos em risco. Assim, de modo que se possa concretizar um quadro-jurídico como é o pretendido, e efetivamente chegar um passo mais à frente na digitalização da UE, a criação deste EEDS deve ser o mais transparente e sólida possível, estando em harmonia total com o RGPD e os restantes diplomas relativos à proteção de dados servindo então de exemplo a futuros mecanismos.

### 3.1. Disposições Gerais

O primeiro capítulo apresenta-nos as disposições gerais cobrindo o primeiro e segundo artigo da proposta. Nesta primeira paragem são estabelecidos os âmbitos de aplicação e as definições que nos irão acompanhar ao longo de todo o diploma sendo de imensa importância que todos os conceitos sejam explícitos não deixando dúvidas ao interpretador.

No seu artigo 1.º temos, como já vimos, expostos os objetivos da proposta, que serão então a criação de um Espaço Europeu de Dados de Saúde, assim como as regras que irão guiar e governar a utilização primária e secundária dos dados de saúde

---

<sup>33</sup> Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho de 23 de outubro de 2018 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE.

<sup>34</sup> Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de Julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Directiva relativa à privacidade e às comunicações eletrónicas).

eletrónicos. Desde logo o regulamento pretende vir reforçar os direitos dos titulares dos dados no que toca ao acesso, disponibilidade e controlo dos seus dados.

Quanto à questão da utilização primária de dados vs. utilização secundária de dados é uma dualidade que surgirá bastantes vezes ao longo do diploma, pelas controvérsias que poderão surgir dela, no entanto, na nossa análise não iremos apreciar a fundo a questão da utilização secundária, considerando apenas os problemas subjacentes à utilização primária. De todo o modo, e esclarecendo o que significam estes dois tipos de utilização de dados, de acordo com a proposta será utilização primária de dados,

*“[O] tratamento de dados de saúde eletrónicos pessoais para a prestação de serviços de saúde a fim de avaliar, manter ou restabelecer o estado de saúde da pessoa singular a quem esses dados dizem respeito, incluindo a prescrição, a dispensa e o fornecimento de medicamentos e dispositivos médicos, bem como para os serviços pertinentes de segurança social, administrativos ou de reembolso”*,

ou seja, essencialmente o tratamento de dados para interesses do próprio titular. Já a utilização secundária está regulada no capítulo IV, fazendo o artigo 1.º uma referência ao facto de que os dados utilizados poderão incluir dados que tenham sido inicialmente recolhidos para fins de utilização primária. Assim, será utilização secundária de dados, o tratamento de dados para a prestação de serviços de saúde ou cuidados para efeitos de saúde pública, investigação, inovação, elaboração de políticas, estatísticas oficiais, segurança dos doentes ou regulamentação, recolhidos por entidades e organismos dos setores da saúde ou da prestação de cuidados, incluindo prestadores públicos e privados, entidades ou organismos que realizam investigação nestes setores e instituições, órgãos e organismos da União.

Em termos práticos parece que relativamente à utilização primária os titulares terão controlo sobre os seus dados de saúde e poderão restringir o acesso a estes. No entanto, o artigo 38.º, n.º 2, estabelece que os organismos responsáveis pelo acesso aos dados de saúde não são obrigados a facultar as informações previstas no artigo 14.º do RGPD. Esta questão é relevante porque o artigo 14.º prevê situações em que os dados não são recolhidos juntos do titular e neste sentido parte-se do princípio de que o titular não terá ideia sobre quem será o responsável e a finalidade do tratamento, ou mesmo quais as categorias de dados a serem tratadas. Para perceber o alcance desta norma, importa sublinhar que este artigo se encontra previsto no capítulo relativo à utilização secundária de dados que, como vimos, abrange não só a investigação científica e

elaboração de políticas, como também a inovação. Não estando estes conceitos definidos de forma precisa, corre-se o risco de circunscrever os direitos dos titulares dos dados a um círculo mais estreito do que aquele permitido ao abrigo do art. 23.º do RGPD.

Estando estabelecido o âmbito objetivo da norma, o artigo 1.º, n.º 3, prevê o seu âmbito de aplicação subjetiva, regulando os sujeitos aos quais o regulamento será aplicável. Porém, na sua alínea a), apesar de referir os fabricantes, fornecedores e utilizadores de sistemas de RSE e de aplicações de bem estar, não refere os fabricantes, fornecedores e utilizadores de dispositivos médicos, ainda que os refira ao longo do regulamento, como serão exemplos os arts. 14.º, n.º 3, 23.º, 32.º e 33.º, n.º1, als. f) e n). Neste sentido entendemos que poderá estar em falta uma clarificação deste aspeto.

No seu parecer conjunto sobre a proposta<sup>35</sup>, o Comité Europeu para a Proteção de Dados (CEPD) e a Autoridade Europeia para a Proteção de Dados (AEPD) entendem que no âmbito deste regulamento e na criação do EEDS não deverão ser incluídos os dados constantes de aplicações de bem-estar ou outras aplicações. Contrariamente aos dispositivos médicos que se encontram sujeitos a legislação específica<sup>36</sup>, a qualidade dos dados recolhidos pelas aplicações não se encontra assegurada.

O artigo 2.º vem estabelecer as definições dos conceitos a serem utilizados ao longo do regulamento. É de notar desde logo as várias remissões aos diferentes diplomas e regulamentos da União sobre proteção de dados como é o caso do RGPD ou do Regulamento de Governação de Dados<sup>37</sup>, compreendendo-se esta opção sob pena de a proposta estar a definir termos já convencionados na UE. No entanto, apesar de fazer esta remissão para alguns conceitos, quanto a outros vem introduzir a sua própria definição, embora já esteja assente noutros regulamentos. Será disto exemplo o artigo 2.º, n.º 2, alínea f), que vem apresentar uma definição de “interoperabilidade”, no entanto, o conceito aparece definido de forma bastante lata, sendo mais tarde feita referência ao anexo II do diploma que pretende estabelecer os requisitos de interoperabilidade. A este nível temos também o Regulamento (UE) 910/2014 do

---

<sup>35</sup> Parecer conjunto 03/2022 do CEPD e da AEPD sobre a proposta de regulamento relativo ao Espaço Europeu de Dados de Saúde, adotado em 12 de julho de 2022, p. 12, parágrafo 36.

<sup>36</sup> Nomeadamente o Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos, que altera a Diretiva 2001/83/CE, o Regulamento (CE)178/2002 e o Regulamento (CE) n.º 1223/2009 e que revoga as Diretivas 90/385/CEE e 93/42/CEE do Conselho.

<sup>37</sup> Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento de Governação de Dados).

Parlamento Europeu e do Conselho de 23 de julho de 2014<sup>38</sup>, que já vem definir tais requisitos. Neste sentido, cremos que seria importante a proposta fazer uma ponte entre estes critérios e aqueles que vem estabelecer, de forma que estes possam ser interpretados de forma uniforme.

Também será um bom exemplo a definição de “detentor de dados” prevista na alínea y) do mesmo artigo, sendo que este conceito também já é definido no Regulamento de Governação de Dados, como,

*[U]ma pessoa coletiva, incluindo organismos do setor público e organizações internacionais, ou uma pessoa singular que não seja o titular dos dados no que diz respeito aos dados específicos em causa, que, (...), tem o direito de conceder acesso a determinados dados pessoais ou dados não pessoais ou de os partilhar;*

e também no Regulamento de Dados,<sup>39</sup> que define o conceito como

*[U]ma pessoa singular ou coletiva que tem o direito ou a obrigação, (...), de utilizar e de disponibilizar determinados dados, nomeadamente, caso tal tenha sido acordado contratualmente, dados relativos a um produto ou dados relativos a um serviço conexo que tenha recuperado ou gerado durante a prestação de um serviço conexo.*

Como podemos ver estas definições, para além de serem distintas entre si, também não são exatamente iguais ao conceito definido na proposta, sendo que os poderes destes detentores acabam por ser mais abrangentes nesta última por lhes ser permitido: não disponibilizar os dados, registar, fornecer, restringir o acesso ou proceder ao seu intercâmbio.

Tendo em conta a expansão da atividade dos detentores, torna-se essencial que o conceito esteja estabelecido de forma que especifique quem efetivamente serão os detentores dos dados. Há também que ter em conta que são estes detentores que disponibilizam os dados pessoais de saúde para efeitos de utilização secundária ao abrigo do artigo 33.º da proposta, pelo que a sua correta identificação deverá ser assegurada.

Outra contradição a apontar neste conceito é o facto de o artigo 3.º, n.º 8, se referir aos detentores de dados do setor da segurança social, sendo certo que a definição

---

<sup>38</sup> Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE.

<sup>39</sup> Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho de 13 de dezembro de 2023 relativo a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização e que altera o Regulamento (UE) 2017/2394 e a Diretiva (UE) 2020/1828.

plasmada no artigo 2.º apenas faz referência ao setor da saúde, pelo que está em falta uma harmonização do conceito dentro do próprio regulamento.

Finalmente é também de fazer uma nota às definições das alíneas k) e z) do artigo 2.º que fazem referência ao “destinatário de dados” e ao “utilizador de dados”, definindo o primeiro como a pessoa singular ou coletiva que recebe dados de um responsável pelo tratamento para fins de utilização primária e o segundo como uma pessoa singular ou coletiva que tem acesso aos dados de saúde para fins de utilização secundária. Ora neste tópico poderemos referir que o conceito de destinatário dos dados está também previsto no RGPD, sendo-nos apresentado um conceito diferente visto que não é referida a questão da finalidade. Assim, faria sentido que fosse feita uma ressalva ou, uma melhor conexão com o RGPD. Já quanto à interação entre os dois conceitos dentro da própria proposta, temos que embora as instituições da União estejam presentes na definição de “detentor de dados” prevista na alínea y), não estarão consagradas em nenhuma destas duas definições das alíneas k) e z); sendo certo que são os responsáveis pelo tratamento que tratam da disponibilização dos dados aos destinatários, e estas instituições, serão, em termos práticos, utilizadoras dos dados para fins de utilização secundária, a verdade é que tal não consta da proposta. Parece-nos então que a interação entre estas três figuras e os papéis que representam na proposta, aquando da leitura desta poderiam ser mais claros visto que ainda deixam espaço para dúvidas.

### 3.2. A Utilização Primária dos Dados de Saúde

Passando para aquele que será o capítulo no qual estenderemos mais a nossa análise, o capítulo II regula a utilização primária dos dados de saúde eletrónicos. Propõe-se a apresentar e especificar “os direitos e mecanismos adicionais destinados a complementar os direitos das pessoas singulares previstos no RGPD em relação aos seus dados de saúde eletrónicos”<sup>40</sup>.

Assim, prevê os direitos das pessoas singulares sobre a utilização dos dados, o acesso dos profissionais de saúde aos dados e as suas obrigações, quais as categorias prioritárias de dados para efeitos da implementação faseada da proposta, de que forma

---

<sup>40</sup> Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao Espaço Europeu de Dados de Saúde, COM/2022/197 final, p. 20, consult. em 24/Fev/2024, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52022PC0197> .

estes dados serão registados e partilhados entre os diferentes Estados-Membros, a criação de uma autoridade de saúde digital responsável pelo controlo e fiscalização dos direitos e obrigações impostas. Também muito relevante será esta obrigação dos Estados-Membros de designar um ponto de contacto nacional encarregado de fazer cumprir estas obrigações.

Começando então a nossa análise pelo artigo 3.º, temos que este vem estabelecer os direitos das pessoas singulares sobre os seus dados de saúde eletrónicos, introduzindo desde logo um dos principais objetivos da proposta que será esta ideia de que com a criação do EEDS as pessoas singulares terão o direito de aceder “imediatamente, *a título gratuito e de forma facilmente legível, consolidada e acessível*”<sup>41</sup> aos seus dados de saúde eletrónicos pessoais tratados no contexto da utilização primária de dados de saúde eletrónicos”( art. 3.º, n.º 1 da proposta).

Ora, o direito de acesso aos seus dados pessoais já é um direito titulado ao abrigo do RGPD, no seu art. 15.º, vindo neste sentido o art. 3.º repetir ou mesmo sobrepor algumas das suas disposições às já previstas pelo RGPD. Porém, apesar de virem regular em muitos aspetos os mesmos direitos, também o fazem de formas distintas. No caso do RGPD há um grande foco em especificar exatamente as informações a que o titular dos dados tem direito a aceder, tais como as finalidades do tratamento, as categorias, os destinatários dos dados e qual a sua origem (se dentro da União Europeia ou no plano internacional), qual o prazo de conservação dos dados, as informações disponíveis sobre a origem dos dados caso não tenham sido recolhidos junto do titular, etc (...). Já a proposta em análise não se foca tanto em especificar estas condições, estabelecendo o direito em termos mais genéricos, mas também tem em atenção aspetos mais direcionados ao plano dos dados de saúde eletrónicos, obviamente. De todo o modo também acreditamos que poderia ser interessante a proposta fazer alguma ressalva ao art. 15.º do RGPD, no próprio art. 3.º de forma a salvaguardar estes direitos já estabelecidos, por entendermos que qualquer interpretação da norma deverá sempre ser feita com base no que já está previsto, por se tratar de informação solidificada dentro da UE, fazendo-se então a sua extensão/aplicação aos dados de saúde eletrónicos.

Em termos de novidades será de apontar sem dúvida a obrigação da criação de um formato europeu de intercâmbio de RSE (arts. 3.º, n.º 2 e 6.º), concretizando então a uniformização de apresentação dos dados e do seu conteúdo, aos titulares, aquando da

---

<sup>41</sup> Itálico nosso.

sua solicitação, pelo menos no que toca às categorias prioritárias de dados. O que são estas categorias prioritárias de dados? Dada a quantidade e qualidade dos dados de saúde eletrónicos, entendeu-se que a implementação do regulamento deverá ser faseada, começando então pela introdução de dados de saúde com uma importância mais elevada, desde logo aqueles factos clínicos essenciais para a prestação de cuidados de saúde eficientes e seguros como: informações de contacto e seguro, alergias, alertas médicos, vacinação, quais os problemas atuais ou mesmo resolvidos, a existência de dispositivos médicos e implantes, historial de gravidez, medicação atual e planos de cuidados e ainda informações sobre alguma doença rara. Estas categorias são melhor exploradas no artigo 5.º da proposta e no seu anexo I, sendo obrigatório que estas obedeçam a determinados critérios como: relevância para a prestação de serviços de saúde; utilização num número significativo de sistemas de RSE empregues nos Estados-Membros; e existência de normas internacionais relativas à categoria, que tenham sido examinadas quanto à possibilidade da sua aplicação na União (art. 5.º, n.º 2, als. a), b) e c)).

No n.º 3 do art. 3.º é feita uma ressalva para o art. 23.º do RGPD, assegurando a sua conformidade com o RGPD, dado que é prevista uma limitação para este direito de acesso aos dados, nomeadamente em situações em que a revelação daquela informação ao titular possa ser prejudicial para este. Acreditamos assim que o objetivo do artigo seria assegurar a proteção/defesa dos titulares dos dados de saúde eletrónicos (art. 23.º, n.º 1, al. i), do RGPD), em situações em que seria eticamente incorreto da parte dos detentores dos dados, nomeadamente, profissionais de saúde, revelarem essa informação por meios eletrónicos. Serão os típicos casos em que há que informar um paciente sobre um diagnóstico complexo com implicações muito graves para a sua saúde, e o facto de um paciente poder a vir ter acesso a essa informação sem o devido contexto poderia causar grandes impactos na sua saúde mental ou mesmo na forma como reagiria à notícia. No entanto, também é referido no artigo que estas limitações ao acesso devem ser temporárias, até que o profissional de saúde em causa possa explicar a situação de forma mais pessoal.

Passando para o n.º 5, fará parte das obrigações dos Estados-Membros a criação de serviços de acesso a dados de saúde eletrónicos a nível nacional, regional ou local, sendo certo que em muitos Estados-Membros essa possibilidade já é uma realidade como por exemplo, através da existência de portais do utente ou aplicações móveis destinadas aos doentes, no entanto a proposta, no seu considerando 9, argumenta que tais sistemas devem estar presentes com mais influência e sublinha a importância de que

o acesso aos dados seja feito por via eletrónica que permita um acesso imediato, sem a necessidade de disponibilização dos dados em suporte de papel ou em formato digitalizado. Tal será importante do ponto de vista dos utentes, que não terão mais um obstáculo aquando da consulta dos seus dados, como também na partilha de dados entre entidades e instituições de saúde – quanto mais célere e organizado for o acesso mais eficiente e útil será a prestação do serviço. Porém, é de notar que também neste considerando é feita uma ressalva relativamente à disponibilização dos dados em papel, sendo que mesmo tratando-se de um sistema eletrónico, a transformação dos documentos em suporte de papel só será exigida quando tal esforço não se mostre desproporcional, não sendo então vinculativo para os Estados a disponibilização dos dados em suporte eletrónico.

Para além deste serviço, é também introduzido o serviço de autorizações/procurações no acesso aos dados de saúde eletrónicos (art. 3.º, n.º 5, alínea b)), de forma que pessoas singulares incapacitadas possam delegar noutras pessoas o acesso e administração destes dados. Estas autorizações deverão ser gratuitas, sendo certo que os Estados-Membros poderão ter liberdade no que toca à regulação de limitações na concessão destas autorizações por motivos de proteção e segurança dos doentes. Tendo a possibilidade de administrar, em representação de outrem o acesso aos seus dados de saúde, é concedido um grande poder e responsabilidade a estes procuradores, que poderão ou não ser tutores legais ou responsáveis pelo titular dos dados. De entre estas capacidades não estará apenas o poder de aceder aos dados, mas também o de os inserir no sistema (n.º 6 do mesmo preceito), o que poderá trazer implicações para o titular de dados, na falta de adoção de garantias adequadas. A verdade é que esta proposta de serviços de procuração está estabelecida através de termos muito gerais que não permitem uma verdadeira concretização segura dos direitos dos titulares dos dados, desde logo porque os requisitos precedentes a este mecanismo de autorização, sobre quem e sob que condições poderá recair a função de representação, não estão claros. Mais do que não estarem claros, estão previstos de forma tão ampla que poderão deixar vulneráveis as pessoas que precisamente pretendem proteger. Ora, o requisito previsto é que a pessoa titular dos dados possa escolher alguém que, em seu nome, aceda aos dados de saúde sendo depois a autorização concedida automaticamente ou mediante pedido.

Propomos, por isso, uma redação que indique, por exemplo, quais as pessoas que podem ser escolhidas, que não se limite ao critério de “pessoa singular”, mas que tenha

em conta um título legal que fundamente a escolha, as condições sobre as quais esta pessoa poderá aceder aos dados, possíveis limitações na inserção de dados, etc (...). Esta situação também se aplicará aos menores, por serem incapazes, sendo os seus tutores responsáveis pelo acesso e controlo dos seus dados de saúde. Porém nem por isso se deixará de ter em conta as situações em que os interesses do menor possam ser distintos das intenções dos seus tutores, sendo permitido aos Estados-Membros assegurar as necessárias restrições. Teremos de tirar o chapéu à iniciativa e admitir e apoiar que esta aproximação dos titulares aos seus dados necessita de ser facilitada, no entanto cremos haver espaço para a criação de requisitos de forma garantir a segurança e defesa dos interesses destes.

Ao abrigo do art. 16.º do RGPD os titulares dos dados têm direito à retificação dos seus dados pessoais quando estes estejam inexatos ou incompletos, devendo tal correção ser feita pelo responsável pelo tratamento através de uma declaração adicional, se tal se mostrar necessário, consoante as finalidades do tratamento, e sem demora injustificada. Ora, a proposta de regulamento, no seu artigo 3.º, n.º 7, vem fazer referência a esse mesmo direito, no entanto vem adaptá-lo à retificação de dados de saúde. Assim como vimos no n.º 5 do artigo em análise, foi proposta a criação de serviços de acesso aos dados de saúde eletrónicos a diferentes níveis, devendo, de acordo com este n.º 7, ser esses mesmos serviços a garantir a retificação em linha desses dados. Porém, seguindo a lógica do art. 16.º do RGPD, quem assegura a retificação dos dados é o responsável pelo tratamento, mas, existindo estes serviços de acesso aos dados, haverá vários responsáveis pelo tratamento, assim como várias fontes e destinatários, quer a nível nacional, da União Europeia e internacional. O facto de tantas entidades terem acesso a estes dados, assim como à sua disponibilização, torna difícil averiguar qual o responsável pelo tratamento daqueles dados especificamente, pelo que seria interessante que, dentro desses serviços de acesso aos dados, existisse uma entidade destacada para esta atuação, sendo mais fácil rastrear os pedidos e a sua retificação e assim assegurar mais firmemente este direito. Com isto não queremos insinuar que esta não tenha sido a intenção do legislador, mas se estas questões não forem especificadas na lei poderão dar azo a que os direitos dos titulares fiquem fragilizados/lesados, por se deixar espaço para interpretações distintas pelas várias entidades envolvidas e ainda pelos próprios titulares, que não saberão como ou a quem se dirigir para este efeito.

O n.º 8 do artigo 3.º consagra uma das aplicações do direito da autodeterminação informacional do titular dos dados, permitindo que o titular possa escolher o destinatário

dos seus dados, facultando-lhe o acesso ou solicitando ao detentor dos seus dados que os transmita para o respetivo destinatário. E ainda, para além do destino dos dados, escolher que dados devem ser transmitidos, consoante a finalidade que lhes esteja destinada. O único entrave será a necessidade de esse destinatário ter de ser uma entidade parte do setor da saúde ou segurança social que esteja identificada no sistema.

Cabe-nos aqui fazer uma menção ao art. 20.º do RGPD que vem consagrar o direito de portabilidade dos dados. De acordo com este o titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir.

De ter em atenção que o artigo 9.º, n.º 1, do RGPD restringe o tratamento de dados de saúde, dados genéticos e biométricos exceto nas situações apresentadas no n.º 2, e que a proposta não faz uma ponte entre o n.º 8 em análise e o art. 9.º do RGPD. No entanto, também podemos colocar a hipótese de nestes casos estarmos perante um dos casos do art. 9.º, n.º 2, al. a), pelo facto de ter sido o próprio titular a solicitar ao destinatário dos dados aquele tratamento, consentindo assim com esta atuação.

Mesmo com este consentimento é relevante o n.º 4 do artigo 9.º do RGPD que refere que os Estados-Membros podem impor ou manter as condições previstas no artigo no que respeita nomeadamente a este tipo de dados (saúde, genéticos e biométricos).

Chegando ao fim do artigo 3.º, é de fazer menção tanto ao n.º 9 como ao n.º 10, que vêm conceder duas novas formas de poder aos titulares dos dados. O n.º 9, como já referimos anteriormente, vem conceder o poder de restringirem o acesso aos seus dados, querendo isto dizer que os profissionais de saúde, caso o titular assim o deseje, podem apenas ter acesso a uma quantidade de dados limitada. Claro que esta questão traz problemas, visto que ao não terem um acesso completo aos dados dos titulares, o seu trabalho pode ser comprometido, mas, por outro lado, deverá ser garantido pela proposta o estabelecimento de permissões de acesso diferenciadas, com base na segregação de funções e necessidade de conhecer aqueles dados pessoais para a prestação do serviço, tal como já está previsto no art. 29.º, n.º 7, al. a) da Lei n.º 58/2019, de 8 de Agosto, cumprindo assim com o princípio da minimização e o princípio “*need to know*”. Havendo esta diferenciação de acesso entre médicos, enfermeiros e outros técnicos, é possível assegurar um novo nível de proteção dos dados, deixando os titulares mais confiantes no sistema e não tão aptos a ocultar informações, já que tudo indica que estas

apenas serão visíveis pelos profissionais cujo aquele conhecimento será relevante.

Deixando uma nota sobre a utilização secundária de dados, parece compreensível que pacientes com determinadas condições (por exemplo: doentes oncológicos), não queiram que os seus dados e o seu registo clínico seja utilizado para fins de investigação, por uma questão de privacidade e apesar de estar em causa o interesse público, é necessário balancear e tentar harmonizar este com o interesse do titular dos dados.

Ainda um aspeto interessante a explorar, no âmbito deste direito, é a sua extensão, porque levanta a questão de saber até onde se poderá restringir o acesso. Será que o profissional de saúde consegue verificar que há dados a serem restringidos, ou quando olha para o perfil do seu paciente nem sequer sabe que há uma parcela de dados aos quais não têm acesso? Julgamos que, por razões de proteção dos interesses vitais do titular e ao abrigo do art. 9.º, n.º 2, al. h), o profissional de saúde, apesar de ser alertado que os dados aos quais está a tentar aceder foram sujeitos a uma restrição, poderá ter acesso a estes. Claro está que esse acesso “indevido” deve ser notificado ao titular que poderá solicitar uma justificação para a ocorrência, mas há uma falta de clareza na proposta quanto a este aspeto.

O n.º 10 vem permitir que os titulares dos dados consigam perceber quais os profissionais/entidades de saúde que tiveram acesso aos seus dados ou perfis. Cremos que a ideia por detrás desta norma seja a mesma existente no sistema português que estabelece que caso o titular bloqueie o acesso aos seus dados, se algum profissional aceder a estes, o titular será notificado do acesso através do e-mail ou telemóvel. No entanto, olhando para o texto da proposta o que transparece é que todos os titulares, independentemente de terem bloqueado o acesso ou não, devem receber esta informação. Assim, entendemos que a proposta poderia especificar as situações de alerta imediato em caso de acessos a dados que à partida estariam restritos, sem prejuízo de permitir aos titulares consultarem, a qualquer momento, um relatório automático de todos os acessos realizados.

Passando para o artigo 4.º, este vem apresentar algumas exceções às conclusões que acabámos de retirar do artigo 3.º, nomeadamente relativamente ao seu n.º 9. Este artigo vem regular o acesso dos profissionais de saúde aos dados de saúde dos titulares, esclarecendo que terão acesso aos dados de saúde eletrónicos dos seus pacientes independentemente do Estado-Membro ao qual aquele paciente esteja afiliado e ainda assegurando que os dados devem estar sempre atualizados, relativamente aos serviços prestados.

Em termos de tratamento dos pacientes compreende-se que seja necessário este acesso, aliás é precisamente com este objetivo em mente que este regime foi pensado, mas, é necessário frisar a importância do princípio da minimização dos dados estabelecido pelo RGPD. Como já vimos supra na definição deste princípio, os dados a tratar devem ser adequados, pertinentes e limitados, consoante o que é exigido por essa finalidade, não se tratando dados desnecessários, sob pena de estarmos perante uma contraordenação muito grave, sancionada nos termos da alínea a) do n.º 5 do artigo 83.º do RGPD<sup>42</sup>.

Assim sendo, há que considerar que este acesso aos dados de saúde dos titulares deve cumprir este princípio de forma estrita, especialmente por se tratar de dados de uma categoria tão sensível. O art. 9.º, n.º 2, al. h) permite o tratamento destes dados quando está em causa a prestação de cuidados médicos, mas consideramos que poderá haver aqui espaço para que o artigo 4.º da proposta limite um pouco mais este acesso, cingindo-se apenas às categorias de dados que sejam estritamente necessárias para *aquela* diagnóstico ou *aquela* prestação de cuidados de saúde, e porque o conhecimento desses dados é *o único meio de prestar aquele serviço*.

Para além da questão do conteúdo dos dados, o princípio da minimização é chamado pelo próprio artigo 4.º, no seu n.º 2, quando determina que nem todos os profissionais de saúde, leia-se, nem todas as categorias de profissionais, devem ter acesso aos mesmos tipos de dados de saúde eletrónicos, pelo que caberá aos Estados-Membros preverem essas limitações, consoante o seu juízo. Neste aspeto apenas referimos que esta possibilidade que é concedida aos Estados-Membros deveria ser estabelecida como uma obrigação, de forma que os direitos dos titulares e a sua privacidade ficassem verdadeiramente assegurados.

O n.º 4 deste artigo faz ainda uma ressalva no que toca aos dados de saúde eletrónicos, cujo acesso tenha sido impedido pelas pessoas singulares ao abrigo do artigo 3.º, n.º 9, da proposta. Relativamente a estes dados restritos, caso o tratamento daqueles dados seja necessário para proteger os interesses vitais do titular, então independentemente das restrições impostas, poderá o profissional de saúde ter acesso a esses dados, na condição que a pessoa singular seja depois informada que o acesso teve de ser concedido, reforçando assim o que dissemos supra sobre este tópico.

---

<sup>42</sup> Diário da República, Lexionário, “Princípio da minimização (tratamento de dados pessoais)”, consult. em 02/Abr/2024  
<https://diariodarepublica.pt/dr/lexionario/termo/principio-minimizacao-tratamento-dados-pessoais>.

Como vimos o artigo 20.º do RGPD fala do direito à portabilidade dos dados, no entanto por este direito estar munido de bastantes restrições, seja a primeira apenas se referir aos dados que são fornecidos pelo próprio titular, ou os que têm por base o consentimento ou um contrato, significa que os dados pessoais relativos à saúde, cujo consentimento deriva da lei, são excluídos. A proposta de regulamento do EEDS pretende evitar que esta seja a única solução, criando então um mecanismo de portabilidade de dados mais abrangente de forma a incluir e facilitar a portabilidade dos dados de saúde. O objetivo será que a transmissão de dados de saúde entre os diferentes prestadores de serviços seja facilitada, quer estejamos a falar de responsáveis pelo tratamento, públicos ou privados, e independentemente do fundamento jurídico que permita o tratamento daqueles dados de saúde eletrónicos.

No seguimento da prestação de serviços, pelos profissionais de saúde, os dados de saúde obtidos devem ser então registados por via eletrónica no sistema de RSE, vindo o artigo 7.º da proposta fazer referência aos requisitos necessários para este registo. Assim, mediante ato de execução a Comissão deverá definir as categorias de prestadores de cuidados de saúde que poderão registar os dados, quais as categorias de dados que deverão ser registadas sistematicamente e ainda quais os requisitos de qualidade dos dados a serem registados.

De acordo com o artigo 9.º, a gestão da identificação dos utilizadores dos serviços de acesso a dados de saúde pessoais caberá a um sistema eletrónico de identificação e autenticação dos utilizadores, entendendo nós que deverá existir neste sistema uma divisão entre os utilizadores comuns e os utilizadores enquanto profissionais de saúde. Quanto a estes últimos consideramos que o nível de autenticação deverá ser mais complexo, visto que os prestadores de cuidados de saúde, enquanto tal, necessitam de aceder a dados de várias outras pessoas e categorias.

O n.º 3 deste artigo faz também uma referência à interoperabilidade deste mecanismo de autenticação num contexto transfronteiriço, o que nos leva novamente à questão das garantias de proteção de dados nos diferentes Estados-Membros. Vivemos numa realidade em que os dados pessoais circulam de forma mais livre e são uma grande força impulsionadora da globalização, sendo uma nova espécie de “matéria-prima”<sup>43</sup>, no entanto a verdade é que não podemos negar a existência de diferentes níveis, isto é,

---

<sup>43</sup> KUNNER, Christopher, “European Data Privacy Law and Online Business”, 2003, p. ix. *apud* KONG, Lingjie, “Data Protection and Transborder Data Flow in the European Context”, in *European Journal of International Law*, 21 (2), 2010, pp. 442.

desigualdades de proteção nos diferentes países. Neste sentido temos que a União Europeia na Diretiva 95/56/CE, e agora no RGPD, veio estabelecer um regime rigoroso de transmissão e fluxo de dados para assegurar que o seu tratamento fosse realizado de forma segura pelos diferentes Estados-Membros.

O artigo 51.º do RGPD prevê a criação de autoridades de controlo, isto é, autoridades públicas independentes responsáveis pela fiscalização da aplicação do RGPD em representação das pessoas singulares e dos seus direitos e liberdades, no que toca ao tratamento dos seus dados. Dada a complexidade envolvida no ramo do tratamento de dados pessoais de saúde, seria impossível responder à procura derivada de reclamações neste tópico sem uma autoridade dedicada a exercer estas funções ao nível da saúde, que viesse garantir a aplicação do regulamento pensado na proposta. O artigo 10.º da proposta vem então estabelecer as condições de funcionamento da autoridade de saúde digital. Assim, esta autoridade será designada por cada Estado-Membro tendo como objetivo fiscalizar a aplicação deste regime a nível nacional, assegurando a aplicação dos direitos e obrigações estabelecidos por este, facilitando o acesso das pessoas singulares aos seus dados, em especial às pessoas com deficiências, supervisionando os diferentes pontos de contacto nacionais e reforçando a implementação da interoperabilidade dos dados de saúde para a fins de utilização primária, entre outros. É de frisar que com a criação desta autoridade não se pretende retirar a atenção das autoridades de controlo ao abrigo do RGPD, das autoridades competentes em matéria de cibersegurança e identificação eletrónica, ou do Grupo de Coordenação dos Dispositivos Médicos. Mas, entendemos que tendo as autoridades de controlo o dever primário de controlar a aplicação e harmonização do RGPD, esta autoridade de saúde digital funcionará a um nível mais específico, focando-se na aplicação deste futuro regulamento.

### 3.3. Os Sistemas de RSE

Cabe-nos fazer menção aos requisitos estabelecidos para os sistemas de RSE relacionados com a garantia da interoperabilidade dos dados e da segurança, segundo os requisitos estabelecidos no Anexo II à proposta. De acordo com estes, um sistema de RSE deverá ser concebido e desenvolvido de forma que preserve os direitos das pessoas singulares, de acordo com as finalidades previstas, e ainda, conseguindo ser utilizado

conjuntamente com outros produtos e dispositivos médicos, de modo fiável e seguro.

Quanto à interoperabilidade, deve o sistema permitir a partilha de dados de saúde eletrónicos pessoais entre profissionais e outras entidades do sistema de saúde, bem como com os utentes, conciliando os diferentes conjuntos de dados e sistemas.

No que toca à segurança, o sistema de RSE deve impedir o acesso não autorizado aos dados, e relativamente aos profissionais de saúde, configurar mecanismos de identificação e autenticação conforme as suas qualificações profissionais.

Causa alguma confusão o ponto 3.8 do Anexo II, dado que relativamente ao período de conservação dos dados, não nos dá uma resposta muito concreta, dizendo apenas que um sistema de RSE deverá ter em consideração os “diferentes períodos de conservação e direitos de acesso que tenham em conta as origens e as categorias dos dados de saúde eletrónicos”. Esta proposta não tem em conta a finalidade dos dados, e, portanto, não nos parece que esteja de acordo com o princípio da minimização dos dados.

### 3.4. Disposições Finais

Como referimos no início do nosso trabalho, não iremos apreciar a questão da utilização secundária dos dados, no entanto não deixaremos de fazer menção a alguns artigos presentes nos capítulos finais do regulamento, relevantes para as questões apresentadas anteriormente.

Assim, temos que o capítulo V, vem apresentar um conjunto de normas que pretendem regular a atividade dos Estados-Membros, no que toca aos seus esforços para o desenvolvimento do EEDS, assim como prever o acesso internacional a dados pessoais e não pessoais.

Como já mencionámos supra, a criação de um EEDS parece possível pelo facto de se conseguir garantir que existirá o respeito pela proteção de dados das pessoas no seu tratamento, caso que não é aplicável a países terceiros, por não estarem sujeitos a órgãos de fiscalização equivalentes aos previstos na legislação europeia<sup>44</sup>, sendo esta a

---

<sup>44</sup> Neste sentido ver os Acórdãos do Tribunal de Justiça (Grande Secção) de 8 de abril de 2014, *Digital Rights Ireland Ltd*, C-293/12 e C-594/12, EU:C:2014:238, n.º 69; e de 21 de dezembro de 2016, *Tele2 Sverige AB contra Postoch telestyrelsen e Secretary of State for the Home Department contra Tom Watson e o.*, C-203/15 e C-698/15, EU:C:2016:970, n.º 122.

maior preocupação no caso de dados sensíveis.

O capítulo VI sobre a governação e coordenação europeias, cria no seu artigo 64.º o Conselho do Espaço Europeu de Dados de Saúde, entidade esta com o objetivo de facilitar a cooperação entre as diferentes autoridades de saúde digital e os organismos responsáveis pelo acesso aos dados de saúde. Prevê ainda a composição deste Conselho, o seu modo de organização e funcionamento, assinalando que a sua presidência caberá à Comissão. No artigo 65.º são definidas as funções do Conselho relativamente à utilização primária e secundária dos dados, cabendo-lhes inclusive a função de partilhar informações e contribuições escritas sobre a aplicação do regulamento, bem como os riscos associados. Porém, esta norma não coordena as funções deste Conselho com as autoridades de proteção de dados como a AEPD e o CEPD.

Finalmente deixamos apenas duas notas quanto aos últimos capítulos. O capítulo VII prevê que a Comissão possa adotar atos delegados sobre o EEDS, tendo margem para alterar as disposições do regulamento, diminuindo, de certo modo, a independência dos Estados-Membros no que toca à definição das suas políticas de saúde.

Quanto à responsabilidade sobre a violação do regulamento e as sanções a aplicar, estas ficarão ao cargo dos Estados-Membros, devendo estes, consoante as suas políticas, decidir conformemente. Porém, consideramos que esta não seria a resposta que esperaríamos do regulamento, entendendo que quanto à questão da responsabilidade poderia estar previsto um mecanismo mais específico de aplicação uniforme, sob pena de causar insegurança jurídica no que toca à aplicação das regras impostas pela proposta.

## 4. CONCLUSÃO

No início do nosso trabalho apresentámos a Proposta de Regulamento relativo ao Espaço Europeu de Dados de Saúde, expondo as suas motivações e objetivos. Desde logo apontámos diversos problemas à concretização do EEDS, tendo analisado a proposta na perspetiva dos riscos que levanta e realizado a comparação entre esta e o RGPD, tecendo, a esse propósito, algumas considerações.

Considerámos os objetivos da proposta claros e que o seu regime vai ao encontro da necessidade de assegurar o acesso das pessoas singulares aos seus dados, aplicando vários mecanismos tais como a criação de serviços de acesso imediato e gratuito à informação, a possibilidade de restrição dos dados, o controlo sobre acessos ilícitos, a criação dos serviços de procuração e a mecanismos que garantam a inserção e retificação de dados.

Contudo, conseguimos perceber que, apesar desses objetivos estarem expostos no diploma, nem sempre estarão regulados da melhor forma possível, dado que ainda há bastantes incoerências e dúvidas às quais o diploma não responde.

Em especial, na articulação com o RGPD, a proposta remete para este diploma diversas vezes, no entanto ocasionalmente consegue contradizer o diploma ou mesmo restringir os direitos por este já assegurados, acreditamos nós não com essa intenção, mas pelo facto de se referir à maior parte dos tópicos de forma tão genérica, não estabelecendo critérios ou condições suficientes para muitos dos direitos cujo exercício pretende regular de forma especial.

Nos capítulos finais, procurámos uma resposta quanto aos mecanismos de controlo e fiscalização do EEDS, assim como a aplicação de sanções face à responsabilidade derivada da violação da aplicação do diploma. No entanto, mais uma vez, a solução apresentada, ao remeter para a regulação pelos Estados-Membros, cria alguma insegurança, por não criar um regime de aplicação uniforme na União Europeia.

Apesar de tudo podemos concluir aplaudindo a iniciativa e a proposta apresentada, entendendo que esta vem contemplar a maioria dos aspetos que careciam de regulamentação, e deixando a nota de que, com as necessárias especificações assinaladas, a proposta poderá complementar os diplomas já existentes, num domínio como o da saúde que carece deste suplemento.

## BIBLIOGRAFIA CONSULTADA

### i) Livros e artigos científicos

BYGRAVE, L. A., “Privacy in a Global Context – A Comparative Overview”, in *Scandinavian Studies in Law*, 47, 2004, pp. 320-348.

CASTRO, Catarina Sarmiento e, “40 anos de «Utilização da Informática» - O artigo 35.º da Constituição da República Portuguesa”, Vol. 3, N.º 3, E-pública: revista eletrónica de direito público, dezembro 2016

[<https://e-publica.pt/article/34442> – consult. em 02/Abr/2024].

CALABRICH, Bruno Freire de Carvalho, “O conceito de tratamento de dados pessoais e o acórdão Lindqvist, do Tribunal de Justiça da União Europeia”, in *R. Trib. Reg. Fed. 1a Região*, Brasília, DF, ano 31, n. 2, 2019.

CANOTILHO, J.J. Gomes; MOREIRA, Vital, “Constituição da República Portuguesa Anotada”, Vol. I, 4ª Edição, Coimbra, Coimbra Editora, 2014.

CORDEIRO, A. Barreto Menezes, “Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019” / coord. A. Barreto Menezes Cordeiro, Coimbra, Almedina, 2021.

CORDEIRO, A. Barreto Menezes, “Direito da proteção de dados: à luz do RGPD e da Lei nº 58/2019”, Coimbra, Almedina, 2020.

DRUEDAHL, L.C., Kälvemark Sporrang, S., “Patient Perspectives on Data Sharing”. In: Corrales Compagnucci, M., Minssen, T., Fenwick, M., Aboy, M., Liddell, K. (eds) *The Law and Ethics of Data Sharing in Health Sciences. Perspectives in Law, Business and Innovation*. Springer, Singapore, 2024.

GONÇALVES, Anabela Susana de Sousa, “O Consentimento como Fundamento de Licitude para o Tratamento de Dados Pessoais na União Europeia”, 2022.

GONÇALVES, Anabela Susana de Sousa, “O tratamento de dados pessoais no Regulamento geral de Proteção de Dados”, in *Scientia Iuridica*, n.º 350, maio/agosto 2019, pp. 179-18.

GONÇALVES, Anabela Susana de Sousa, “O Consentimento como Fundamento de Licitude para o Tratamento de Dados Pessoais na União Europeia”, in *10 anos de atuação na justiça militar: homenagem ao Ministro General de Exército Luis Carlos Gomes Mattos/Maria Elizabeth Guimarães Teixeira Rocha*, Flávio Henrique Albuquerque de Freitas (Coordenadores), Reginalda dos Santos de Melo da Cruz (Organizadora) – Brasília: Superior Tribunal Militar, Gabinete da Ministra Dra. Maria Elizabeth Guimarães Teixeira Rocha, Diretoria de Documentação e Gestão do Conhecimento, 2022. , pp. 51 – 60.

KIM J, Kim H, Bell E et al., Patient perspectives about decisions to share medical data and biospecimens for research. *JAMA Netw Open* 2(8):e199550, 2019.

KONG, Lingjie, “Data Protection and Transborder Data Flow in the European Context”, in *European Journal of International Law*, Vol. 21, N.º 2, 2010, pp. 441 – 456.

KUNNER, Christopher, “European Data Privacy Law and Online Business” (2003), p.ix.

SANYER O, Butler JM, Fortenberry K et al., Information sharing via electronic health records in team-based care: the patient perspective. 2021, *Fam Pract* 38(4):468–472, 2021.

## **ii) Outros documentos**

Deliberação n.º 984/2018 da Comissão Nacional da Proteção de Dados, Processo n.º 9932/2018, de 9 de outubro de 2018.

Grupo de Trabalho do Artigo 29º para a Proteção de Dados, Documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde electrónicos (RSE), 00323/07/PT WP 131, adotado em 15 de fevereiro de 2007.

Grupo de Trabalho do Artigo 29º para a Proteção de Dados, Parecer 4/2007 sobre o conceito de dados pessoais, 01248/07/PT WP 136, adotado em 20 de junho de 2007.

Grupo de Trabalho do Artigo 29º para a Proteção de Dados, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, adopted on 2 April 2013.

Parecer conjunto 03/2022 do CEPD e da AEPD sobre a proposta de regulamento relativo ao Espaço Europeu de Dados de Saúde, adotado em 12 de julho de 2022.

### **iii) Diplomas legais, decisões e recomendações da União Europeia**

Decisão n.º 1786/2002/CE do Parlamento Europeu e do Conselho, de 23 de setembro de 2002, que aprova um programa de ação comunitária no domínio da saúde pública (2003-2008).

Decisão de Execução (UE) 2019/1269 da Comissão, de 26 de julho de 2019, que altera a Decisão de Execução 2014/287/UE, que define critérios para a criação e avaliação de redes europeias de referência e dos seus membros, bem como para facilitar o intercâmbio de informações e experiências sobre a criação e avaliação das referidas redes (JO L 200 de 29.7.2019, p. 35).

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

Diretiva (UE) 2016/2102 do Parlamento Europeu e do Conselho, para as pessoas

com deficiência.

Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de Julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Directiva relativa à privacidade e às comunicações eletrónicas).

Recomendação (UE) 2019/243 da Comissão de 6 de fevereiro de 2019 relativa a um formato europeu de intercâmbio de registos de saúde eletrónicos.

Regulamento (CE) n.º 1338/2008 do Parlamento Europeu e do Conselho de 16 de Dezembro de 2008 relativo às estatísticas comunitárias sobre saúde pública e saúde e segurança no trabalho.

Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho de 23 de outubro de 2018 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE.

Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos, que altera a Diretiva 2001/83/CE, o Regulamento (CE)178/2002 e o Regulamento (CE) n.o 1223/2009 e que revoga as Diretivas 90/385/CEE e 93/42/CEE do Conselho.

Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento de Governação de Dados).

Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014,relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE.

Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho de 13 de

dezembro de 2023 relativo a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização e que altera o Regulamento (UE) 2017/2394 e a Diretiva (UE) 2020/1828.

Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao Espaço Europeu de Dados de Saúde, COM/2022/197 final,

<https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52022PC0197> ,  
consult. em 24/Fev/2024.

#### **iv) Decisões jurisprudenciais**

Acórdão do Tribunal de Justiça da União Europeia do Processo de Reenvio Prejudicial C-101/01, de 06 de novembro de 2003, “Acórdão Lindqvist”.

Acórdão do Tribunal de Justiça (Grande Secção) de 8 de abril de 2014, Digital Rights Ireland Ltd, C-293/12 e C-594/12, EU:C:2014:238, n.º 69.

Acórdão do Tribunal de Justiça (Grande Secção) de 21 de dezembro de 2016, Tele2 Sverige AB contra Postoch telestyrelsen e Secretary of State for the Home Department contra Tom Watson e o., C-203/15 e C-698/15, EU:C:2016:970, n.º 122.