Universidade do Minho
Escola de Direito

Yuri Rodrigues Ladeia

A PORTABILIDADE DE DADOS DE SAÚDE DENTRO E FORA DA UNIÃO EUROPEIA - DESAFIOS JURÍDICOS E TÉCNICOS NO ÂMBITO DA PROTEÇÃO DE DADOS

Julho de 2021

UMinho | 2021 Yuri Ladeia A PORTABILIDADE DE DADOS DE SAÚDE DENTRO E FORA DA UNIÃO EUROPEIA - DESAFIOS JURÍDICOS E TÉCNICOS NO ÂMBITO DA PROTEÇÃO DE DADOS

Universidade do Minho
Escola de Direito

Yuri Rodrigues Ladeia

A PORTABILIDADE DE DADOS DE SAÚDE DENTRO E FORA DA UNIÃO EUROPEIA - DESAFIOS JURÍDICOS E TÉCNICOS NO ÂMBITO DA PROTEÇÃO DE DADOS

Dissertação de Mestrado em
Direito e Informática

Trabalho efetuado sob a orientação da
Profª Doutora Teresa Alexandra Coelho Moreira

e do
Prof. Doutor José Machado

Julho de 2021

DECLARAÇÃO DE DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS

Este é um trabalho académico que pode ser utilizado por terceiros desde que respeitadas as regras e boas práticas internacionalmente aceites, no que concerne aos direitos de autor e direitos conexos.

Assim, o presente trabalho pode ser utilizado nos termos previstos na licença abaixo indicada.

Caso o utilizador necessite de permissão para poder fazer um uso do trabalho em condições não previstas no licenciamento indicado, deverá contactar o autor, através do RepositóriUM da Universidade do Minho.

Atribuição - Não Comercial - Com partilha Igual
CC BY-NC-SA

https://creativecommons.org/licenses/by-nc-sa/4.0/

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

DEDICATÓRIA

Aos meus queridos e amados pais, que com todo esforço e fé, desde a minha génese, apoiam-me incondicionalmente.

AGRADECIMENTOS

Aos meus orientadores, Professora Doutora Teresa Moreira e Professor Doutor José Machado, assim como à Dra. Ana Maria da Faculdade de Direito da Universidade do Minho, pela solidariedade, que de modo compreensivo ajustaram os seus compromissos e instruíram-me face aos meus desafios de conjugação académica e profissional, permitindo a concretização deste trabalho e o avanço para um próximo nível.

À Dra. Sónia Dória, minha mentora, que de modo sempre diligente, com o espírito de partilha e instigando-me aos desafios, tem dedicado, desde o início desta jornada na privacidade e proteção de dados, o seu conhecimento, consideração e tempo, permitindo-me evoluir apoiado pela sua orientação.

Aos meus pais por acompanharem-me e apoiarem-me sempre de perto, ainda que nesta fase de desafio estivéssemos fisicamente distantes.

A PORTABILIDADE DE DADOS DE SAÚDE DENTRO E FORA DA UNIÃO EUROPEIA - DESAFIOS JURÍDICOS E TÉCNICOS NO ÂMBITO DA PROTEÇÃO DE DADOS

RESUMO

Constituído por três capítulos, este trabalho teve como objetivo oferecer um ponto de vista técnico jurídico sobre o quadro de normalização atual do exercício do direito de portabilidade de dados de saúde, em um contexto de dentro e fora da União Europeia. Para o efeito, foram considerados os processos e medidas em prestação de cuidados de saúde e as respetivas necessidades operacionais, extraindo das mesmas o que implicaria na necessidade de um intercâmbio de dados de saúde, dentro e fora da União Europeia, considerando a proteção especial inerente aos mesmos e considerando alguns conceitos jurídicos diversos, mas com alguma intercessão, como o direito de acesso e de portabilidade. Foram observadas as medidas de interoperabilidade a nível nacional, continental Europeu e os desafios a nível transcontinental na saúde, tendo em conta a matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais face ao exercício do direito de portabilidade e o caráter normalizador global que a União Europeia tem assumido em matéria de interoperabilidade para o exercício do direito de portabilidade de dados ao abrigo do RGPD. Foram estudadas e buscadas soluções recorrendo à lógica de *Soft-law*, para alcançar uma normalização que não enfrentasse as limitações de aplicação geográfica aplicáveis às normas vinculadas a um ordenamento jurídico – *Hard-Law* no setor da saúde, buscando perceber se um *standard* de boas práticas para a portabilidade neste seguimento seria viável, aflorando ao final as soluções encontradas e as dificuldades pendentes de solução.

Palavras-chave: Quadro regulatório intercontinental para a portabilidade de dados; Cuidados de saúde transfronteiriços; Os Direitos dos titulares de dados; Regulamento Geral sobre a Proteção de Dados; Privacidade e Proteção de Dados.

HEALTH DATA PORTABILITY IN AND OUTSIDE THE EUROPEAN UNION - LEGAL AND TECHNICAL CHALLENGES IN DATA PROTECTION

ABSTRACT

Consisting of three chapters, this work aimed to provide a technical legal viewpoint on the current standardization framework of the right to health data portability, in a context within and outside the European Union. For this purpose, the processes and measures in health care provision and their respective operational needs were considered, extracting from them what would imply the need for an exchange of health data, inside and outside the European Union, considering the special protection inherent to them and considering some diverse but somewhat interrelated legal concepts, such as the right of access and portability. Interoperability measures at the national, continental European and transcontinental levels in health were observed, taking into account the matter of security architecture of networks and information systems regarding personal data in the face of exercising the right to portability and the global standardizing character that the European Union has assumed in matters of interoperability for the exercise of the right to data portability under the GDPR. Non-binding rules, as soft law, were studied in order to reach beyond the limitations of the scope of the regional legal system in the health sector, seeking to understand whether a standard of good practice for portability in this area would be feasible. At the end, the solutions found and the difficulties pending solution were highlighted.

Key-words: Intercontinental regulatory framework for data portability; Cross-border healthcare; The rights of data subjects; General Data Protection Regulation; Privacy and Data Protection.

ÍNDICE GERAL

LISTA DE ABREVIATURAS, SILGAS E ACRÓNIMOS

EU - União Europeia

RGPD - Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho

EEE - Espaço Económico Europeu

CEDH – Convenção Europeia dos Direitos do Homem

CNPD – Comissão Nacional de Proteção de Dados

CRP – Constituição da República Portuguesa

DPO – Data Protection Officer

DUDH – Declaração Universal dos Direitos Humanos

ONU – Organização das Nações Unidas

PIA – Privacy Impact Assessment

RGPD – Regulamento Geral Europeu de Proteção de Dados Pessoais

SNS – Serviço Nacional de Saúde

SPMS – Serviços Partilhados do Ministério da Saúde

TFUE – Tratado sobre o Funcionamento da União Europeia

TIC – Tecnologias da Informação e da Comunicação

UNESCO – Organização das Nações Unidas para a Educação, a Ciência e a Cultura

TFUE - Tratado sobre o Funcionamento da União Europeia

GAIC - Gabinete de Acesso à Informação Clínica

IA - Inteligência Artificial

G20 - Grupo dos 20

Mhealth - Mobile Health

GPS – Sistema de glocalização Global

XML 1.1 - Extensible Markup Language 1.1 (Second Edition)

API's - Interface de Programação de Aplicação,

MODO DE CITAR E OUTRAS CONVENÇÕES

No âmbito da normalização de referências bibliográficas o presente trabalho considera as referências bibliográficas de acordo com a norma *Chicago-Style.*

A citação no texto é uma forma abreviada de fazer referência no corpo de texto a conteúdo de outros autores.

No estilo Chicago Autor-Data, o formato da citação no texto é igual para todo o tipo de documentos: Inclui apenas os dois primeiros elementos da referência bibliográfica - o autor e o ano de publicação (sem qualquer pontuação), entre parênteses.

Cada citação no texto pode ser repetida as vezes que forem necessárias, e deve sempre corresponder a uma referência bibliográfica.

A bibliografia está ordenada por ordem alfabética do último apelido de cada um dos autores. Quando a autoria for da responsabilidade de até três autores, todos serão referenciados no cabeçalho da referência.

Quando a autoria for da responsabilidade de quatro ou mais autores, indica-se apenas o nome do primeiro, seguido da abreviatura **et al.** No caso de obras coletivas com indicação do nome do editor literário, compilador, organizador ou diretor, deve indicar-se o nome do editor ou compilador, seguido da expressão adequada: **ed.** ou **eds, org.**, ou **dir.**, conforme o caso.

INTRODUÇÃO

Os cuidados de saúde são uma matéria sensível e um domínio altamente regulamentado. Ao abrigo deste tema central encontram-se os desdobramentos jurídicos e técnicos relativos à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais de saúde e à livre circulação dos mesmos, sob os quais recaem um complexo quadro regulatório, que implica a desafiadora conjugação de requisitos legais, recursos de gestão e tecnologias, em especial sobre a matéria de interoperabilidade para a condução dos cuidados em saúde na era da informação, que ao abrigo do Regulamento Geral da Proteção de Dados (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 – RGPD, se concretiza como o Direito à Portabilidade, na forma do artigo 20..°.

A Portabilidade facilita a partilha de experiências de saúde, cuidados coordenados e investigação para entregar aos utentes os melhores resultados em tratamentos de saúde. Na forma do artigo 20..° do RGPD, consiste na possibilidade do titular dos dados, enquadrado ao abrigo do art. 4.°, n..°1 do RGPD, receber os dados pessoais que lhe digam respeito e que tenha fornecido a um Responsável pelo Tratamento, enquadrado na forma do artigo 4.°, n.º 7,.° do RGPD, num formato estruturado, de uso corrente e de leitura automática e o direito de transmitir esses dados a outro responsável pelo tratamento.

A portabilidade dos dados dos registos de saúde eletrónicos integrados sem falhas é uma necessidade contemporânea. Contudo, ainda não é uma realidade aplicável a todas as situações, apesar de o RGPD prever no seu considerando 68. ° que os Responsáveis pelo tratamento de Dados deverão ser encorajados a desenvolver formatos interoperáveis, de uso corrente, de leitura automática, que permitam a portabilidade dos dados, especialmente quando tal tratamento for automatizado. Isto porque a implementação de sistemas de dados de saúde ainda precisa de ultrapassar várias questões e limitações de interoperabilidade, usabilidade, ética, segurança e regulamentação geográfica para proporcionar os benefícios para atender às necessidades em saúde da atualidade, conforme Kouroubali e G. Katehakis (2019).

Ocorre que os Sistemas de Saúde são complexos e, nos seus circuitos para o trânsito da informação, participam de diversos Responsáveis Pelo Tratamento envolvidos na prestação dos cuidados. Estes são organizados em cuidados primários, secundários e terciários, os quais abordam o utente titular de dados, enquadrado na forma do artigo 4. °, n. °1, do RGPD, de formas diversas, uma vez que nos cuidados de saúde primários as doenças vão e vêm e os

doentes ficam. Nos cuidados de saúde secundários, as doenças ficam e os doentes vão e vêm, conforme defende Duarte (2014).

Devido a estas diferenças e complexidades, por vezes os utentes são acompanhados por partes e não como um todo, uma vez que não existe consciência da interdependência na prestação de cuidados, o que pressupõe a passagem do utente e dos respetivos dados por diversas entidades de saúde Responsáveis pelo Tratamento, nem sempre localizadas dentro do mesmo espaço geográfico e ordenamento jurídico, sujeitas às mesmas limitações e possibilidades de nível regulatório.

Apesar de ser necessário reduzir as disparidades a nível intercontinental para a interoperabilidade e, consequentemente, portabilidade de dados, é possível que nenhuma solução seja suficiente para normalizar e minimizar completamente tais desafios, de modo a se adequar a todas as circunstâncias. Contudo, observando a complexidade do quadro regulatório Europeu e Nacional a respeito da interoperabilidade dos dados de saúde e a proteção de dados pessoais, bem como outros ordenamentos jurídicos externos ao Espaço Económico Europeu – EEE, com a convicção de que este âmbito ainda pouco desenvolvido reveste uma certa novidade, ao longo deste trabalho, buscar-se-á encontrar algumas respostas ou hipóteses de respostas para traçar uma estratégia setorial no âmbito da saúde, para que as entidades consigam operacionalizar o exercício do Direito da Portabilidade de Dados dos seus respetivos titulares de dados, identificando o mais próximo de uma segurança jurídica e técnica, o que envolverá implicações práticas de conjugação multidisciplinar entre o Direito e a Informática, para apoiar a partilha de dados, abordando contextos regionais, nacionais e transfronteiriços.

CAPÍTULO I – ENQUADRAMENTO GERAL

1. A PRIVACIDADE E PROTEÇÃO DE DADOS NA EUROPA E A INFLUÊNCIA REGULATÓRIA EM PAÍSES TERCEIROS COMO *GLOBAL STANDARD*

O Direito da União, no qual se inclui a regulamentação sobre a proteção de dados dentro do EEE, se divide em direito primário e direito derivado. O primeiro concretiza-se em tratados e constituem a base jurídica para tomar todas as medidas da UE, ao passo que o segundo se concretiza por regulamentos, diretivas e decisões, decorrendo dos princípios e objetivos estabelecidos nos tratados, sendo a vertente de maior interesse para este trabalho.

As Diretivas, no âmbito do Direito da União Europeia, são atos legislativos que fixam um objetivo geral que todos os países da UE devem alcançar. Contudo, cabe a cada país elaborar a sua própria legislação para dar cumprimento a esse objetivo, transpondo a mesma em lei do direito nacional do estado membro. De outro lado, os regulamentos são atos legislativos vinculativos, aplicáveis em todos os seus elementos e em todos os países da UE, sendo este o caso do RGPD.

O direito à proteção dos dados pessoais é um direito fundamental e objetivo da União Europeia, pelo que foi consagrado na Carta dos Direitos Fundamentais da União Europeia do ano 2000, que dispõe na forma do artigo 8. ° sobre o Direito à proteção dos dados de caráter pessoal a todas as pessoas, devendo estes serem tratados de modo leal e com fundamento legítimo previsto legalmente, para fins específicos. Neste sentido, tal direito fundamental relaciona-se com o direito ao respeito da vida privada, consagrado no artigo 7. ° da mesma carta, conjugado com o previsto no artigo 16. °, n.º 1, do Tratado sobre o Funcionamento da União Europeia

Em um contexto histórico, em meados dos anos 1990, a Comunidade Europeia dotou-se de diversos instrumentos jurídicos com o objetivo de, em um primeiro momento, garantir a proteção dos dados pessoais no Espaço Económico Europeu – EEE, iniciando com a 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, adotada com base no artigo 100. °, A CE. Tal Diretiva, à época, constituiu o principal ato jurídico da União nesta matéria, estabelecendo condições gerais de

licitude do tratamento dos dados pessoais, bem como os direitos dos titulares de dados, os quais eram resguardados pelas autoridades de proteção de dados independentes e de controlo, instituídas nos Estados-Membros.

Em seguida, a Diretiva 2002/58/CE complementou a Diretiva 95/46/CE, no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas. Além disso, no âmbito do espaço de liberdade, segurança e justiça a Decisão-Quadro 2008/977/JAI regulamentou (até maio de 2018) a proteção dos dados pessoais no domínio da cooperação judiciária em matéria penal e policial.

Em 2016, a União Europeia procedeu à reforma do quadro jurídico geral nesta matéria e para o efeito, adotando o RGPD, que revoga, por exemplo, a Decisão-Quadro 2008/977/JAI e o principal ato legislativo anterior, a Diretiva 95/46/CE. Isto porque com a interoperabilidade crescente do Mercado Único Europeu e a crescente digitalização global, em especial na Europa, as inconsistências causadas em matéria de proteção de dados prejudicaram a circulação dos dados de um modo fluído, vez que ainda que no EEE, não estavam submetidos aos mesmos critérios, devido às particularidades de transposição da diretiva para o direito nacional dos estados membros, que o fizeram cada qual a sua maneira. Neste sentido, tornou-se necessário um ato legislativo vinculativo, aplicável em todos os seus elementos em todos os estados-membros, conforme a Direção da Investigação e Documentação do Tribunal de Justiça da União Europeia (2020).

Diante deste histórico, o quadro regulamentar em matéria de Proteção de dados da União Europeia – UE tem sido considerado como um padrão normalizador em todo o mundo, ao longo dos últimos 25 anos. Esta referência tem sido gerada pelo caráter precursor da União Europeia, que de modo primeiro tem estado na dianteira a regular sobre o assunto, assim como, de modo contemporâneo, devido à postura adotada pela Comissão Europeia ao determinar, com base no artigo 45..° do RGPD, a limitação à transferência de dados pessoais para um país terceiro ou uma organização internacional, condicionada à existência de uma decisão pela mesma de que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado, equivalente ao proporcionado no EEE.

Outra solução para a transferência de dados a países terceiros e não dotados de uma decisão de adequação são as Clausulas-Tipo de proteção de dados adotadas pela Comissão Europeia pelo procedimento de exame referido no artigo 93. °, n.º 2 e na forma do artigo 46.

° e 47. °do RGPD. Atualizadas em 04/06/2021, substituem as anteriores Cláusulas Contratuais-Tipo, na sequência do acórdão *Schrems II* do Tribunal de Justiça Europeu – TJE, que invalidou o *Privacy Shield UE-EUA* e exigiu que os exportadores e importadores de dados tomassem medidas para assegurar que as obrigações contratuais fossem efetivamente aplicadas.

Facto é que as cláusulas-tipo e as decisões de adequação, apesar de terem abordagens em vertentes diferentes, têm o objetivo comum de introduzir um elevado padrão de responsabilidade tanto para os importadores de dados como para os exportadores. No caso da primeira, busca-se a vinculação por um compromisso contratual e, na segunda, por obrigação legal, decorrente e vigente no ordenamento jurídico local.

A aplicação extraterritorial do regulamento, prevista no artigo 3..°, n..°2 do RGPD pretende salvaguardar o tratamento de dados pessoais de titulares de dados que se encontrem na União por um responsável ou subcontratante que não esteja estabelecido na União, desde que tal ofereça bens ou serviços a esses titulares de dados na União e/ou realize o controlo do seu comportamento, por exemplo. Isto significa dizer que, basta que a entidade ou país terceiro pretenda participar do mercado único europeu, direta ou indiretamente, tendo esta atividade lugar na união, estará submetido às regras em causa, na forma da explicação dos considerandos 23 e 24 do RGPD.

O artigo 3.º do RGPD pressupõe que o responsável pelo tratamento tem uma ligação substancial à UE, seja porque ali tem um estabelecimento ou porque trata os dados pessoais de titulares de dados neste território localizados, tendo as suas atividades direcionadas para os mesmos, no âmbito do mercado da UE, para a sua comunidade comercial. Desta forma, o nexo principal com o território da UE não é a presença de um responsável pelo tratamento ou de um subcontratante na mesma, mas sim a localização dos titulares de dados neste território, para os quais as atividades em causa (de oferta de produtos e serviço ou a monitorização de comportamentos) são direcionadas, conforme aduz Moniz (2018).

Assim, a abordagem do regulamento, na forma do artigo 3. ° e considerandos 23 e 25 sugere que é relevante para determinar a aplicação ou não do RGPD a avaliação de qual é a localização do titular de dados. Se for na União Europeia, seja este nacional, residente ou viajante temporário será aplicável, sendo indiferente a localização geográfica do responsável pelo tratamento.

Em decorrência da relevância do mercado único europeu em relação aos países

terceiros e a necessidade destes de acederem a à esta comunidade comercial, tendo como condição pretérita, estes submeteram-se indiretamente a nível de proteção de dados pessoais, por influência do Direito da União Europeia, à adoção de um quadro regulatório que ofereça garantias equivalentes. É exemplo deste fenómeno legislativo por influência transcontinental os Estados Unidos, que estão a aprovar uma nova legislação sobre privacidade, adequada às exigências europeias, após a revogação da Decisão de Adequação anteriormente concedida e invalidada pelo Tribunal de Justiça da União – TJUE, como resultado do recente acórdão "Schrems II", em 16 julho de 2020.

Outros exemplos são a Suíça, detentora de decisão de adequação desde 26 de julho de 2000, o Japão, com a Lei relativa à proteção de informações pessoais (Lei n.° 57, 2003), dotado de decisão de adequação concedida em e 23 de janeiro de 2019, bem como o Brasil, com a Lei Geral da Proteção de Dados – LGPD, Lei nº 13.709, de 14 de agosto de 2018, ainda não dotado de uma decisão de adequação,, nos termos do artigo 45.° do RGPD

A adoção de regimes semelhantes de privacidade e proteção de dados, em território internacional por países terceiros, demonstra a influência intercontinental dos padrões Europeus, que indiretamente, tem atingindo um alcance jurisdicional de efeito global, conforme Saunders e Reifman (2021), demonstrando, dentre outros fatores, um avanço a nível de normalização sobre a matéria, abrindo margem para a construção de um quadro transcontinental para fluxo de dados pessoais com garantias aos direitos e liberdades dos titulares de dados, apesar das limitações atuais, em benefício da interoperabilidade, que é de interesse para a portabilidade dos dados de saúde.

2. DADOS DE SAÚDE ENQUANTO DADOS PESSOAIS DE CATEGORIA ESPECIAL – AS LIMITAÇÕES E GARANTIAS PARA O TRATAMENTO

São dados pessoais aquelas informações relativas a uma pessoa singular identificada ou identificável, direta ou indiretamente, pessoa esta que é considerada titular dos dados, nos termos do artigo 4. °, n. °1 do RGPD. Diante desta definição geral, o quadro legislativo europeu em proteção de dados especifica um rol de dados de categoria especial, no qual se incluem as informações que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, o tratamento de dados genéticos, os

dados biométricos, dados relativos à vida sexual ou orientação sexual de uma pessoa e os dados de saúde, na forma do artigo 9..°, n.°1 do RGPD, este último de maior relevo para as reflexões deste ensaio.

Os dados pertencentes a esta categoria são considerados sensíveis pela influência direta e indireta nos direitos fundamentais dos titulares de dados. Os direitos fundamentais são as posições jurídicas básicas reconhecidas pelo direito português, europeu e internacional, com vista à defesa dos valores e interesses mais relevantes que assistem às pessoas singulares, independentemente da nacionalidade que tenham. Isto posto e considerando a obrigação do Estado de respeitar e concretizar os direitos fundamentais, quer através de leis, quer nos domínios administrativo e judicial, o RGPD, pelo Direito da União Europeia, buscou tutelar tais direitos em benefício das pessoas individuais, que em matéria de proteção de dados são considerados titulares de dados.

À luz da Constituição portuguesa de 1976, existem duas categorias de direitos fundamentais: os "direitos, liberdades e garantias" e os "direitos e deveres económicos, sociais e culturais". Para os primeiros são exemplos: o direito à liberdade e à segurança, à integridade física e moral, à propriedade privada, à participação política e à liberdade de expressão, a participar na administração da justiça, correspondem ao núcleo fundamental da vivência numa sociedade democrática. De outro lado estão os direitos económicos, sociais e culturais, a exemplo dos Direitos ao trabalho, à habitação, à segurança social, ao ambiente e à qualidade de vida.

Os mencionados Direitos Fundamentais, também previstos na supramencionada Carta dos Direitos Fundamentais da União Europeia, dependem da existência de condições para a sua concretização e não relativização e a categorização de tais dados como especiais pelo RGPD, à qual são inerentes as garantias aos titulares de dados, as obrigações acessórias e limitações impostas aos responsáveis pelo tratamento, contribui para concretização de tais condições. Isto porque o RGPD considera o tratamento não conforme de dados de categoria especial, pela sua sensibilidade e influência face aos direitos fundamentais, de gravidade elevada, uma vez que pode prejudicar os mencionados direitos e liberdades fundamentais de um titular de dados.

Neste sentido, apesar de o RGPD apenas categorizar os dados de categoria especial, entende-se que aqueles não incluídos neste rol são considerados dados pessoais "comuns". Importa esta distinção para destacar que, pela própria índole, os dados pessoais sensíveis,

carecem de proteção mais elevada, uma vez que da violação dos mesmos, na forma do n. ° 12 do artigo 4. ° do RGPD, podem surgir danos mais elevados para os direitos e liberdades fundamentais em comparação com a ocorrência da mesma hipótese com os dados de categoria "comum". Diante disso, as condições de licitude para tratar os dados comuns estão no artigo 6. ° do RGPD, ao passo que as exceções à proibição do tratamento de dados de categoria especial constam no artigo 9. ° do RGPD, de modo que ambos podem ou não se confundir.

Incluídos na definição de dados pessoais de categoria especial, nos termos do artigo 9. °, n.º 1 do RGPD, os dados de saúde, que são aqueles relacionados com a saúde física ou mental de uma pessoa singular, na forma do n.º 15 do artigo 4. ° do RGPD, só deverão ser objeto de tratamento quando tal for necessário para atingir os objetivos no interesse das pessoas singulares e da sociedade no seu todo, nomeadamente no contexto da gestão dos serviços e sistemas de saúde ou de ação social, assegurando a continuidade dos cuidados de saúde e da prestação de cuidados de saúde transfronteiras, para fins de segurança, monitorização e alerta em matéria de saúde, para fins de arquivo de interesse público, investigação científica ou histórica, para fins estatísticos baseados no direito da União ou dos Estados-Membros e que têm de cumprir um objetivo, assim como para os estudos realizados no interesse público no domínio da saúde pública, na forma do considerando 53 do RGPD.

Diante da sensibilidade, conforme acima colocado, as possibilidades de tratamento dos dados de saúde são limitadas, uma vez que os permissivos para o fazer são exceções à proibição, desde que atendidas a algumas das hipóteses constantes nas alíneas do n. ° 2 do artigo 9. ° do RGPD. Estas limitações e exceções às limitações na forma de hipóteses a serem atendidas possibilitam condições harmonizadas para o tratamento de categorias especiais de dados pessoais relativos à saúde, tendo em conta necessidades específicas.

Neste sentido, o n. º 4 do artigo 9. ° do RGPD permite que os Estados-Membros mantenham ou imponham novas condições, incluindo limitações, no que respeita ao tratamento de dados relativos à saúde, o que em Portugal verifica-se, dentre outras legislações, na Lei n.º 58/2019 de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do RPGD. Tal constatação está concretizada na forma do artigo 29. °, n. °1 da referida lei, que condiciona o acesso aos dados de saúde à ponderação à luz do princípio da necessidade de conhecer a informação, de modo que se tal acesso precisa ser efetuado por um profissional que deve estar obrigado ao dever de sigilo e de confidencialidade, devendo ser garantidas medidas adequadas de segurança da informação nesta interação.

Diante dos riscos aos Direitos e Liberdades dos Titulares de Dados que os tratamentos de dados pessoais de categoria sensível podem acarretar, a exemplo dos dados de saúde, os mesmos mereceram uma proteção mais elevada na nível regulatório, que necessita de intervenção técnica em certa medida, de modo que tais dados especiais só deverão ser objeto de tratamento quando tal for necessário para atingir os objetivos no interesse das pessoas singulares e da sociedade no seu todo.

3. O QUADRO TÉCNICO NACIONAL NORMALIZADO EM MATÉRIA DE ARQUITETURA DE SEGURANÇA DAS REDES E SISTEMAS DE INFORMAÇÃO RELATIVOS A DADOS PESSOAIS E O EXERCÍCIO DO DIREITO DE PORTABILIDADE DE DADOS EM SAÚDE

Por força do que exige o artigo 32..° relativo à segurança do tratamento dos dados em conjugação com o n.º 4 do artigo 9..° do RGPD , relativo à possibilidade dos estados-membros da União Europeia imporem condições sobre tratamento de dados de saúde, o estado Português regulou sobre o tema, na forma do artigo 29..°, n.°.1 da Lei n.º 58/2019 de 8 de agosto, que estabeleceu que nos tratamentos de dados de saúde, o acesso a dados pessoais reger-se-á pelo princípio da necessidade de conhecer a informação. Neste sentido, o mesmo artigo 29..°, no n. º 7 estabelece que as medidas e os requisitos técnicos mínimos de segurança inerentes ao tratamento de dados a que alude o n.º 1 acima mencionado são aprovados por portaria dos membros do Governo responsáveis pelas áreas da saúde e da justiça, que na forma das alíneas A,B e C, deve regulamentar, nomeadamente, as seguintes matérias: Estabelecimento de permissões de acesso aos dados pessoais diferenciados, em razão da necessidade de conhecer e da segregação de funções, Requisitos de autenticação prévia de quem acede, Registo eletrónico dos acessos e dos dados acedidos.

No mesmo esteio, o n. °2 do artigo 32. ° da lei nacional n.º 58/2019 de 8 de agosto aduz que, no âmbito das bases de dados ou registos centralizados de saúde estas devem preencher os requisitos de segurança e de inviolabilidade previstos no RGPD. Diante da exigência e liberdade regulatória concedida, o estado Português, no âmbito da administração pública, procedeu à revisão do Regulamento Nacional de Interoperabilidade Digital, através da Resolução do Conselho de Ministros n.º 2/2018.

A referida Resolução urge proceder à revisão do Regulamento aprovado

pela Resolução do Conselho de Ministros n.º 91/2012, de 8 de novembro, no que se refere às especificações técnicas e formatos digitais a adotar pela Administração Pública. A alteração atende à premissa de que a utilização de formatos abertos (não proprietários) é imprescindível para assegurar a interoperabilidade técnica e semântica, em termos globais, dentro da Administração Pública, na interação com o cidadão e titular de dados ou a empresa e para disponibilização de conteúdos e serviços, criando a necessária independência dos fornecedores ou soluções de *software* adotadas.

Em cumprimento do disposto no n.º 4 do artigo 5.º da Lei n.º 36/2011, de 21 de junho, o projeto de Regulamento foi publicado a 5 de outubro de 2015, que aprovado pela mencionada resolução, assenta prioritariamente em especificações técnicas e formatos digitais definidos e mantidos por organismos internacionais e está dividido em especificações técnicas e formatos digitais obrigatórios e recomendados, de modo que o incumprimento das especificações técnicas e formatos digitais obrigatórios tem, para fins de contratação pública, as consequências previstas no artigo 9.º da Lei n.º 36/2011, de 21 de junho, relativamente à nulidade dos atos de contratação promovido pela Administração Pública que incorram no incumprimento.

As especificações técnicas e formatos digitais recomendados pelas referidas normas portuguesas são orientações que constituem boas práticas, ajustadas com o que instrui o Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho, que regula sobre as especificações técnicas com as quais os atuais ou futuros produtos, processos de produção ou serviços para a compatibilidade e a interoperabilidade com outros produtos ou sistemas, bem como alinhados com o artigo 199.°,alínea g) da Constituição, o Conselho de Ministros, no âmbito das competências administrativas do Governo para o desenvolvimento económico-social e à satisfação das necessidades coletivas, na qual se inclui a proteção de dados pessoais, resolveu, dentre outros temas de interesse menor para a Portabilidade de Dados:

(I) Alterar o Regulamento Nacional de Interoperabilidade Digital;

(II) Estabelecer que as entidades, serviços e organismos abrangidos pelo âmbito de aplicação do Regulamento estão obrigados a cumprir as especificações técnicas e formatos digitais obrigatórios e a procurar seguir as especificações técnicas e formatos digitais recomendados de acordo com a respetiva classificação, nos termos definidos na Lei n.º 36/2011, de 21 de junho;

(III) Determinar que a implementação, licenciamento ou evolução de sistemas informáticos tem obrigatoriamente de considerar o disposto no Regulamento, em cumprimento do disposto no n.º 1 do artigo 4.º da Lei n.º 36/2011, de 21 de junho.

Para o Direito da Portabilidade de Dados Pessoais as definições relevantes são aquelas relativas ás normalizações dos Formatos de documentos estruturados, na forma do n.º 4 alíneas b e h do Regulamento Nacional de Interoperabilidade Digital, podendo as especificações técnicas e formatos digitais adotados classificarem-se como obrigatório ou recomendado, nos termos do n.º 5 do mesmo Regulamento. É exemplo da normalização, com efeito para a Portabilidade de Dados, o domínio de tecnologia de interface *web* a Linguagem para descrição de documentos e formatação de dados, para interpretação não humana, na especificação técnica *Extensible Markup Language 1.1 (Second Edition)* - XML 1.1, de caráter obrigatório.

No mesmo esteio, a Resolução do Conselho de Ministros n.º 41/2018, que define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais, observado o reforço da proteção jurídica dos direitos dos titulares dos dados imposto pelo RGPD, buscou atender às novas regras e procedimentos do ponto de vista tecnológico. A referida Resolução reconhecendo que a tecnologia e o Direito estão espelhados nos princípios da proteção de dados desde a conceção e por defeito, ao abrigo do artigo 25.º do RGPD e nas medidas adequadas para garantir a segurança do tratamento, ao abrigo do artigo 32.º do RGPD.

Para o exercício Direito ao à Portabilidade de Dados, consagrado no artigo 20.º do RGPD é reconhecido que é necessário a implementação de tecnologias de informação que utilizem formatos interoperáveis, sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia, motivo pelo que o Governo Português definiu orientações técnicas para a Administração Pública, recomendando-as ao setor empresarial do Estado, em matéria de arquitetura de segurança das redes e sistemas de informação e procedimentos a adotar de modo a cumprir as normas do RGPD. É exemplo para a normalização técnica o requisito geral de caráter obrigatório, oriundo da Resolução do Conselho de Ministros n.º 41/2018, a necessidade de as tecnologias de informação permitirem a portabilidade e a exportação de dados pessoais, através das seguintes medidas específicas:

(I) garantindo a utilização de formatos digitais compatíveis, que assegurem a interoperabilidade técnica e semântica dentro da Administração Pública, na interação com o cidadão ou com a empresa e para disponibilização de conteúdos e serviços;

(II) adotando as especificações técnicas e formatos digitais definidos no Regulamento Nacional de Interoperabilidade Digital, aprovado pela Resolução do Conselho de Ministros n.º 91/2012, ou noutro que o venha a substituir.

Diante destas definições, apesar das exigências limitarem-se ao âmbito da administração pública, ainda que reste como desafio uma normalização específica para o setor privado, é razoável dizer que a exigência no âmbito público gerará influência indireta no âmbito privado. Isto porque a interação destes com o público é inevitável, a exemplo daquelas que recorrem da prestação serviço e fornecimento de bens, seja na forma de soluções informáticas a nível de *software* ou suporte em *hardware* ao serviço publico nacional de saúde, o que fará com que, por força dos quadro regulatório estabelecido, as ofertas de soluções estejam conformidade com tais requisitos desde a conceção e por padrão, criando algo como um *gold standard* a nível da Arquitetura de segurança das redes e sistemas de informação, naquilo que tange à proteção de dados pessoais.

Finalmente, importa mencionar que na Saúde, a nível mundial, as especificações padrões abertas em informática em saúde, que descrevem o gerenciamento e armazenamento, recuperação e troca de dados de saúde em registros eletrônicos de saúde, OpenEHR e o HL7 FHIR são referências a nível de interoperabilidade e e-*health / m-health*, detentoras das seguintes características que justificam esta afirmação, segundo Machado (2021):

A. são especificações "*open-source*";
B. facilitam a gestão, o armazenamento, a recuperação e a troca de informações clínicas:
C. são standards para a interoperabilidade semântica;
D. são um passo importante para a interoperabilidade conceitual, fundamental para o desenvolvimento de soluções inteligentes;
E. FHIR e HL7 são capazes de "co-habitar" tirando partido da versatilidade de cada um;
F. o "*querying*" é assegurando por APIs que utilizam JSON em vez de XML (neste

momento XML pode ser considerado obsoleto).

Considerando que é necessário haver integração do serviço publico de saúde com o privado, para garantir uma cada vez maior e mais eficaz interoperabilidade e reduzir custos e desdobramentos indesejados causados pela não normalização, é possível que ambos caminhem no mesmo sentido, tendo como linha guia o *Gold Standard* estabelecido pela administração pública.

CAPÍTULO II – A INTERSEÇÃO E CONJUGAÇÃO DOS CONCEITOS JURÍDICOS RELEVANTES PARA O DIREITO DE PORTABILIDADE DE DADOS

1. OS DIREITOS DOS TITULARES DE DADOS – PORTABILIDADE DOS DADOS E ACESSO: A CONJUGAÇÃO DE DOIS DIREITOS DIVERSOS E CONEXOS – AS TRANSFERÊNCIAS DE DADOS ENTRE RESPONSÁVEIS PELO TRATAMENTO

A digitalização da vida em sociedade tem tomado proporções elevadas, de modo que a evolução tecnológica tem causado relevante alteração na dinâmica social, tornando-se um fator de extremo relevo para o desenvolvimento econômico, ambiental e social para o contexto global, conforme Belluzzo (2019). Atualmente, a sociedade move-se em torno do digital, uma vez que é cada vez mais notório que as tecnologias e as medias dominam os espaços importantes e essenciais no atual modelo de sociabilidade que configuram os âmbitos da sociedade, tais como: comércio, política, entretenimento, relacionamentos, informações, serviços e outros desdobramentos emergentes.

Deste modo, os resultados provenientes da digitalização fazem-se presentes no cotidiano das pessoas enquanto titulares de dados, uma vez que o combustível para mover a locomotiva da tecnologia são dados enquanto género, do qual decorre a espécie dados pessoais, que nesta tempestade de novas demandas e possibilidades para pessoas individuais e coletivas, na era da economia informacional, tem sido tratado em alto volume, por diversos responsáveis pelo tratamento, em diversos territórios e para variadas finalidades, o que incrementou a dispersão da informação pessoal dificultando, na prática, as possibilidades de conhecimento e controlo do seu titular. Logo, o imperativo da proteção de dados pessoais tem sido, justamente, assegurar esse conhecimento e controlo, conforme Canto Moniz (2018).

No sentido de munir o titular de dados de uma espécie instrumento manejador que permitisse, em alguma medida, manejar os seus dados pessoais tratados por outrem, o RGPD buscou outorgar tal faculdade através dos chamados direitos dos titulares de dados, previstos desde o artigo 12..° ao 22..° e 34..° do RGPD. Tal faculdade, assim como todo o RGPD, é assistida por uma abordagem tecnicamente neutra, ou seja, independente das técnicas utilizadas, desde que com as mesmas consiga-se chegar ao objetivo, que é o

exercício dos direitos dos titulares de dados, na forma do considerando 15 do RGPD.

Dentre tais Direitos, dois são de mais relevo para este ensaio, nomeadamente o Direito de Acesso, previsto no art. 15.° do RGPD, e o Direito de Portabilidade, previsto no artigo 20..° do RGPD. O primeiro permite o titular dos dados obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe dizem respeito são ou não objeto de tratamento e acede-los, assim como às informações relativas ao seu tratamento. O segundo permite o titular de dados receber os dados pessoais que lhe dizem 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, quando o tratamento de dados for baseado no consentimento enquanto condição de licitude e execeção à limitação do tratamento de dados de categoria especial nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a) do RGPD, ou ainda, quando necessário para execução de um contrato do qual o titular de dados faz parte nos termos do artigo 6.º, n.º 1, alínea b) do RGPD. O mesmo direito se aplica quando o tratamento de dados for realizado por meios automatizados.

Diante das definições e os desdobramentos práticos, é tênue a linha que separa ambos os direitos que, apesar de diversos, confundem-se em certa medida. Isto porque o ato de "aceder" aos inerente ao Direito de acesso, na forma do n.°1 do artigo 15..° do RGPD também pode ser verificado na possibilidade de o titular de dados "receber" os próprios dados pelo Direito de Portabilidade, na forma do artigo 20.° n.°1 do RGPD, uma vez que em ambos os casos trataria-se de "tomar conhecimento" dos dados que lhe dizem respeito.

Ao abrigo do Direito de Acesso o titular de dados poderá obter uma cópia dos dados pessoais em fase de tratamento, que se for pedida por meio eletrónica, pelo mesmo meio deverá ser fornecida, num formato eletrónico de uso corrente, na forma do n.°3 do artigo 15.° do RGPD. De outro lado, ao abrigo do Direito de Portabilidade, semelhante ao direito de acesso, 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, de modo semelhante à forma do direito de acesso, com a adição de que o formato deve ser de leitura automática, nos termos do n.°1 do artigo 20.° do RGPD.

O Direito de Acesso é satisfeito quando o titular de dados toma conhecimento de que dados pessoais que lhe digam respeito são ou não objeto de tratamento perante a um responsável pelo tratamento, através do fornecimento de uma cópia dos dados pessoais em

causa, sendo esta a extenção e limite do seu exercício. Uma vez os dados sob guarda do titular dos dados, este tem a liberalidade de enviálos, à sua conta, a quem pretender, inclusive pra outro responsável pelo tratamento, que caso o faça, na forma do desenho aqui colocado, após o fornecmento dos dados pelo responsável pelo tratamento inicial, este não terá implicações de resposnabildiade pela transferência.

Ocorre que no direito de portabilidade, além da abordagem acima colocada, a qual é satisfeita com a entrega dos dados ou com o conhecimento sobre os mesmos pelo seu titular, o circuito de interações continua com a possibilidade de os dados pessoais serem transmitidos diretamente entre responsáveis pelo tratamento em favor do titular dos dados, sempre que tal seja tecnicamente possível, na forma do n.° 2 do artigo 20.° do RGPD, sendo este o fator diferencial entre os direitos supracitados.

Portanto, um dos fatores diferenciais encontra-se na extensão dos direitos, que para a portabildiade é mais alargada com a possiblidade de transferência dos dados entre responsáveis pelo tratamento e em favor e a pedido do titular dos dados, enquanto para o acesso o exercicio do direito é satisfeito quando ao mesmo são fornecidos os dados e informações acessórias ao mesmo. Outro fator de diferença é a finaldiade da transferência dos dados pessoais a outro responsável pelo tratamento, previstas nas hipóteses do n.°2 do artigo 15 do RGPD e do n.° 3 do artigo 20.° do RGPD, de modo que a primeira é feita por iniciativa do Responsável pelo tratamento diante dos seus interesses e na condução da sua operação legítima, com a qual o titular dos dados envolve-se, ao passo que na hipótese segunda a transferência é feita a pedido e em função do titular dos dados, o qual é operacionalizado pelo responsável pelo tratamento.

Sinalizada as diferenças, uma das semelhanças leva a discussões que extrapolam o âmbito jurídico da proteção de dados e demanda uma abordagem organizacional e tecnológica, no sentido de normalização, que é o desafio maior em matéria de portabilidade de dados no âmbito da proteção de dados. O tema controverso e carente de solução em causa é a definição de qual é o “formato estruturado de uso corrente” ideal para o fornecimento e transferência dos dados no âmbito da saúde dentro do espaço económico europeu e a partir desta para países terceiros? Quais são os desafios técnicos para a satisfação desta obrigação jurídica? As respostas a estas perguntas e outras, tentarão ser dadas nos números adiante.

2. TRANSFERÊNCIA, TRANSMISSÃO E PORTABILIDADE DE DADOS – A RELAÇÃO DOS CONCEITOS PARA A PROTEÇÃO DE DADOS;

O exercício do Direito de Portabilidade de Dados pode se concretizar através de duas maneiras: a primeira através do recebimento dos dados pessoais do titular de dados a que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, ao abrigo do artigo 20.° , n. ° 1 do RGPD. A segunda forma seria através da transmissão direta entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível, nos termos do n. ° 2 do artigo 20. ° do RGPD.

A transmissão configura uma modalidade de tratamento de dados nos termos do n. ° 2 do artigo 4. ° do RGPD, que pode em alguma medida ser confundida com o conceito de transferência de dados, uma vez que ambos se tratam de um intercâmbio de dados. A nomenclatura "transmissão" é mencionada no sentido e em referência a um intercambio de dados pessoais, nos considerandos 48 e 50, no artigo 4.° n.°2 do RGPD e nos artigo 8.° , n.°2, artigo 23.° n.°2 e artigo 29.°, n.º 3 da Lei Portuguesa de n.º 58/2019 de 8 de agosto, que assegura a execução, na ordem jurídica nacional do RGPD. No mesmo sentido a nomenclatura "transferência" é referida nos artigos 22.°, 37.°, n.°1, al. J, 25.°, al. K da Lei Portuguesa de n.º 58/2019 de 8 de agosto e nos considerandos 101, 102, 107, 112, 153 e artigos 15.° , n.°2, 40.° , n. ° 2 al. J, 44.° , 45.°, 49.° , n.°1 , 70.° , n.°1 al. J, 85.° , n.°2, 88.°, n.°2, 96.°, 97.° , n.°2, al. A do RGPD.

A diferença das nomenclaturas está no contexto e no sentido a que maioritariamente foram aplicadas e a que finalidade se referem. Enquanto a "transmissão" é utilizada em um contexto que maioritariamente se refere a um intercambio de dados dentro do EEE, a "transferência" é utilizada maioritariamente em um contexto em que a norma buscou dizer respeito ao intercâmbio de dados para países terceiros à UE. Na hipótese de diferenciação entre os conceitos, a "transferência", sendo um intercambio de dados para fora do EEE, implicará na necessidade de um nível de segurança mais elevado que aquela aplicável à "transmissão", aplicando medidas técnicas, organizativas e jurídicas suficientes para o efeito, ao abrigo do capítulo V do RPGD, sobre as transferências de dados pessoais para países terceiros ou organizações internacionais.

Apesar da diferença presumida mas não explicita pelos atos legislativos em proteção de dados, nacional e Europeu, é prudente dizer que o intercambio de dados para o exercício

da portabilidade de dados nos moldes do n.°2 do artigo 20.° do RGPD, mesmo estando sob a nomenclatura "transferência", também se refere a interações entre responsáveis pelo tratamento dentro e fora do EEE, uma vez que o exercício enquanto do direito do titular de dados, pode pressupor as duas possibilidades, que devem ser consideradas e apreciadas justificadamente, sob pena de restrição injustificada dos direitos e liberdades do titular, salvo se justificadamente impedido por ser tecnicamente impossível. Neste caso, o exercício do direito seria redirecionado daquilo que se deseja para aquilo que é possível, na forma da entrega do ficheiro estruturado ao titular dos dados, para que o próprio realize as transferências que lhe interessarem aos responsáveis de tratamento que pretender, diretamente, dentro e fora da EEE, entretanto, sem a vinculação nestas atividades posteriores do responsável pelo tratamento inicial.

CAPÍTULO III – OS DESAFIOS TECNICOS E JURÍDICOS PARA A PORTABILIDADE DOS DADOS PESSOAIS DENTRO E FORA DA UNIÃO EUROPEIA

1. SAÚDE EM LINHA – A INTEROPERABILIDADE EM SISTEMAS DE SAÚDE E A RELEVÂNCIA DOS DADOS NO SETOR DA SAÚDE;

A transformação digital é realidade na Sociedade em geral e nas Organizações em particular, com as tecnologias emergentes a potenciarem um conjunto de oportunidades de satisfação das necessidades, na forma de otimização dos recursos disponíveis e dos riscos relacionados. A otimização tem possibilitado um crescimento considerável tanto da oferta, pelo lado dos prestadores de serviços, como da procura, por parte dos utentes, de produtos e serviços tecnológicos e digitais no setor da saúde, segundo os Serviços Partilhados do Ministério da Saúde, E. P. E. (2017).

Em saúde, a desmaterialização dos processos, a digitalização do acesso à informação e a introdução de novas tecnologias associadas à prestação de cuidados médicos constituem fator importante e determinante no contexto do circuito clínico de um doente e da dinâmica clínica a nível nacional, continental e intercontinental, uma vez que o tratamento de saúde é baseado em registos, que cada vez mais passam a ser digitais. Além da otimização e benefícios mencionados, trazem preocupações e cuidados acessórios a respeito da segurança, privacidade e proteção dos dados dos utentes, em particular dos dados de saúde e informação clínica, motivo pelo que o assunto foi regulado pelo RGPD.

Uma das *Key Actions* do programa *Shaping Europe's Digital Future*, de iniciativa do Directorate-General for Communications Networks, Content and Technology of European Commission, envolve a promoção de registos de saúde electrónicos baseados em um formato de intercâmbio europeu comum, de modo a possibilitar aos cidadãos europeus o acesso e o intercâmbio de dados de saúde em toda a EU, por forma munir a saúde europeia um espaço de dados de ampla acessibilidade, segura, protegendo os dados de saúde ,que permitindo um direccionamento e uma maior rapidez na investigação, diagnóstico e tratamento em saúde, a partir de 2022, segundo a Comissão Europeia (2020). É justamente este o ponto de equilíbrio que se busca para tornar a portabiliade de dados do artigo 20.° do RGPD exequível, a nível nacional, transnacional e intercontinental.

Neste contexto, em matéria de portabilidade de dados, a digitalização com o avanço informático e a necessidade de conjugação com as normas de proteção de dados, levou à duvida de como normalizar processos e metodologias à forma das normas de proteção de dados vigente em cada ordenamento jurídico, sem prejuízo do melhor interesse na continuidade da prestação dos cuidados em saúde, o que tem implicado na pergunta: como as Organizações a nível do setor da saúde nacional, continental e intercontinental passarão a operacionalizar, com tais variáveis, entre outros assuntos de interesse para a matéria, os métodos para a portabilidade de dados pessoais? A persecução destas respostas tem como passo intermediário, a interoperabilidade e os desafios da mesma nos níveis acima mencionados, encontrando questões de compatibilidade técnica e regulatória para ajuste de boas práticas.

As Tecnologias da informação e comunicação são de utilidade transversal no serviços de saúde, que para haver a interoperabilidade necessária é preciso considerar as Entidades públicas prestadoras de cuidados de saúde, da administração direta e indireta, assim como do setor público empresarial, designadamente: (i) os agrupamentos de centros de saúde; (ii) os estabelecimentos hospitalares, independentemente da sua designação e natureza jurídica (As Entidades de saúde e centros hospitalares tanto do setor público administrativo como do setor público empresarial); e (iii) as unidades locais de saúde, isto a nível nacional, segundo os Serviços Partilhados do Ministério da Saúde, E. P. E. (2017).

A nível internacional, a interoperabilidade em linha, no setor público e privado encontra os mesmos desafios, entretanto, em um nível ainda mais profundo, caminho que a nível europeu tem sido perseguido pela comissão europeia em suas estratégias.

2. A INTEROPERABILIDADE A NÍVEL EUROPEU

Para colaborar com a interoperabilidade em linha e transfronteiriça em cuidados de saúde, surgiram alguns projetos, a exemplo de: PHArA-ON - que cria “um conjunto de plataformas abertas interoperáveis integradas e elevadamente customizadas” para impactar na população europeia envelhecida20; o Smart4Health - que cria um sistema de intercâmbio de registos médicos eletrónicos, centrado no cidadão, para estimular cuidados de saúde personalizados; o InteropEHRate - que visa promover a interoperabilidade dos registos

médicos eletrónicos, mediada pelo paciente, e que, perante a sua autorização, poderá acarretar uma interoperabilidade transfronteiriça entre os registos médicos e as aplicações de investigação científica; o ASSESS CT - que tem em vista "contribuir para uma melhor interoperabilidade semântica nos serviços de e-Saúde na Europa"; o e-Standards - que "avança uma interoperabilidade na e-Saúde e um alinhamento global dos padrões", conformeAbreu (2020)

No domínio da saúde, a Diretiva 2011/24/UE do Parlamento Europeu e do Conselho estabelece um quadro para facilitar o acesso a cuidados de saúde transfronteiriços seguros e de elevada qualidade. Concretamente, essa diretiva criou a rede de saúde em linha para dar resposta à questão da interoperabilidade entre os sistemas de saúde eletrónicos. A rede de saúde em linha pode adotar orientações sobre o conjunto mínimo de dados que deverão ser objeto de intercâmbio transfronteiriço em caso de prestação de cuidados de saúde imprevistos e de emergência e em caso de prescrição eletrónica de serviços transfronteiriços, segundo o Parlamento Europeu (2015).

Considerando a sensibilidade dos dados de saúde e a necessidade de comunicação transfronteiriça, conjugando a disposição do RGPD acima colocadas e os termos do n.º 1 do artigo 168. ° do Tratado sobre o Funcionamento da União Europeia (TFUE), deve ser assegurado um elevado nível de proteção da saúde na definição e execução de todas as políticas e ações da União Europeia. Nos termos do considerando 50 da respetiva diretiva, os Estados-Membros ficaram incumbidos de facilitar a cooperação entre os prestadores de cuidados de saúde, os utentes e os reguladores dos diferentes Estados-Membros, a nível nacional, regional ou local, identificando a forma mais eficiente de organizar os serviços de saúde para a prestação continuada desses nos diferentes Estados-Membros.

Essa cooperação pode incluir o planeamento conjunto, o reconhecimento mútuo ou a adaptação de procedimentos ou normas, a interoperabilidade dos respetivos sistemas nacionais de tecnologias de informação e comunicação (TIC), mecanismos práticos que assegurem a continuidade dos cuidados de saúde ou medidas que facilitem na prática a prestação, por profissionais de saúde, de cuidados de saúde transfronteiriços numa base temporária ou ocasional.

Ocorre que o considerando 56 da mesma diretiva indica que a implantação de sistemas de TIC no domínio da saúde é inteiramente da competência nacional, ao passo que o considerando 57 aduz que a interoperabilidade dos serviços de saúde em linha deverá ser

feita no respeito das legislações nacionais relativas aos serviços de prestação de cuidados de saúde adotadas tendo em vista a proteção dos doentes. Neste caso, considerando que a diretiva de 2011 é anterior ao RGPD de 2018, estão incluídas as exigências do mesmo para a interoperabilidade em saúde, na forma da portabilidade de dados do artigo 20. ° do RGPD, enquanto Direito do Titular de Dados.

Ocorre que a concretização da interoperabilidade tratada na Diretiva 2011/24/EU, pela natureza deste ato legislativo no Direito da União Europeia, poderia ser feita, conforme mencionado acima, à definição nacional dos estados membros, o que cria disparidades na interação entre os mesmos em alguma medida. Com o advento do Regulamento Geral da Proteção de Dados, pela natureza deste ato legislativo, a integração uniforme das normas é uma pedra de toque para a matéria de proteção de dados, dentro do EEE, para o seu funcionamento.

Logo, por consequência, pensar em portabilidade de dados pessoais de saúde, é indiretamente pensar em interoperabilidade entre sistemas de saúde. Deste modo, a execução prática e conforme dos dois conceitos, leva a conjugação entre a liberdade que dá a diretiva na implementação da interoperabilidade versus a necessidade de uniformização do regulamento, em matéria de portabilidade de dados pessoais, além da necessidade fundamental de um padrão aceito internacionalmente para que seja possível a interação tecnicamente célere e fiável a este nível, independente da exigência jurídica.

Sendo função da Comissão Europeia defender os interesses gerais da UE, mediante a apresentação de propostas legislativas e a execução da legislação, das políticas e do orçamento da EU, a partir da qual surgiram as respetivas diretivas e regulamentos, a nível europeu entre os estados membros e face à países terceiros, esta deveria emitir orientações e definições uniformizadas para os Estados-Membros promoverem a portabilidade, através de medidas técnicas de interoperabilidade, à semelhança do que faz nos termos do artigo 45.° do RGPD, relativamente às decisões de adequação para transferência de dados para países terceiros, de modo a evitar divergências jurídicas que conduzam a interoperabilidade ou inviabilidade técnicas em prejuízo do exercício dos direitos dos titulares, em respeito ao primado do Estado de direito e direitos humanos e liberdades fundamentais, no âmbito da saúde em linha.

A rede de saúde em linha precisa considerar a necessidade de uniformização, pilar fundamental do RGPD, na forma do artigo 14.°, n.°2 A da Diretiva 2011/24/EU, na criação de

sistemas e serviços de saúde em linha e aplicações interoperáveis, que proporcionem vantagens económicas e sociais sustentáveis, com vista a alcançar um elevado nível de confiança e segurança, reforçar a continuidade dos cuidados e assegurar o acesso a cuidados de saúde seguros e de elevada qualidade, que pode se desdobrar na definição de formato de ficheiro e/ou sistemas de informações fiáveis para a comunicação, incluindo o setor publico e privado.

A nível Europeu uma série de barreiras e riscos associados exigem consideração além dos desafios dos âmbitos técnico e jurídico, a exemplo da literacia, da alfabetização do cidadão para o exercício do direito de portabilidade, face à saúde em linha, de modo a que possa ser utilizada adequadamente por todos àqueles a quem se destinam a tutela da proteção de dados pessoais.

A nível da União Europeia, o serviço público nacional tem caminhado cada vez mais para ultrapassar as fronteiras nacionais, por forma a estarem interconectados com serviços idênticos ao nível da UE, contribuindo assim para o mercado único digital. Para tal, tem sido trabalhada uma abordagem coordenada, a todos os níveis: quanto a legislação, quando as administrações públicas e seus processos administrativos, quanto as informações e os sistemas de informação para executar serviços públicos. Neste esteio, um dos maiores flagelos a combater neste âmbito, relativamente à portabilidade e interoperabilidade, é a fragmentação digital, uma vez que que compromete a oferta de serviços públicos conectados em toda a UE.

Neste nível continental do bloco económico europeu, os serviços públicos nacionais devem estar ligados e ultrapassar as fronteiras nacionais, por forma a estarem interconectados com serviços idênticos ao nível da UE, contribuindo assim para o mercado único digital. Para tal, tem sido perseguida uma abordagem coordenada, a todos os níveis, relativamente a legislação, organização dos processos públicos administrativos e soluções em sistemas de informação, com objetivo de limitar e evitar a fragmentação digital, que pode comprometer a oferta de serviços públicos conectados em toda a EU.

Se comprometido ou inviabilizado o exercício do direito de portabilidade, estarão violados os direitos fundamentais do cidadão enquanto titular de dados, em prejuízo das garantias estabelecidas na Carta dos Direitos Fundamentais da União Europeia pelo artigo 8 .° em conjugação com o previsto no artigo 1.° , n.°1 do TFUE, no que respeita ao Direito à proteção dos dados de caráter pessoal.

Desta forma, a capacidade das entidades diversas interagirem para a persecução de objetivos comuns, definidos em comum alinhamento, implicando a partilha de informações e conhecimentos entre si, no âmbito de processos a que dão apoio, mediante o intercâmbio de dados entre os respetivos sistemas de TIC, aferindo o impacto e os riscos desta interação para os utentes titulares de dados face à manipulação de dados pessoais de natureza especial, sem observar o padrão em vigor na União Europeia, é o desafio da construção do ambiente técnico propício para o exercício do direito à portabilidade de dados em um contexto internacional dentro do EEE.

3. A INTEROPERABILIDADE DOS DADOS DE SAÚDE PARA FORA DO EEE - DESAFIOS DE ARTICULAÇÃO TÉCNICA E JURÍDICA

A economia dos dados é a aposta da estratégia de União Europeia Digital, considerando que os grandes volumes de dados oferecem oportunidades de fomentar o desenvolvimento de modelos governamentais e empresariais inovadores e competitivos, incluindo soluções a nível da saúde, ao mesmo tempo que primar por respeitar o quadro da UE sobre a proteção de dados, uma vez que pode implicar riscos e desafios consideráveis, nomeadamente no que diz respeito aos direitos fundamentais (incluindo a privacidade e a proteção de dados), segundo o Parlamento Europeu (2016).

A nível global, atualmente, não existe uma estrutura internacional de proteção de dados consolidada e de comum normalização, apesar dos esforços de diversos países terceiros à união europeia nivelarem a regulação do tema com base no *gold standard europeu*. O surgimento da proteção de dados no âmbito nacional, no continente europeu, ao ocorreu entre o final dos anos 1960 até os anos 1980, através de legislações que buscaram dar algum controlo ao titular de dados sobre as suas informações utilizadas por agencias governamentais e grandes corporações privadas, figurando nesta gênesis A Áustria, a Dinamarca, a França, a República Federal da Alemanha, o Luxemburgo, a Noruega e a Suécia, chegando à maturidade jurídica, que levou, àquela época, a três países europeus, incorporarem a proteção de dados como um direito fundamental na Constituição, nomeadamente a Espanha, Portugal e Áustria, segundo Rudgard (2012).

Importa mencionar que, de modo pioneiro, Portugal consagrou no artigo 35° da carta

magna, desde 1976, o direito à proteção de dados pessoais, em uma época em que o tema era pouco difundido e as tecnologias ainda eram maoritariamente analógicas. Estabelecendo condições aplicáveis ao tratamento automatizado, conexão, transmissão e utilização dos dados, teve foco na utilização informática, que na atualidade passou a contribuir e integrar o quadro regulamentar em matéria de proteção de dados pessoais, estando ainda as disposições pertinentes e aplicáveis contemporaneamente ao avanço tecnológico.

Na arena europeia, o Conselho da Europa adotou as Resoluções 73/22 e 74/29, que foram seguidas pelo surgimento da Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de carácter pessoal pelo Conselho da Europa, em 1981. Outra iniciativa notável no mesmo período foram as diretrizes da Organização para a Cooperação e Desenvolvimento Econômico – OCDE, sobre a proteção da privacidade e fluxos transfronteiriços de dados pessoais, de 1980, que estabelecem as regras básicas que regem os fluxos de dados transfronteiriços e a proteção de informações pessoais e privacidade, a fim de facilitar a harmonização da legislação de proteção de dados entre os países. Posteriormente, a Diretiva 95/46/CE foi aprovada em 1995, para corrigir divergências entre os diferentes regimes de proteção de dados, constituída no trabalho anterior em relação à Convenção 108 e estabeleceu o primeiro o padrão normalizador internacional de proteção de dados. Este padrão foi agora delineado no mais alto nível de normalização a nível europeu, através do RGPD, embora a proteção de dados também tenha começado a evoluir em outras ordens jurídicas, uma vez que as diferenças entre esses regimes e o do RGPD são fatores de menor interoperabilidade e maior disparidade, o que impossibilita a portabilidade de dados.

Outras ordens jurídicas regionais não oferecem atualmente um nível comparável de proteção de dados ao encontrado na cultura jurídica europeia, onde uma espessa camada de proteção de dados existe há décadas. Apesar disto, esforços notáveis em regiões e países terceiros à UE foram realizados, a exemplo do trabalho na área de proteção de dados realizado pela *Organization of American States* – OAS, incluindo a adoção de princípios para promover a proteção de dados na região. Na União Africana, foi criada a *African Union Convention on Cyber Security and Personal Data Protection*, com o objetivo de promover a proteção dos direitos humanos na região africana e que, portanto, em certa medida, pode ser comparada ao que foi feito pelo Conselho da Europa.

Apesar disto, ainda é necessário a nível intercontinental a colaboração entre estados para normalização, conforme preconiza Slokenberga (2018).

Tendo em conta a necessidade de interação com países terceiros em todos este níveis, no que respeita à saúde, a exemplo da necessidade de um titular de dados dar continuidade do seu tratamento em saúde em um país terceiro, os seus dados produzidos no EEE por um serviço de saúde europeu, independente da nacionalidade do titular de dados, podendo este ser seguido a nível do tratamento médico em outra instituição, sendo essa possibilidade garantida por um direito, que são posições jurídicas básicas reconhecidas pelo direito português, europeu e internacional, com vista à defesa dos valores e interesses mais relevantes que assistem às pessoas singulares, independentemente da nacionalidade que tenham.

Neste sentido, a União Europeia poderia cooperar com países terceiros para promover projetos de interesse comum e assegurar a interoperabilidade das redes, promover a cooperação em matéria de desenvolvimento tecnológico, na forma do n.º 3 do artigo 171. ° e artigo 180. ° al. B do TFUE, entretanto, a nível específico da portabilidade de dados em saúde, não há uma definição exata para o efeito, havendo apenas disposições esparsas que permitem em alguma medida desenhar o quadro de limites, possibilidades e fragilidades para o exercício deste direito tutelado, entretanto, não plenamente operacionalizado para exercício.

No mesmo sentido, ao abrigo do artigo 50. °, al. A e D do RGPD, relativamente à cooperação internacional no domínio da proteção de dados pessoais, em relação a países terceiros e a organizações internacionais, a Comissão Europeia e as autoridades de controlo podem tomar as medidas necessárias para estabelecer regras internacionais de cooperação destinadas a facilitar a aplicação efetiva da legislação em matéria de proteção de dados pessoais, promovendo Promover o intercâmbio e a documentação da legislação e das práticas em matéria de proteção de dados pessoais, nomeadamente no que diz respeito a conflitos jurisdicionais com países terceiros, o que é extremamente útil a nível da portabilidade de dados para fora do EEE.

Juridicamente, a portabilidade de dados de saúde, enquanto categoria especial, para fora da união europeia, na forma do artigo 9.°, n.°1 e 20.°, n.°2 do RGPD, encontra pouca estrutura para a sua concretização diante atual quadro técnico pouco normalizado assim como impedimentos a nível regulatório a nível global, ainda que o titular de dados tenha o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, considerando a ausência contemporânea de um formato de intercâmbio

transfronteiriço comum, bem como de medidas para a transmissão fiável, torna-se tecnicamente e juridicamente impossível. Isto porque também há que se conjugar as disposições do capítulo V do RGPD, relativamente as transferências de dados pessoais para países terceiros ou organizações internacionais, nomeadamente as disposições para assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento nesta interação, conforme o artigo 44.° do RGPD.

O exercício da portabilidade de dados na forma do artigo 20.°, n.°2 do RGPD para uma entidade fora do EEE, a pedido do titular dos dados, configura uma transferência de dados para um país terceiro, que pode ocorrer em conformidade de algumas formas: com base numa decisão de adequação, na forma do artigo 45.° do RGPD ou sujeita ao compromisso contratual, extensivo das garantias de proteção de dados europeia em ordenamento jurídico diverso, na forma das Cláusulas-tipo de proteção de dados adotadas pela Comissão Europeia, na forma do artigo 46.° do RGPD. Alternativamente, na falta de uma destas hipóteses, a transferência pode ser efetivada através 49.° do RGPD, que apresenta derrogações para situações específicas, que no contexto da prestação de cuidados em saúde, aplicam-se as hipóteses das alíneas A, B do n.°1 do referido artigo (quando o titular dos dados tiver explicitamente dado o seu consentimento à transferência prevista, após ter sido informado dos possíveis riscos de tais transferências para si próprio devido à falta de uma decisão de adequação e das garantias adequadas, quando a transferência for necessária para proteger interesses vitais do titular dos dados ou de outras pessoas, se esse titular estiver física ou legalmente incapaz de dar o seu consentimento), conjugando com os requisitos de informação ao titular de dados previstos nos artigos 13.° e 14.° do RGPD.

Apesar da matéria pressupor um nível o máximo de normalização possível, de modo a evitar inconsistências e diferenças que impeçam o exercício prático do direito, o n. ° 5 do artigo 49.° do RGPD aduz que na ausência de uma decisão de adequação, os estados membros da UE podem estabelecer expressamente limites à transferência de categorias específicas de dados para países terceiros ou organizações internacionais, o que se feito cada um à sua maneira, poderá levar a incompatibilidades e diferenças na execução do direito entre os estados-membros, à semelhança da dificuldade de normalização existente com a Diretiva 95/46/CE pela natureza não uniformizadora deste ato legislativo, na contramão da natureza do Regulamento, enquanto ato legislativo do Direito da União Europeia.

Diante das dificuldades de garantir segurança do tratamento na transferência de

dados para países terceiros, na forma do artigo 32.°do RGPD, enquanto meio para efetivar o direito de portabilidade de dados de saúde, é uma saída o titular dos dados apenas 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, conforme o artigo 20.°, n.°1 do RGPD. Desta maneira e modo independente, sem a intermediação dos responsáveis pelo tratamento, presentes e externos ao EEE, o titular de dados cederia os dados à entidade que lhe interessa.

Apesar de ser uma alternativa que pode remediar a ausência de definições e técnicas normalizadas para a segurança jurídica e informática de uma transferência, ainda restará pendente a articulação para a definição do formato estruturado, de uso corrente e de leitura automática, que caso não definido, poderá colocar em causa a efetividade do exercício do direito, posto que, caso a entidade de destino não consiga dar a destinação destes dados para os fins que o utente titular dos dados pretende, por incompatibilidade técnica, ainda que a jurídica esteja superada, todos os esforços ficarão sem efeito, em prejuízo do titular de dados pessoais.

Em Portugal, pela faculdade concedida pelo RGPD aos estados-membros de definirem os limites para a portabilidade, através do artigo 18. ° n.°1 a 3 da lei n.º 58/2019 de 8 de agosto, para solucionar a dificuldade da conceção de um formato universal, foi definido, de modo tecnicamente neutro, que a portabilidade dos dados deve, sempre que possível, ter lugar em formato aberto.

Apesar de lúcida a definição da lei Portuguesa, no sentido de mitigar as diversas complicações a nível de definição do formato, especialmente pelos entraves que isto geraria a nível transcontinental, ainda assim, naquilo que for a hipótese de transferência de dados para o exercício da portabilidade, entre responsáveis pelo tratamento, sendo um destes externo ao EEE, para garantir a segurança nesta interação, o setor da saúde poderia definir a melhor prática neste sentido, sendo esta uma abordagem mais prudente, mas que ainda demandará bastante articulação.

4. OS DESAFIOS TÉCNICOS INFORMÁTICOS DE UNIFORMIZAÇÃO REGIONAL E INTERNACIONAL DE UM FORMATO DE USO CORRENTE PARA PORTABILIDADE DOS DADOS DE SAÚDE;

A regulação da proteção de dados pessoais tem origem em atos legislativos e, no caso da União Europeia concretiza-se com o RGPD, que em síntese normaliza as obrigações jurídicas sobre o tema a nível europeu, orienta sobre quais são os limites que um Tratamento de Dados Pessoais deve respeitar, orienta sobre quais são as hipóteses permitidas para tratar dados pessoais, indica os critérios que os métodos para tratar dados pessoais devem observar, de modo tecnicamente neutro, orienta sobre as implicações de responsabilidade e o dever de promover segurança a que está sujeito quem trata dados pessoais, determina coimas e punições a quem trata dados pessoais em caso de violação de Direitos e liberdades dos titulares de dados e confere direitos aos titulares face ao tratamento a que os seus dados forem submetidos por um responsável pelo tratamento, segundo Ladeia (2020).

Para operacionalizar e concretizar algumas das exigências jurídicas relacionadas com a proteção de dados, as matérias informática e segurança da informação figuram como pilar fundamental para a conformidade. A segurança da informação e a informática, para efeitos da proteção de dados, tem utilidade enquanto métodos técnicos e organizacionais de um conjunto de requisitos, processos e controlos, que tem por objetivo mitigar e gerir adequadamente o risco de uma organização a nível da informação/dados, sendo peça componente do *Puzzle* de Conformidade com a proteção de dados pessoais e parte dos requisitos para a aplicar, a nível prático, a conformidade com o RGPD, que aliadas às exigências e medidas jurídicas (tais como acordos/contratos/registos e *reports*) compõe o quadro de conformidade, conforme aduz Ladeia (2020).

Importa destacar que, para a informática no âmbito da segurança da informação, são de interesse todos tipos de dados/informações, inclusive os dados pessoais (relacionando com o RGPD), incluindo as informações não pessoais (sem relação com o RGPD, a exemplo de um contrato puramente comercial), entretanto, neste trabalho terá lugar aquilo que se relaciona com a proteção de dados pessoais.

Nesse sentido, a definição e normalização do formato estruturado, de uso corrente e de leitura automática, referido no artigo 20. °, n.°1 do RGPD para o efeito da Portabilidade de Dados Pessoais, além de necessitar de articulação jurídica para sua concretização, é um desafio de interoperabilidade informática. Desafio este que tem a complexidade agravada considerando a abrangência nacional, internacional e intercontinental de normalização que é preciso atingir, afim de tutelar os Direitos do titular que teve os seus dados tratados no EEE

e deseja que os mesmos o acompanhem em sua mobilidade geográfica, considerando a melhor prática para os setores publico e privado. Isto porque no na saúde, é elevado o número de Sistemas de Informação presentes nas instituições regionais, internacionais e intercontinentais, divergindo em matéria de especificidade e utilidade, o que leva a um problema severo relacionado às integrações entre os mesmos, conforme Loureiro e Nogueira (2019).

A portabilidade de dados pessoais enquanto definição e exigência jurídica, desdobra em medidas técnicas e organizacionais informáticas para ser concretizada, que no contexto da saúde, em diversos níveis geográficos, requer uma visão interorganizacional, com definição das estruturas e mecanismos de governação e rastreabilidade, protocolos de colaboração e partilha de dados, em especial quando trata-se do exercício do direito de portabilidade ao abrigo do n.°2 do artigo 20 do RGPD, que pressupõe que os dados pessoais podem ser transmitidos diretamente entre os responsáveis pelo tratamento.

Para dar dimensão do que a viabilidade do Direito de Portabilidade necessita considerar e superar, são pertinentes as menções às *nuances* que compõem o conceito de interoperabilidade, que informaticamente podem ser definidas como a habilidade de transferir e utilizar informações de maneira uniforme e eficiente entre várias organizações e sistemas de informação, tecnologicamente diferentes, operando em contextos organizacionais distintos. Neste esteio, a interoperabilidade pode ser dividia em alguns tipos:

- Tecnológica, que consiste, em ligação dos sistemas e serviços de informática, que permitem os sistemas e dispositivos trocarem dados com fiabilidade e sem custos acrescidos. Para isto, os aspetos da interoperabilidade devem incluir especificações de interface, serviços de interconexão, serviços de integração de dados, apresentação com troca de dados e protocolos de comunicação seguros.
- Semântica, que é definida como uma garantia de que o significado preciso da informação trocada é compreensível, com um nível de arquitetura informacional transversal, para que os dados e informações trocados sejam preservados e compreendidos ao longo das trocas entre as partes.
- Organizacional, baseada na definição de objetivos de atividades, modelagem de processos de negócios, que permita as entidades relacionadas que alinhem os seus processos de negócio, responsabilidades e expetativas para alcançar objetivos

comuns, aceites e mutuamente benéficos, atendendo aos anseios da comunidade de utilizadores, disponibilizando serviços facilmente identificáveis, acessíveis e focados no utilizador.

- Legal, que é definida como ponto agregador para a legislação ao nível nacional e europeu, de forma a garantir que as organizações que operam sob diferentes marcos legais, políticos e estratégicos possam trabalhar juntas, conforme Almeida (2019).

Isto posto, a estrutura de interação consiste nas relações entre os tipos acima. Baseia-se na interoperabilidade tecnológica, que inclui aplicação e infraestrutura que conectam sistemas e serviços. Na mesma linha, a função da interoperabilidade semântica é garantir que os dados fornecidos por esses serviços não sejam mal interpretados ou confundidos, garantindo que o significado dos dados seja retido e compreendido por qualquer outra aplicação. A partir desse tipo de interação, o modelo de negócios de organizações com objetivos comuns e benefícios mútuos pode ser ajustado por meio da troca de informações / dados (interoperabilidade organizacional). Na vanguarda está a interoperabilidade jurídica, que normaliza as regras para a troca de informações entre organizações, sendo esse o caso do RGPD.

A nível nacional, em Portugal, a portabilidade no poder público encontra amparo regulatório na Lei n.º 36/2011, de 21 de junho, que estabelece a adoção de normas abertas nos sistemas informáticos do Estado e atribui à Agência de Modernização Administrativa a elaboração do Regulamento Nacional de Interoperabilidade Digital, concretizado pela Resolução do Conselho de Ministros n.º 91/2012 e atualizado pela Resolução do Conselho de Ministros n.º 2/2018, que nas respetivas tabelas I a V anexas define as especificações técnicas e formatos digitais a adotar pela Administração Pública, obedecendo as especificações europeias elencadas no Regulamento (UE) n.º 1025/2012, do Parlamento Europeu e do Conselho, de 25 de outubro de 2012. Dentre as definições estão abrangidos desde o Formato de dados, Formato de documentos, Tecnologias de interface web, Protocolos de *streaming*, Protocolos de correio eletrónico, Sistemas de informação geográfica, Especificações técnicas e protocolos de comunicação em redes informáticas, Especificações técnicas de segurança para redes, serviços, aplicações e documentos a Especificações técnicas e protocolos de integração, troca de dados e orquestração de processos de negócio na integração interorganismos.

Lucidamente, tais normas reconhecem que a utilização de formatos abertos é imprescindível para assegurar a interoperabilidade técnica e semântica, em termos globais, na interação com o cidadão/titular dos dados e para a disponibilização de conteúdos e serviços, para o que é necessário a independência dos fornecedores ou soluções de *software* adotadas. O Regulamento, alinhado com as diretrizes europeias em termos de interoperabilidade, contribui para a universalidade de acesso e utilização da informação, para a preservação dos documentos eletrónicos e para uma redução de custos de licenciamento de *software*, conforme a Presidência de Conselho de Ministros (2012), o que é pertinente para efeitos para a portabilidade de dados em saúde, que além dos desafios da administração publica, encontra a necessidade de ser útil da mesma forma no setor privado.

É um exemplo de normalização a nível continental da utilização de um formato aberto no setor da saúde o certificado COVID-19. O certificado tem por objetivo facilitar a livre circulação dos cidadãos na EU, de modo que o mesmo será introduzido nos Estados-Membros da EU, que poderão emiti-lo e utiliza-lo a partir de 1 de julho de 2021, segundo a Comissão Europeia (2021). Os esforços centralizados pela Comissão reuniram as autoridades nacionais responsáveis pela saúde em linha de daca estado membro, na preparação da interoperabilidade dos certificados de vacinação, para a criação do Certificado Verde Digital, regulado, à época deste ensaio, pelo acordo provisório entre o Parlamento Europeu e o Conselho, que tem regulação em concreto em andamento, através da proposta 2021/0068(COD) de 17.03.2021 pela Comissão Europeia (2021).

Dos principais elementos do regulamento proposto, relativamente ao que interessa para a portabilidade de dados de saúde estão: (I) a emissão do certificado em papel e digital, ambas as versões dispondo de um código QR, que contém informações necessárias, bem como uma assinatura digital, para garantir a autenticidade do certificado e (II) a criação de um portal e apoiará os Estados-Membros a desenvolver *software* que permita às autoridades verificarem todas as assinaturas de certificados em toda a UE.

A nível de do tratamento dos dados, para o efeito do certificado, em respeito aos princípios da minimização, limitação das finalidades e responsabilidade, na forma das alíneas A, B e E do n.° 1 do artigo 5.° do RGPD, nenhum dado pessoal dos titulares de certificados é transmitido no portal ou conservado pelo Estado-Membro que efetua a verificação, segundo a Comissão Europeia (2021). Neste sentido, caminhando para uma normalização eficaz a nível continental, os Estados-Membros aplicarão o quadro de confiança e as normas técnicas,

acordados na rede de saúde em linha, a fim de assegurar a implementação técnica atempada do Certificado Verde Digital, a sua interoperabilidade e o pleno respeito da proteção de dados pessoais.

Apesar do relevante avanço, esta solução foi direcionada a uma vertente apenas das causas de portabilidade de dados em saúde a nível continental, útil para a união europeia limitada a matéria de COVID-19, o que demonstra a possibilidade de haver integração e normalização em grande escala, mas que ainda encontra-se distante do objetivo de estender-se a todas as matérias em saúde, considerando um contexto transcontinental, necessário para o pleno exercício do direito de portabilidade de dados em saúde, na forma garantida pelo artigo 20.° do RGPD.

Diante disto, é certo dizer que para a concretizar a portabilidade de dados pessoais é preciso um entendimento transcontinental daquela que seria a melhor prática e formato para o efeito, traduzir tais definições ainda inexistentes tecnicamente e regular juridicamente para dar segurança jurídica à pratica dos conceitos estabelecidos, por forma a ser suficientemente seguro e flexível, para adequar-se a maior parte das realidades dos sistemas em saúde, medidas técnicas e organizativas de partilha de dados de saúde.

4.1. O *SOFT LAW EM ALTERNATIVA ÀS OMISSÕES DA HARD LAW* PARA A NORMALIZAÇÃO DA PORTABILIDADE DE DADOS NO SETOR DA SAÚDE A NÍVEL INTERCONTINENTAL

É problemática e causa insegurança jurídica, diante da necessidade, a ausência de quadros legais comuns que permitam a colaboração a nível da portabilidade dados em saúde a favor do titular dos dados, através da transferência de dados entre dois responsáveis pelo tratamento. Com a aplicabilidade do Regulamento Geral sobre a Proteção de Dados, os obstáculos à partilha de dados que envolvem o intercâmbio de dados dos Estados-Membros da União Europeia para países terceiros tornou-se uma questão latente e carente de solução.

A ausência de definições por parte da comissão europeia e de um consenso intercontinental que entregue segurança jurídica por parte do direito corrente para a interoperabilidade em prol da portabilidade de dados pessoais, entre a UE e países terceiros, poderia ser minimizada através da utilização de instrumentos regulamentares não

vinculativos. Ainda que tais instrumentos possam não ser, por si só, suficientemente adequados para satisfazer todos os requisitos do RGPD, poderiam ser a base sobre a qual poder-se-ia elevar globalmente a linha guia de proteção de dados, pelo menos no âmbito da portabilidade de dados de saúde. Diante disto, uma questão que surge é: em que medida o recurso à *soft aw,* pode ser viável neste sentido no âmbito do Direito da União Europeia e outros países terceiros?

Antes de avançar para a construção da resposta desta questão, importa conceituar *Soft Law e hard Law,* que em um contexto de internacionalização são instrumentos relevantes do direito internacional. A *Softlaw* ou fontes de direito não-legislativas, são processos de normalização, de estabelecimento de um entendimento comum sobre determinada prática ou matéria, de adesão facultativa, sem caráter vinculativo e cujo o incumprimento não está associado a sanções jurídicas, de modo que a sua criação não vinculada ao poder legislativo de um ordenamento jurídico, mas poderá se dar por meio de associações e outros organismos representantes de categorias de responsáveis pelo tratamento.

Nesta modalidade, a norma assume um caráter residual, cujo escopo é estabelecer vinculações exortatórias, baseada na autonomia da vontade e na boa-fé típica das entidades que decidem aderir ao *standard*, de modo a alcançar uma fiabilidade que é endossada pelas categorias de responsáveis pelo tratamento que participam deste mesmo ambiente normativo e tem o mesmo como uma boa prática. É um exemplo deste instituto e de interesse para a proteção de dados a norma ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*, que é o padrão e a referência internacional para a gestão da Segurança da informação.

A *Hard law* são normas tradicionais, de caráter prescritivo e vinculante, na forma de atos legislativos originados de um ordenamento jurídico corrente, que pelo seu caráter coercitivo tem o condão de impingir sanções em caso de incumprimento do que estabelece. São exemplos deste instituto e de interesse para a proteção de dados o RGPD e o TFUE.

Contextualizados os conceitos e o ponto de situação do quadro regulatório continental e transcontinental sobre a proteção de dados, as arestas que ainda precisam ser lapidadas e os pontos vazios que carecem de preenchimento a respeito da definição do formato interoperável válido a nível global, para a proteção de dados, independentemente da *Hard Law* a que as entidades de saúde ao redor do mundo submetem-se, poderiam ser

normalizadas por diretrizes que emanam de *Soft Law*, à semelhança do que é feito a nível da segurança da informação, com a norma ISO/IEC 27001, sobre a qual as entidades que buscam um nível de elevado e reconhecido de segurança da informação, adotam e endossam as medidas técnicas e organizativas propostas pela mesma.

Essa abordagem encontra amparo no RGPD e no TFUE. Pelo RGPD as diretriz com recurso à *Soft Law* para o setor das saúde podem ser enquadradas na forma de um código de conduta e certificação, ao abrigo do artigo 40.° do referido regulamento, que nos termos do n.° 2 al. F, H e J, há a liberdade para que as associações e outros organismos representantes de categorias de responsáveis pelo tratamento ou de subcontratantes elaborarem códigos de conduta, alterem ou aditem a esses códigos, a fim de especificar a aplicação do presente regulamento, segundo Slokenberga (2018).

É exemplo de solução para efeitos do exercício dos direitos dos titulares dos dados, como tema central deste trabalho: a viabilidade da portabilidade de dados em saúde enquanto direito dos titulares de dados, por meio da definição de um *standard* quanto ao formato do ficheiro que atenda aos critérios dos n.° 1 e 2 do artigo 20.° do RGPD, em um contexto de transferência de dados para fora do EEE, ao abrigo do exercício deste direito entregando segurança e melhores práticas nestas operações. Conjugado com o RGPD e endossando esta possibilidade, estão os termos do artigo 171.° do Tratado de Funcionamento da União Europeia – TFUE, que aduz ser obrigação da União Europeia a condução de ações que possam revelar-se necessárias para assegurar a interoperabilidade das redes, em especial no domínio da harmonização das normas técnicas, inclusive de modo a cooperar com países terceiros para promover projetos de interesse comum e assegurar a interoperabilidade das redes.

Esta abordagem em prol da normalização permitiria que o próprio setor da saúde regulasse sobre aquilo que tem mais intimidade a nível prático, conjugado com os critérios da proteção de dados, articulando posteriormente para proporem uma sugestão de definição mais concreta com a comissão europeia para a proteção de dados, que poderá consolidar a(s) proposta(s) de certificações e códigos de conduta – *soft law*, endossando as boas práticas nos termos do artigo 40.° n.°9 do RGPD, de modo a que a solução obteria um estatuto jurídico considerável, com maior segurança jurídica, pelo menos no EEE, e divulgável com ainda mais credibilidade para o setor da saúde no "mundo" como um *gold standard* não vinculativo, uma vez que a UE já é um normalizador indireto global para a proteção de dados

pessoais.

5. A INTELIGÊNCIA ARTIFICIAL NO AUXÍLIO À DECISÃO CLÍNICA E A AUSÊNCIA DE DEFINIÇÃO EM PORTABILIDADE DE DADOS DE SAÚDE – OPORTUNIDADES E LIMITAÇÕES

A inteligência artificial ou os algoritmos que compõem os sistemas de apoio à decisão clínica, em síntese, são uma sequência de instruções de apoio à decisão, com objetivo de identificar e evitar erros médicos. Deste modo, os sistemas de suporte à decisão têm como objetivo primordial mitigar erros, sendo exemplo da minimização o desvio daquelas que não são as melhores práticas clínicas, segundo Kohn, Corrigan e Donaldson (2000).

A inteligência artificial – IA é um agregado de tecnologias em rápida evolução capaz de oferecer um vasto conjunto de benefícios económicos e sociais a todo o leque de indústrias e atividades sociais, tais como: melhorar as previsões, otimizar as operações e a afetação de recursos e personalizar o fornecimento dos serviços, de modo que tornar-se-á um cada vez mais um recurso essencial e principal para os setores de elevado impacto, dentre os quais encontra-se a saúde.

Relativamente aos sistemas de informação em saúde, entre as mais complexas dificuldades, está a reunião das diferentes partes de registo dos utentes evitando o risco de equívoco na identificação dos mesmos, , uma vez que os cuidados de saúde devem ser consistentes e direcionados à individualidade dos utentes que, em caso de erro, restará comprometida a qualidade dos dados e a prestação de cuidados, segundo De Loureiro e Nogueira (2019). Diante disto, resta claro que para a efetividade dos sistemas de apoio à decisão clínica, os dados devem estar em uma condição técnica que respeite os princípios da exatidão, integridade, transparência e responsabilidade, previstos no artigo 5.° do RGPD, de modo que os dados transferidos por meio do exercício do direito de portabilidade sejam fiáveis quando alocados em seu destino e para os fins de continuidade da prestação dos cuidados, sob pena de induzir a erro a decisão clínica.

A transferência dos dados de saúde para a continuidade da prestação de cuidados, a pedido do titular dos dados, na forma do artigo 20. °, n.º 1 e 2 do RGPD, caracteriza-se como o exercício do direito de portabilidade de dados pessoais. Uma vez que a disponibilidade de

dados é fator fundamental para a utilização da inteligência artificial, torna-se ainda relevante a necessidade de definição de um formato normalizado e interoperável entre sistemas que leiam e interpretem tais informações, sob pena de uma difusão inconsistente da informação com a utilização de inteligência artificial na saúde causar incoerências naquilo que for a recomendação à decisão clínica.

As características específicas dos sistemas de inteligência artificial podem criar novos riscos relacionados com a segurança dos utilizadores e a proteção dos direitos fundamentais, de modo que a não normalização dos critérios técnicos podem criar situações que conduzem à insegurança jurídica para o tecido público e privado, o que pressuporá a uma adoção de uma postura menos proativa e logo mais lenta das tecnologias de inteligência artificial por parte das entidades e dos titulares de dados, devido à falta de confiança pela insegurança jurídica e técnica, bem como pela falta de literacia e viabilidade. Assim, se com a evolução técnica no tema houver disparidade de respostas regulamentares por parte das autoridades nacionais, a consequência será a fragmentação do mercado.

Diante deste cenário, a Comissão Europeia (2021), através da proposta de regulamento sobre a inteligência artificial, 2021/0106(COD), de 21.4.2021, tem buscado uma abordagem baseada no risco, com quatro níveis, quais sejam:

(I) Risco inaceitável: conjunto limitado de utilizações particularmente nocivas de inteligência artificial que transgridem os valores da UE, pois violam direitos fundamentais, que serão proibidas;

(II) Risco elevado: número limitado de sistemas de inteligência artificial, enumerados na proposta, que afetam negativamente a segurança das pessoas ou o respeito dos seus direitos fundamentais (consagrados na Carta dos Direitos Fundamentais da UE). O quadro proposto é coerente com a Carta dos Direitos Fundamentais da União Europeia e está em consonância com os compromissos da UE em matéria de comércio internacional;

(III) Risco limitado: Determinados sistemas de inteligência artificial a que são impostos requisitos de transparência específicos, por exemplo quando haja um risco manifesto de manipulação (como seja a utilização de sistemas de conversação automática);

(IV) Risco mínimo: todos os restantes sistemas de inteligência artificial, que podem

ser desenvolvidos e utilizados no respeito da legislação em vigor e sem obrigações jurídicas adicionais.

Para fiscalizar o cumprimento e orientar sobre o Regulamento da Inteligência Artificial, à semelhança da matéria de proteção de dados, os estados membros designarão uma ou várias autoridades nacionais competentes para supervisionar a aplicação e a execução, bem como para realizar atividades de fiscalização do mercado, que naturalmente precisarão articular com aquelas relativas à proteção de dados, uma vez que a "matéria prima" para a utilidade da inteligência artificial são os dados, que poderão ser de natureza pessoal e de categoria especial, como é o caso setorial da saúde. Existirá para o efeito, a nível europeu, um Comité Europeu para a Inteligência Artificial, à semelhança do Comité Europeu para a Proteção de Dados.

Ainda que historicamente os sistemas jurídicos tenham provocado diversas limitações perante a sociedade, um dos principais objetivos do Direito de modo geral é estabelecer regras coerentes para uma posterior conduta, geralmente surgindo de modo reativo, após o surgimento do facto ou fenómeno que se pretende regular. Entretanto, em matéria de Regulação tecnológica, nomeadamente da inteligência artificial e proteção de dados, o caráter metodologicamente ou tecnologicamente neutro destes contemporâneos atos normativos permitem, diversamente a definição acima, como um fator de fomento.

Isto porque o quadro regulamentar europeu tem a pretensão de reforçar a adoção da inteligência artificial de duas formas:

(I) Devido à novidade e falta de literacia sobre o tema, proporcionando um aumento da confiança dos utilizadores, o que fomentará a procura de inteligência artificial pelo setor privado e pelo público.

(II) (II) Devido ao reforço da segurança jurídica e à harmonização das regras, os fornecedores de inteligência artificial terão acesso a mercados maiores, que como consequência beneficiará a económica envolta ao tema e aos destinatários enquanto beneficiários e matéria prima (titulares de dados) para a utilidade das soluções, conforme a Comissão Europeia (2021).

A nível internacional e intercontinental, do mesmo modo que tem ocorrido com a proteção de dados, a União Europeia tem assumido a vanguarda regulatória a respeito do

tema, e como consequência tornar-se-á referência para países terceiros que queiram gozar dos mesmos benefícios pela UE percebidos. A proposta de quadro regulamentar e o Plano Coordenado para a Inteligência Artificial fazem parte dos esforços da União Europeia para ser um líder na promoção de uma inteligência artificial fiável a nível internacional.

A inteligência artificial tornou-se estrategicamente importante na interseção da geopolítica, dos interesses comerciais e preocupações de segurança e países ao redor do mundo optaram por usar a inteligência artificial como um veículo para realizar suas aspirações de avanço tecnológico, motivados por sua utilidade e potencial. Apesar de a inteligência artificial ainda estar em gênesis, a UE tem tomado medidas para trabalhar em estreita colaboração com parceiros internacionais para promover o estabelecimento de normas globais nesta área, em consonância com o sistema multilateral baseado em regras e os seus valores. É exemplo da pretensão em causa as coalizões e alianças com seus parceiros, como Japão, EUA e Índia, bem como com agentes de nível multilateral, por exemplo: OCDE e do Grupo dos 20 – G20 (formado pelos ministros de finanças e chefes dos bancos centrais das 19 maiores economias do mundo mais a União Europeia) e regionais, a exemplo do Conselho da Europa, conforme a Comissão Europeia (2021).

Colocadas as considerações e contextualização, de modo acessório aos benefícios da inteligência artificial, encontram-se os novos riscos ou consequências negativas para os cidadãos e a sociedade associados a este recurso, que à luz da velocidade da evolução tecnológica e dos possíveis desafios, a União Europeia tem empenhado em alcançar uma abordagem equilibrada. Tal abordagem culminou na proposição do Regulamento do Parlamento Europeu e do Conselho, que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento da Inteligência Artificial) e altera determinados atos legislativos da união, em 21/04/2021, conforme a Comissão Europeia (2021).

Nesse sentido, há a necessidade de coordenar às implicações humanas e éticas da inteligência artificial face aos riscos. É exemplo de risco: a opacidade de alguns algoritmos, que pode gerar incerteza e dificultar a aplicação efetiva da legislação em vigor em matéria de segurança e direitos fundamentais.

Logo, quanto menos abrangente e normalizadas a nível geográfico as definições de quais critérios são aceites e suficientes para concretizar a usabilidade de um ficheiro interoperável em saúde em um formato estruturado, de uso corrente e de leitura automática, útil para alimentar os sistemas de inteligência artificial, a serem executados nas

respetivas máquinas que suportam a tecnologia para suporte à decisão clínica, menor será a difusão dos métodos e em menor grau serão atingidos e percebidos os benefícios da inteligência artificial em saúde para a melhor prática clínica.

Portanto, a falta de estrutura técnica e regulamentar normalizada para suportar o exercício do Direito de Portabilidade, ao abrigo do artigo 20.º do RGPD poderá direta e indiretamente comprometer os benefícios dos sistemas de apoio a decisão clinica se o utente precisar ser seguido fora do ambiente em que ocorreu a recolha inicial dos dados clínicos ou se o seguimento da prestação de cuidados em saúde tiver lugar fora do EEE.

Deste modo, a referida ausência implica no comprometimento dos Protocolos Clínicos Interpretáveis por Máquinas. Este problema está relacionado com a falta de expressividade dos modelos que lhes estão subjacentes, a complexidade da aquisição de conhecimento utilizando as suas ferramentas, a ausência de suporte ao processo de decisão clínica e o estilo de comunicação dos Sistemas de Apoio à Decisão Clínica que implementam Protocolos Clínicos Interpretáveis por Máquinas. Tais problemas constituem obstáculos que impedem estes sistemas de apresentarem propriedades como modularidade, flexibilidade, adaptabilidade e interatividade, propriedades estas que refletem o conceito de *living guideline*, conforme Oliveira (2017).

Por fim, importa mencionar que a Inteligência Artificial é cada vez as tomadas de decisão por máquinas ou por programas de modo autónomo, ou seja, sem intervenção humana, o que poderá pressupor Decisões individuais automatizadas, incluindo definição de perfis, na forma do artigo 22.°, n.º 4 do RGPD, o que leva à discussão de quais seriam as medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados de categoria especial de saúde. Por exemplo, na condução autónoma, é impossível que não sejam as máquinas a tomar decisões. Na cirurgia, pode ocorrer algo de semelhante.

Deste modo, diante dos desafios, possibilidades jurídicas e técnicas, a Inteligência Artificial e o seu respetivo Regulamento terão desdobramentos e conjugação com o Regulamento Geral da Proteção e Dados Pessoais e com o novo “Regulamento Máquinas” (que assegura que a nova geração de máquinas preserva a segurança dos utilizadores e consumidores e incentiva a inovação), segundo a Comissão Europeia (2021). Isto porque para a Inteligência artificial pressupõe os dados em elevado volume, incluindo dados pessoais, assim como depende de *hardware* adequado para atingir as benefícios e soluções

algorítmicas, que são parte componente do quadro geral da eficácia e viabilidade da Inteligência Artificial.

6. SAÚDE MÓVEL/*MHEALTH,* PORTABILIDADE DE DADOS E A ECONOMIA DE DADOS

Os sistemas de saúde têm vindo a seguir a inovação digital e as aplicações de saúde móvel ou *mHealth apps* tem sido cada vez mais utilizada. Entre outras vantagens, as aplicações móveis permitem melhorar a eficiência e a qualidade dos cuidados de saúde, através da comunicação e a coordenação dos cuidados de saúde entre especialistas, médicos, enfermeiros e outros, proporcionando o acesso a serviços independentemente do tempo e da localização. Por meio destas soluções, por exemplo, os profissionais da saúde podem aceder aos registos dos doentes, ver os resultados dos testes e prescrever medicamentos, de modos que os profissionais e podem partilhar informações como diagnósticos, receitas médicas, resultados laboratoriais e até marcar consultas, segundo Muchagata e Ferreira (2021).

A portabilidade de dados, enquanto direito consagrado no artigo 20.° e considerandos 68 e 73 do RGPD, no contexto das aplicações mHealth leva à seguinte reflexão: O exercício deste direito tem o condão de reforçar o controlo sobre dados pessoais dos utilizadores, entretanto, encontra desafios decorrentes da interoperabilidade entre as aplicações.

O tema implica duas questões primordiais: A primeira é a interpretação normativa do Direito, ao passo que a segunda pondera até que ponto a portabilidade de dados é possível do ponto de vista técnico (interoperabilidade) entre aplicações *mHealth*, concomitante com as dúvidas sobre quais são os riscos de privacidade. Para estes efeitos precisam ser clarificadas as lacunas jurídicas existentes e futuras na implementação do direito à portabilidade de dados no sector *mHealth*, segundo Nikchevska (2019).

Conforme tratado nos capítulos acima, é uma das questões de interesse a determinação do formato correcto e as possibilidades de implementação de transmissão directa e de API's - Interface de Programação de Aplicação, que consistem em rotinas e padrões de programação para acesso a um aplicativo de *software* ou plataforma baseado na *Web*. Outra questão é a distinção entre dados fornecidos (em bruto) e dados inferidos

(derivados); a separação de dados obtidos com consentimento ou contrato de outros dados recolhidos ao abrigo de diferentes condições de licitude e permissivos para tratar dados de categoria especial; a determinação de violação contra os direitos e liberdades dos titulares de dados e a potencial redacção automática de dados pessoais; e o desafio de implementar a portabilidade "sem obstáculos", ao mesmo tempo que se implementam "medidas de segurança adequadas", que são na sua maioria obstrutivas por natureza, segundo Bozdag (2018).

A interação entre utentes titulares de dados e prestadores de cuidados de saúde, na qualidade de Responsáveis do Tratamento ou Subcontratantes, na forma do artigo 4. °, n. ° 7 e 8. ° do RGPD, através de aplicações móveis, pode potencialmente melhorar a eficiência e a qualidade dos cuidados de saúde, segundo Muchagata e Ferreira (2021). Apesar das vantagens das soluções em *Mobile Health – mHealth* (termo que é utilizado para a prática da medicina e da saúde pública suportada por dispositivos móveis) a maioria das aplicações móveis tem implicações a nível da proteção de dados e de segurança da informação, que no âmbito do Direito da Portabilidade de Dados pessoais encontra pouca orientação e fiabilidade sobre como promovê-lo, de modo a ainda estar pendente o desenvolvimento com um equilíbrio adequado entre disponibilidade e confidencialidade dos formatos interoperáveis para o efeito.

Fato é que os *mHealth apps* são cada vez mais utilizados, entregando vantagens como o melhoramento, a eficiência e a qualidade dos cuidados de saúde através da comunicação e da coordenação dos cuidados entre especialistas, médicos, enfermeiros e outros, proporcionando o acesso a serviços independentemente do tempo e da localização. É exemplo desta facilidade a possibilidade de os médicos acederem aos registos dos doentes, aos resultados dos testes e de prescrever medicamentos, conforme aduzem Muchagata e Ferreira (2021).

Concomitante à interação profissional, os utentes titulares de dados que utilizam aplicações móveis poderão ter acesso aos seus dados e a possibilidade de contribuir com a atualização dos mesmos em seus Registos de Saúde Eletrónicos, através da alimentação dos sistemas com métricas geradas e introduzidas no dispositivo móvel, a exemplo dos inputs comportamentais do dia-a-dia, a exemplo dos horas de sono, dieta, comportamento cardíaco, entre outras variáveis. Além disto, poderão receber a partilha por parte do profissional e entidade de saúde que lhe segue, com informações como diagnósticos, receitas

médicas, resultados laboratoriais e até podendo marcar consultas. Apesar de todos os benefícios, existem preocupações jurídicas e de segurança da informação, por exemplo: algumas aplicações, para além de armazenarem e tratarem dados de saúde (que são dados sensíveis na acessão do artigo 9.° n. ° 1 do RGPD), também recolhem informações (incluindo dados sensíveis), tais como nome de utilizador, palavra-passe, informações de contacto, idade, sexo, lista de contactos, fotografias pessoais, entre outros dados, podendo também aceder à funcionalidade do sistema de posicionamento global - GPS, que permite obter a localização do dispositivo, e por sua vez, o utilizador (utente titular de dados) que o transporta, o que poderá configurar o desrespeito aos princípios da limitação da finalidade, minimização e limitação do tratamento, previstos nas alíneas A, B e C do n.°1 do artigo 5.° do RGPD.

Face à novidade da proteção de dados, para a maioria da população há uma grande iliteracia sobre o tema, de modo que não sabem como os seus dados vão ser utilizados nem por que tipo de entidades, importando neste ensaio aquilo que se refere ao exercício do Direito à proteção de Dados em Saúde. Há também uma falta de medidas de normalização e segurança na maioria das aplicações, bem como uma baixa proteção nas Transferéncias de Dados Pessoais, através das redes móveis e sem fios, o que prejudica o Direito em causa.

Muito do que diz respeito à preocupação com a conformidade com a proteção de dados pessoais neste contexto passa pela definição de onde estarão os servidores que armazenam os dados e, se no sítio geograficamente escolhido, são aplicáveis o Direito da União Europeia para que sejam aproveitáveis as garantias jurídicas do RGPD ou as suas derrogações, assim como são de interesse as transferências de dados entre entidades em nome do titular ou diretamente para o mesmo. Outra questão que provoca especial atenção é a definição de perfis dos doentes que as soluções necessitam fazer para entregarem os seus benefícios, na forma do n.°4 do artigo 4.° e 22.° do RGPD, de modo a avaliar os aspetos de saúde dos utentes.

Uma primeira questão é se o tratamento de dados ou parte são abrangidas pelo RGPD. Isto porque quando os dados são verdadeiramente anonimizados, o RGPD não será aplicável, visto que regula apenas aquilo que diz respeito a dados pessoais. Neste sentido, importa destacar que são dados pessoais qualquer informação relativa a uma pessoa singular identificada ou identificável (titular dos dados), nos termos do artigo 4. ° n.°1 do RGPD.

Ocorre que a anonimização de dados em saúde é quase impossível quando a intenção

tem relação com a condução da prestação de cuidados em saúde, que pela própria natureza tem caráter individualizado, o que causa a necessidade de identificar o titular dos dados, apesar de na prática clínica os conceitos de encriptação, cifragem, pseudonimização e anonimização serem confundidos. Ocorre que a Pseudonimização, nos termos do n.°5 do artigo 4.° do RPGD, é um tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável, ao passo que a cifragem e encriptação são métodos para a pseudonimização, ao passo que a anonimização somente ocorreria se de nenhuma maneira fosse possível retroceder e chegar aos dados do utente.

Nessa situação, os dados podem ser tratados por qualquer parte para qualquer fim legítimo, variando desde fins comerciais a investigação médica ou estatística. Mas o RGPD coloca a fasquia alta na anonimização, afirmando no considerando 26 GDPR que os dados são anónimos quando "não dizem respeito a uma pessoa identificada ou identificável". A anonimização é uma técnica aplicada aos dados pessoais a fim de conseguir uma de identificação irreversível e o mesmo considerando clarifica que os dados pessoais que são "apenas" pseudónimos, devem continuar a ser considerados como informações sobre uma pessoa singular identificável.

Para determinar se é razoavelmente provável que sejam utilizados meios para identificar a pessoa singular, devem ser tidos em conta todos os fatores objetivos, tais como os custos e o tempo necessário para a identificação, tendo em consideração a tecnologia disponível no momento do processamento e da evolução tecnológica.

Portanto, como medida para permitir a interoperabilidade nos diversos sistemas de saúde, para além das medidas de segurança mencionadas, sendo da natureza das solução uma dinâmica ágil, a exportação de dados ser possível em vários formatos, definidos objetivamente, pelo critério de quais são os mais recorrentes em diferentes entidades e nas principais plataformas, sendo inevitável o risco residual de ser possível abranger a todos os formatos. Paralelamente, seria uma outra vertente de solução, segmentar os standards de formato para exportação ou intercambio dos dados de saúde, a separação do formato por práticas clínicas.

7. OS LIMITES AO EXERCÍCIO DOS DIREITO À PORTABILIDADE EM SAÚDE;

O artigo 11.° do RGPD apresenta uma hipótese de Isenção à necessidade de atender a um pedido de exercício do Direito de portabilidade, que é aplicável se o Responsável pelo Tratamento puder demonstrar que não consegue identificar o titular dos dados. Se, no entanto, o titular dos dados fornecer ao responsável pelo tratamento informações adicionais que lhe permitam ser identificado no conjunto de dados, o mesmo deve ser autorizado a exercer os seus direitos.

Entretanto, se os dados pessoais forem desidentificados a um ponto que o Responsável pelo tratamento já não consiga identificar o titular de dados, mesmo com informações complementares, o pedido de exercício do Direito de Portabilidade não precisará ser atendido, devido à impossiblidade de o fazer. Diante desta reflexão, deveriam os responsáveis pelo tratamento serem obrigados a utilizar algoritmos de reidentificação ou outro método aproveitando os dados adicionais fornecidos pelo titular de dados, a fim de reidentifica-lo para executar o pedido de exercício do direito de portabilidade de um indivíduo, conjugando o artigo 20.° com o artigo 11.° n.° 2 do RGPD?

Em uma lógica que considera o princípio da minimização da recolha de dados, previsto no n.°1 alínea C do artigo 5.° do RGPD, recolher mais dados para esta finalidade seria uma medida contrária ao princípio em causa, que conjugando com o n.° 2 do artigo 5.° do RGPD, elevará a responsabilidade do Responsável pelo Tratamento, que precisará, de modo acessório à esta prática, comprovar que a medida não extrapola o princípio da limitação das finalidades, previsto no n.°1 alíena B do artigo 5.° do RGPD. Na mesma linha de raciocínio, importa considerar o conceito de dados pessoais, que nos termos do artigo 4.° n.°1 do RGPD consiste em informação relativa a uma pessoa singular identificada ou identificável, ao passo que é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador.

Ora, se não é possível identificar os dados no estado em que se encontram, ainda que com um indicador sumplementar, tais informações não podem ser consideradas dados pessoais, na forma do conceito acima colocado, sendo, portanto, dados anónimos, o que exime a aplicabilidade do RGPD, uma vez que consiste em regras em matéria de proteção relativamente ao tratamento de dados pessoais. Portanto, o Direito de Portabilidade de dados Pessoais não seria sequer aplicável, visto que nesta hipótese não aproveita a tutela do

RGPD. Reforçando esta teoria, o considerando 26 do RGPD dispõe que os princípios da proteção de dados não deverão aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado, não dizendo o RGPD respeito ao tratamento das informações anónimas.

De outro lado e antes de adentrar no raciocínio da segunda hipótese, importa mencionar o conceito de Pseudonimização, que nos termos do artigo 4.° n.°5 do RGPD, consiste no tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico, sem recorrer a informações suplementares. Conjugado este conceito com o conceito de dados pessoais do n.° 1 do artigo 4.° do RGPD acima mencionado, é certo concluir que os dados pseudonimizados são de natureza pessoal, o que pressupõe a tutela do RGPD e a necessidade de atender ao pedido de exercício do direito de portabilidade.

Assim, se os dados estão pseudonimizados, ainda será possível serem atribuídos a uma pessoa singular, mediante a utilização de informações suplementares, sendo portanto, dado pessoal e identificável, o que torna possível o esforço para reidentificar o titular de dados para o efeito do exercício do direito de portabilidade. Portanto, nesta análise que deve ser causuística, para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção para identificar direta ou indiretamente a pessoa singular.

Superada a instância jurídica, tendo concluído que o RGPD é aplicável, para implementar a exigência legal será preciso ponderar a possiblidade em instância técnica. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular e, portanto, de cumprir com o pedido de exercicio do direito de portabilidade, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica.

O Direito de Portabilidade também encontra limitação se o tratamento se basear num fundamento jurídico que não seja o consentimento ou um contrato, bem como restará impedido se for pretenção exercê-lo em relação aos responsáveis pelo tratamento que tratem dados pessoais na prossecução das suas atribuições públicas, conforme o considerando 68.° do RGPD. Além destas, também é hipótese de limitação quando o

tratamento de dados pessoais for necessário para o cumprimento de uma obrigação jurídica à qual o responsável esteja sujeito, para o exercício de atribuições de interesse público ou para o exercício da autoridade pública de que esteja investido o responsável pelo tratamento, conforme o mesmo considerando.

Ademais, quando um determinado conjunto de dados pessoais disser respeito a mais de um titular, o direito de receber os dados pessoais não deverá prejudicar os direitos e liberdades de outros titulares de dados nos termos do presente regulamento. Além disso, esse direito também não deverá prejudicar o direito dos titulares dos dados a obter o apagamento dos dados pessoais nem as restrições a esse direito estabelecidas no presente regulamento e, nomeadamente, não deverá implicar o apagamento dos dados pessoais relativos ao titular que este tenha fornecido para execução de um contrato, na medida em que e enquanto os dados pessoais forem necessários para a execução do referido contrato, segundo o considerando 68 do RGPD.

Finalmente, uma reflexão prática sobre a hipótese de limitação aplicável quando o direito de portabilidade puder prejudicar os direitos e liberdades de outros titulares, na forma do considerando 68 do RGPD, encontra-se na possibilidade de leitura do Certificado Digital UE Passe Covid COVID-19, por meio de uma aplicação disponível a qualquer cidadão Português. A aplicação para telemóveis “SNS 24”permite a emissão e apresentação do Certificado Digital da UE em formato eletrónico, podendo cada cidadão obter, consultar e armazenar o seu certificado digital COVID da EU.

Desenvolvida pelos Serviços Partilhados do Ministério da Saúde – SPMS, a aplicação móvel “SNS 24”de leitura do Certificado Digital UE “Passe COVID”, pretende permitir que as entidades que precisem de validar os Certificados Digitais COVID da União Europeia (UE), que entraram em vigor no passado dia 1 de julho, possam fazê-lo de forma digital e rápida. A “app”, desenvolvida pela Imprensa Nacional Casa da Moeda – INCM , pode ser descarregada e utilizada por todos, nomeadamente transportadoras aéreas, organizadores de eventos culturais, corporativos, desportivos e familiares (como casamentos e batizados). Através desta aplicação poderão ser validados automaticamente os três tipos de certificados – de vacinação, de teste e de recuperação – emitidos pelos países membros da UE. Para isso, baste apontar a câmara do telemóvel para o código QR do Certificado Digital COVID apresentado (em papel ou em formato digital).

O resultado pode ser positivo ou negativo: um resultado com sinal verde significa que

o Certificado Digital COVID foi validado com sucesso; um resultado com sinal vermelho significa que o certificado não é válido. Durante o processo, apenas serão visualizados o nome, data de nascimento e informação sobre a verificação de validade do Certificado, sendo que nenhum dado pessoal supostamente será armazenado pela aplicação, segundo a Direção Geral de Saúde (2021).

Ocorre que, conforme introduzido nos capítulos anteriores deste trabalho, a proposta 2021/0068(COD) de 17.03.2021 da Comissão Europeia, relativo a um quadro para a emissão, verificação e aceitação de certificados interoperáveis de vacinação, testes e recuperação, a fim de facilitar a livre circulação durante a pandemia de COVID-19 (Certificado Verde Digital), através do artigo 9.° n.°2 sobre a proteção de dados, os dados pessoais incluídos nos certificados referidos no artigo 3.º da mesma proposta devem ser tratados pelas autoridades competentes do Estado-Membro de destino ou pelos operadores de serviços de transporte transfronteiras de passageiros obrigados pela legislação nacional a aplicar determinadas medidas de saúde pública durante a pandemia de COVID-19, para confirmar e verificar a situação vacinal, de testes e de recuperação do titular dos certificados.

É mencionado, ainda, que para o efeito, os dados pessoais devem limitar-se ao estritamente necessário, o que leva a crer que o acesso à possibilidade de efetuar a leitura de um certificado verde digital uma medida desproporcional, uma vez o cidadão comum e não imbuído dos deveres acima descritos, não figurará como autoridade ou agente operador de serviço de transporte e afins, em clara violação ao princípio da limitação das finalidades, previsto no artigo 5.°, n. ° 1 alínea B do RGPD, o que pressupõe uma violação aos direitos e liberdades do titular dos dados.

Apesar de a leitura do certificado só ser possível com a disponibilização ou divulgação do mesmo pelo titular de dados, é facto que nem sempre é possível o mesmo exercer a faculdade de recusar a um pedido de exposição de tal documento, nomeadamente quando se encontra em situação de vulnerabilidade.

É exemplo de vulnerabilidade para o efeito a situação hipotética de um recrutamento profissional, em que a entidade recrutadora pede aos candidatos interessados na vaga para enviarem, dentre diversos documentos, o certificado digital, com o objetivo explicito ou implícito de verificar o estado de vacinação ou de infeção passada de COVID-19, o que servirá para uma tomada de decisão, uma vez que a função para a qual os candidatos se aplicam é operacional e pressupõe a presença do colaborador escolhido junto ao público. Diante disto,

a ausência de vacinação por uma pessoa de faixa etária que não tem previsão de vacinação breve ou por outros motivos, poderá dar lugar a uma segregação ou preferência por um dos pares concorrentes, que já tenha sido vacinado ou que esteja mais próximo de vacinar-se do que o outro. Um exemplo de motivo da segregação, ainda que a vacinação não seja obrigatória a nível legal em Portugal, seria pelos custos que a ausência de um funcionário geraria ao precisar substitui-lo temporariamente, considerando que a recuperação de alguém não vacinado poder ser mais demorada do que aquela de quem foi vacinado.

Considerando que qualquer cidadão poderá descarregar a aplicação para a finalidade, será dificultosa a tarefa de impedir tais abusos, uma vez que, em contrário à orientação a nível europeu da proposta de regulamento, o estado português não limitou a possibilidade de leitura dos dados pelo formato interoperável do *QR Code* por parte apenas das autoridades e entidades competentes para o efeito, antes alargou a todos os cidadãos tal possibilidade.

Portanto, o limite do Direito da Portabilidade de Dados deve ser identificado casuisticamente, conjugando os critérios acima colocados, sempre ponderando o exercício do direito respeitando os direitos e liberdades do próprio titular de dados, nunca em detrimento dos direitos da coletividade ou de um outro par.

CONCLUSÃO

Derivado dos processos e operações em cuidados de saúde encontram-se os desdobramentos jurídicos e técnicos relativos à proteção de dados pessoais, ao abrigo do RGPD e demais normas correlatas para o efeito. Incluídos na definição de dados pessoais de categoria especial, nos termos do artigo 9. °, n. ° 1 do RGPD, por esta natureza, os dados de saúde aproveitam de uma proteção especial relativamente ao seu tratamento, que são condicionados a permissivos para e efeito, desde que atendidas a algumas das hipóteses constantes nas alíneas do n. ° 2 do artigo 9. ° do RGPD.

Dentre os direitos dos titulares de dados, encontra-se o Direito de Portabilidade do artigo 20. ° do RGPD, que foi objeto deste estudo, o qual implica, para além da ponderação jurídica, desdobramentos técnicos para possibilitar o exercício do mesmo. A nível nacional e continental Europeu, existe algum consenso sobre interoperabilidade em saúde, o que tem permitido um intercâmbio de dados entre os países membros da união europeia e em dentro de Portugal em alguma medida, restando como desafio maior a definição de quais são as melhores práticas ou abordagens para as transferência para fora do EEE, respeitando os preceitos das normas em privacidade e proteção de dados, conjugando com o desafio de normalização em diferentes ordenamentos jurídicos.

Em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais e o exercício do direito de portabilidade de dados em saúde, a normalização a nível nacional partiu da iniciativa publica, que cada vez mais tem influenciado a iniciativa privada, servindo com regra de ouro, através das quais espera-se normalizar o todo, em medida relevante.

A nível jurídico, alguns conceitos de interesse para a portabilidade se confundem em alguma medida, a exemplo do direito de acesso e de portabilidade, de modo que, em síntese, a diferenciação consistirá na observação da extensão dos direitos, que para a portabilidade é mais alargada com a possibilidade de transferência dos dados entre responsáveis pelo tratamento, em favor e a pedido do titular dos dados, enquanto para o direito de acesso o

exercício do direito é satisfeito quando ao mesmo são fornecidos os dados e informações acessórias que foram requeridas.

Também se confundem os conceitos de transferência e transmissão para efeito do exercício da portabilidade de dados, de modo ambos são utilizados em um contexto que se refere a um intercâmbio de dados. Diante das reflexões deste trabalho, concluiu-se que a diferença das nomenclaturas está no contexto e no sentido a que maioritariamente foram aplicadas na redação do RGPD e a que finalidade se referem. Enquanto a "transmissão" é utilizada em um contexto que maioritariamente se refere a um intercambio de dados dentro do EEE, a "transferência" é utilizada maioritariamente em um contexto em que a norma buscou dizer respeito ao intercâmbio de dados para países terceiros à UE.

A interoperabilidade a nível transcontinental, para fora do EEE, relativamente à portabilidade de dados ao abrigo do n.°1 e 2 do artigo 20.° do RGPD tem encontrado desafios técnicos jurídicos, sendo o primeiro referente à definição do formato de leitura comum e interoperável, funcional no número máximo de sistemas de informação em variadas instituições, e o segundo relativo a uma normalização que garantisse segurança jurídica nas nos referidos intercâmbio de dados para o efeito do exercício do direito de portabilidade. Como alternativa, as normalizações por via de *Sof-Law* poderiam estabelecer, pelo menos no setor da saúde, um *standard* de boas práticas para a portabilidade, ultrapassando aquilo que não pode alcançar o direito corrente de um ordenamento jurídico, devido à limitação de jurisdição geográfica e soberania dos estados soberanos ao redor do Globo. Neste sentido e com tal definição *standard* que indicasse quais seriam os formatos interoperáveis para exportação mais comuns e fiáveis a nível da segurança da informação, de modo a torna a designação e orientação uma prática corrente no âmbito da saúde intercontinental.

O sucesso ou o insucesso da portabilidade de dados tem influência na redundância, exatidão e fiabilidade dos dados em matéria de utilidade em sistemas de inteligência artificial, que em matéria de saúde tem grande utilidade no que diz respeito aos sistemas de auxílio à decisão clínica. Sendo um tema embrionário a nível regulatório, este trabalho identificou mais perguntas do que respostas, esperando que o regulador europeu responda aos anseios sobre a matéria, através do novo já proposto regulamento sobre o tema.

Por fim, este trabalho buscou refletir sobre os limites do direito de portabilidade de dados em saúde, chegando a conclusão de que o limite do exercício deste direito deve ser proporcional ao esforço que o responsável pelo tratamento deve fazer, ponderando o que

poderia ser ou não prejudicial aos direitos e liberdades do próprio titular de dados ou de outro titular terceiro, não podendo este direito sobrepor ou ser exercido em detrimento dos direitos da coletividade ou de um outro par, devendo a análise sobre o tema deve ser feita casuisticamente.

Diante do exposto, os desafios da portabilidade de dados de saúde, dentro e fora da união europeia, têm natureza jurídica e técnica, encontrando dificuldades a nível regional, continental e global, tendo como principal preocupação a normalização nestas duas vertentes. Para alguns desafios, os caminhos para as soluções foram identificados, enquanto para outros ainda é esperada uma posição do regulador ou de comportamento mercadológico, que na ausência ou omissão do primeiro, poderá ser sanada por normas não vinculativas, não oriundas do direito corrente de um ordenamento jurídico, de modo que este *standard* seja uma boa prática entendida como fiável por grande parte do setor da saúde global.

BIBLIOGRAFIA

29, GRUPO DO ARTIGO. 2017. «Orientações sobre o direito à portabilidade dos dados». WP 242 rev.01. https://n3x0.com/wp-content/uploads/2019/08/Orientações_WP242_-sobre-o-direito-à-portabilidade-dos-dados.pdf.

Abreu, Joana Covelo de. 2020. «A e-Saúde (eHealth) no contexto da presente emergência pandémica - a proteção de dados pessoais e a interoperabilidade nas aplicações móveis de rastreabilidade de contactos (tópicas reflexões)». *Repositório da Universidade do Minho*, 2020. https://doi.org/10.21814/uminho.ed.25.12.

Alexandra, Maria, e Figueira Pinto. 2017. «O PROFISSIONAL DE INFORMAÇÃO EM SAÚDE NO APOIO À DECISÃO CLÍNICA E À INVESTIGAÇÃO». UNIVERSIDADE DE LISBOA. https://repositorio.ul.pt/bitstream/10451/31844/1/ulfl242347_tm.pdf.

Almeida, Ana Paula Martins Vieira. 2019. «O Papel da Interoperabilidade na Administração Pública : Contributos para melhorar a gestão de informação e a satisfação dos cidadãos O Papel da Interoperabilidade na Administração informação e a satisfação dos cidadãos». Universidade de Lisboa. https://www.repository.utl.pt/bitstream/10400.5/20412/1/1_Dissertação_Final.pdf.

Belluzzo, Regina Celia Baptista. 2019. «Transformação digital e competência em informação: reflexões sob o enfoque da Agenda 2030 e dos Objetivos de Desenvolvimento Sustentável». *Revista Conhecimento em Ação* 4 (1): 3–30. https://doi.org/10.47681/rca.v4i1.26573.

Bouridane, Ahmed, Richard Jiang, Somaya Al-maadeed, e Danny Crookes. 2017. *Biometric Security and Privacy*. Editado por Azeddine Beghdadi. *Biometric Security and Privacy - Opportunities & Challenges in the Biga Data Era*. Springer. https://doi.org/978-3-319-47301-7.

Bozdag, Engin. 2018. «Data Portability Under GDPR: Technical Challenges». *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3111866.

Comissão das Comunidades Europeias. 2021. *REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo a um quadro para a emissão, verificação e aceitação de certificados interoperáveis de vacinação, testes e recuperação, a fim de facilitar a livre circulação durante a pandemia de COVID-19 (Certifica*. *Jornal Oficial da União Europeia*. Europa. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52021PC0130.

Costa, Angelo, Aliaksandra Yelshyna, Teresa C. Moreira, Francisco C.P. Andrade, Vicente Julián, e Paulo Novais. 2017a. «A legal framework for an elderly healthcare platform: A privacy and data protection overview». *Computer Law & Security Review* 33 (5): 647–58. https://doi.org/10.1016/j.clsr.2017.03.021.

———. 2017b. «A legal framework for an elderly healthcare platform: A privacy and data protection overview». *Computer Law & Security Review* 33 (5): 647–58. https://doi.org/10.1016/j.clsr.2017.03.021.

Duarte, Sara Lima. 2014. «Partilha de dados na prestação de cuidados de saúde – análise têmporo-

espacial». Universidade Beira da Interior. https://ubibliorum.ubi.pt/bitstream/10400.6/6410/1/3380_6777.pdf.

Europa, Conselho da. 1980. «Council of Europe: Draft Convention for the Protection of Individuals with regard to Automatic Processing of Persobal Data». *International Legal Materials* 19 (2): 284–324. https://doi.org/10.1017/S0020782900043230.

———. 2021. *Interoperability of health certificates Trust framework*. Europa: eHealth Network. https://ec.europa.eu/health/sites/health/files/ehealth/docs/trust-framework_interoperability_certificates_en.pdf.

Europeia, Comissão. 2020. «Shaping Europe ’ s digital future The Europeana platform». https://doi.org/10.2759/48191.

Europeia, Direção da Investigação e Documentação do Tribunal de Justiça da União. 2018. *Ficha Temática: Proteção de Dados*. Europa: Tribinal de Justiça da União Europeia. https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_pt.pdf.

Europeia, União. 2016. *Carta dos Direitos Fundamentais Da Uniao Euopeia*. *Jornal oficial da União Europeia*. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR.

Europeu, Parlamento. 2018. *DECISÃO (UE) 2015/2240 DO PARLAMENTO EUROPEU E DO CONSELHO, de 25 de novembro de 2015, que cria um programa sobre soluções de interoperabilidade e quadros comuns para as administrações públicas, as empresas e os cidadãos europeus (Programa ISA2) como um m*. Vol. 2018. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015D2240&from=LV.

Gago, Pedro, Manuel Filipe Santos, Alvaro Silva, Paulo Cortez, José Neves, e Lopes Gomes. 2005. «INTCare: a Knowledge Discovery Based Intelligent Decision Support System for Intensive Care Medicine». *Journal of Decision Systems* 14 (3): 241–59. https://doi.org/10.3166/jds.14.241-259.

Guptill, Janet. 2005. «Knowledge management in health care». *Health Care Finance*, 4–10. https://pubmed.ncbi.nlm.nih.gov/16080410/.

Kohn, Linda T., Janet M. Corrigan, e Molla S. Donaldso, eds. 2000. *To Err is Human - Building a Safer Health System*. Washington (DC): Institute of Medicine (US) Committee on Quality of Health Care in America. https://www.ncbi.nlm.nih.gov/books/NBK225182/.

Kouroubali, Angelina, e Dimitrios G. Katehakis. 2019. «The new European interoperability framework as a facilitator of digital transformation for citizen empowerment». *Journal of Biomedical Informatics* 94 (April): 103166. https://doi.org/10.1016/j.jbi.2019.103166.

Ladeia, Yuri. 2020. «LGPD (quase) em vigor e as lições para o Brasil após 2 anos de GDPR na Europa». Portal Canaltech. 2020. https://canaltech.com.br/legislacao/lgpd-adiantando-expectativas-da-pratica-com-a-experiencia-europeia-pelo-gdpr/.

———. 2021. «Conformidade com a proteção de dados: RGPD vs Segurança da Informação». Linkedin. 2021. www.linkedin.com/feed/update/urn:li:activity:6813084283993948160/?commentUrn=urn%3Ali%3Acomment%3A(ugcPost%3A6812670673111060480%2C6813084195280228352.

Leal, Maria Filipa Rodrigues. 2013. «Avaliação da Qualidade do Registo Clínico Eletrónico». Universidade do Minho. https://repositorium.sdum.uminho.pt/bitstream/1822/27778/1/dissertacao_Maria Filipa Rodrigues Leal_2013.pdf.

Lysaght, Tamra, Hannah Yeefen Lim, Vicki Xafis, e Kee Yuan Ngiam. 2019. «AI-Assisted Decision-making in Healthcare». *Asian Bioethics Review* 11 (3): 299–314. https://doi.org/10.1007/s41649-019-00096-0.

Machado, José. 2021. «Inteligência Artificial na área clínica».

Maria de Fátima Marinho de, Souza. 2008. «Dos dados a política: a importância da informação em saúde». *Epidemiologia e Serviços de Saúde* 17 (1): 5–6. https://doi.org/10.5123/S1679-49742008000100001.

Moniz, Canto. 2018. «Finalmente : coerência no âmbito de aplicação do regime da União Europeia de proteção de dados pessoais ! O fim do enigma linguístico do artigo 3 . º , n . º 2 do RGPD». *UNIO - EU Law Journal* 4 (2): 119–31. https://revistas.uminho.pt/index.php/unio/article/download/25/57/154.

Moniz, Graça Canto. 2018. «Direitos do Titular de Dados Pessoais: O Direito à Portabilidade». Em *Anuário da Proteção de Dados*, editado por Centro de I & D sobre Direito e Sociedade Universidade Nova de Lisboa; Faculdade de Direito; CEDIS, 11–35. https://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf.

Morr, Christo El, e Julien Subercaze. 2016. *Knowledge Management in Healthcare*. Editado por Lorri Zipperer. *Knowledge Management in Healthcare*. Routledge. https://doi.org/10.4324/9781315591179.

Muchagata, Joana, e Ana Ferreira. 2018. «Translating GDPR into the mHealth Practice». Em *2018 International Carnahan Conference on Security Technology (ICCST)*, 1–5. IEEE. https://doi.org/10.1109/CCST.2018.8585546.

Nikchevska, Andrijana. 2019. «mHealth apps and Right to Data Portability: Law and Reality». Università di Bologna. http://amsdottorato.unibo.it/9051/.

Nogueira, Ana Cláudia de Loureiro e. 2019. «Validação da identificação de utentes num integrador de mensagens HL7 para monitorização e portabilidade de dados na área da saúde». Universidade do Porto. https://repositorio-aberto.up.pt/bitstream/10216/124629/2/369646.pdf.

Nunes, Gonçalo Alexandre Ferreira. 2019. «O Tratamento de Dados Pessoais de Saúde à luz do Regulamento Geral Europeu de Proteção de Dados Pessoais». Universidade de Coimbra. https://estudogeral.sib.uc.pt/bitstream/10316/89580/1/Dissertação_Gonçalo_MGES_VF.pdf.

Oficial, Jornal, U E Do, Parlamento Europeu, D O Conselho, e Social Europeu. 2011. «Directiva 2011/24/UE do Parlamento Europeu e do Conselho de 9 de Março de 2011 relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços». *Jornal Oficial da União Europeia* 2009: 45–65. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32011L0024.

Oliveira, Daniela Sofia Rijo. 2017. «Plataforma de Apoio à Prática de Cuidados de Enfermagem em Contexto Hospitalar». Universidade do Minho. http://repositorium.sdum.uminho.pt/handle/1822/22675%0Ahttp://repositorium.sdum.uminho.pt/%0Ahttp://hdl.handle.net/1822/35337.

Oliveira, Tiago José Martins. 2017. «Clinical Decision Support: Knowledge Representation and Uncertainty Management». Universidade do Minho. https://repositorium.sdum.uminho.pt/handle/1822/48713.

Parlamento e Conselho Europeu. 1995. «Directiva 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». *Jornal Oficial das*

Comunidades Europeias 1995: 31–50.

Parlamento Europeu. 2014. *Para uma economia dos dados próspera*. *Jornal Oficial da União Europeia*. https://www.europarl.europa.eu/doceo/document/TA-8-2016-0089_PT.pdf.

Pinheiro, Lena Vania Ribeiro, e Lêna Vânia Ribeiro. 2005. «PROCESSO EVOLUTIVO E TENDÊNCIAS CONTEMPORÂNEAS DA CIÊNCIA DA INFORMAÇÃO». *Informação & Sociedade* 15 (1): 13–48. http://www.ies.ufpb.br/ojs/index.php/ies/article/view/51.

Portela, Filipe. 2009. «Sistemas de Apoio à Decisão na Medicina Intensiva Baseados na Descoberta de Conhecimento em Base de Dados». Universidade do Minho. https://repositorium.sdum.uminho.pt/bitstream/1822/26281/1/MEGSI - Sistemas de Apoio à Decisão na Medicina Intensiva.pdf.

Portuguesa, Diário da República. 2021. «DIREITOS FUNDAMENTAIS». 2021. https://dre.pt/lexionario/-/dj/115078775/view.

Presidência do Concelho de Ministros. 2017. *Resolução do Conselho de Ministros n.º 41/2018*. https://www.dgadr.gov.pt/estrategia-nacional-para-a-agricultura-biologica.

———. 2018. «Resolução do Conselho de Ministros n.º 2/2018, de 5 de Janeiro». *Diário da República*, 121–27. https://dre.pt/application/file/a/114461891.

Rama, Nuno José, João Paiva Pimentel, e Vitor Manuel Raposo. 2016. «A importância das bases de dados na gestão do conhecimento em saúde». *Revista Portuguesa de Cirurgia*, 4.

Ramos, Ana Rita, e Cristina Silva. 2009. «Evolução do seguro de saude em Portugal». *Instituto de Seguros de Portugal*, 11.

Reifman, Susanne, e David Saunders. 2021. «The case for a global data privacy adequacy standard». International Association of Privacy Professionals - IAPP. 2021. https://iapp.org/news/a/the-case-for-a-global-data-privacy-adequacy-standard/.

Rodrigues, Bruno Jorge de Sales. 2015. «Segurança no acesso ao registo clínico eletrónico». Universidade do Minho. https://repositorium.sdum.uminho.pt/bitstream/1822/40860/1/Bruno Jorge de Sales Gomes Rodrigues.pdf.

Rodrigues, Paulo Renato Dias. 2013. «Universidade do Minho Escola de Engenharia Data Warehouses suportados por Nuvens». Universidade do Minho. http://repositorium.sdum.uminho.pt/bitstream/1822/27849/1/eeum_di_dissertacao_pg19826.pdf.

Rudgard, Sian. 2012. «Origins and Historical Context of Data Protection Law». *European Privacy: Law and Practice for Data Protection Professionals*, 3–17. https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf.

Sandi, Ale Antonio Auad. 2015. «A importância dos Sistemas de Informação em Saúde – Estudo de caso na USF CelaSaúde». *Faculdade de Economia da Universidade de Coimbra*, 1–84.

Saúde, Direção Geral de. 2021. «Novas aplicações móveis permitem emitir e aceder a Certificados Digitais». covid19.min-saude.pt. 2021. https://covid19.min-saude.pt/novas-aplicacoes-moveis-permitem-emitir-e-aceder-a-certificados-digitais/.

Semidão, Rafael Aparecido Moron [UNESP. 2014. «Dados, informação e conhecimento enquanto elementos de compreensão do universo conceitual da ciência da informação: contribuições teóricas». Universidade Estadual Paulista. https://repositorio.unesp.br/handle/11449/110783%0Ahttp://files/658/Semidão - 2014 - Dados, informação e conhecimento enquanto elemento.pdf.

Serviços Partilhados do Ministério da Saúde. 2017. «Privacidade da Informação no setor da Saúde - Guia sobre o Regulamento Geral de Privacidade de Dados». http://www.spms.min-saude.pt/wp-content/uploads/2017/03/Guia-Privacidade-SMPS_RGPD_digital_20.03.172-v.2.pdf.

Silva, Álvaro José Barbosa Moreira da. 2007. «Modelos de inteligência artificial na análise da monitorização de eventos clínicos adversos, disfunção/falência de órgãos e prognóstico do doente crítico». *Repositório aberto da Universidade do Porto*. Instituto de Ciências Biomédicas Abel Salazar da Universidade do Porto. https://repositorio-aberto.up.pt/handle/10216/64592.

Silva, Guilherme Almeida Rosa da. 2013. «O processo de tomada de decisão na prática clínica: a medicina como estado da arte». *Rev. Soc. Bras. Clín. Méd* 11 (1): 75–79.

Slokenberga, Santa. 2018. «Biobanking between the EU and Third Countries — Can Data Sharing Be Facilitated via Soft Regulatory Tools?» *European Journal of Health Law* 25 (5): 517–36. https://doi.org/10.1163/15718093-12550397.

Sousa, Mariana Leite. 2017. «OpenEHR como solução para o Regulamento Geral de Proteção de Dados na área da saúde». Universidade do Porto. https://www.bad.pt/eventos/wp-content/uploads/2018/01/CIGIA_COM_10.pdf.

SUPERVISOR, EUROPEAN DATA PROTECTION. 2018. «The History of the General Data Protection Regulation». edps.europa.eu. 2018. https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

Teresa Coelho Moreira, Paulo Novais, Francisco Pacheco Andrade, e Carneiro Davide. 2016. «Interdisciplinary Perspectives on Contemporary Conflict Resolution». *Information Science Reference - IGI Global* i (Abril): 21–33. https://books.google.com.my/books?id=ozwBDAAAQBAJ.

Tinto, Ana Rita Ramos Y Rio. 2018. «Protecção de dados de saúde: Percepção e conhecimento dos Administradores Hospitalares acerca do novo Regulamento Geral de Protecção de Dados da União Europeia». Universidade Nova de Lisboa. https://run.unl.pt/bitstream/10362/58821/1/RUN - Dissertação de Mestrado - Rita RioTinto.pdf.

União Europeia. 2016. «Tratado de Funcionamento da União Europeia». *Jornal Oficial da União Europeia*, 47–200. https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF.

———. 2021a. «Novas regras para a inteligência artificial — Perguntas e respostas Índice : Novo quadro regulamentar em matéria de inteligência artificial». Jornal Oficial da União Europeia. 2021. https://ec.europa.eu/commission/presscorner/detail/PT/qanda_21_1683.

———. 2021b. «PT ANEXO I TÉCNICAS E ABORDAGENS NO DOMÍNIO DA INTELIGÊNCIA ARTIFICIAL referidas no artigo 3.º, ponto 1». *Jornal Oficial da União Europeia*.

Veale, Michael, Reuben Binns, e Jef Ausloos. 2018. «When data protection by design and data subject rights clash». *International Data Privacy Law* 8 (2): 105–23. https://doi.org/10.1093/idpl/ipy002.

Volchkova, Ekaterina. 2018. «Sistema de Gestão Integrada de Privacidade e Segurança da Informação . Alinhamento com o Regulamento Geral sobre a Proteção de Dados». Universidade Nova de Lisboa. https://run.unl.pt/bitstream/10362/31313/1/TGI0124.pdf.