U.PORTO

2.° CICLO DE ESTUDOS

CIÊNCIAS JURÍDICO-CIVILÍSTICAS

Autodeterminação Digital no Contexto COVID 19

Eduardo Braga Tavares Paes

M
2022

Eduardo Braga Tavares Paes

Autodeterminação Digital no Contexto COVID 19

Dissertação conducente à obtenção do grau de Mestre em Ciências Jurídico-Civilísticas, realizada sob a orientação da Professora Doutora Maria Regina Redinha

Julho de 2022

RESUMO

O presente trabalho tem como objetivo examinar os impactos de algumas das medidas adotadas pelas autoridades públicas no contexto da pandemia do COVID-19, especialmente na União Europeia e mais especificamente em Portugal, relativamente ao conjunto de normas de proteção de dados.
A análise é feita partir dos conceitos jurídicos que interessam ao direito da proteção de dados, tendo como norte a autodeterminação informativa digital.
O estudo versa sobre temas concretos como o tratamento de dados de saúde pelas autoridades públicas com divulgação de informações sobre infetados, a imposição de obrigação de instalação e operação de aplicação que permite o rastreio de contatos de infetados e, também, a criação e utilização do chamado Certificado Digital COVID-19. O confronto dessas situações com o ordenamento jurídico voltado à proteção de dados pessoais permite conhecer a medida da eficácia dos instrumentos legais de proteção dos dados pessoais de saúde no ambiente da COVID-19.

Palavras-chave: Privacidade, Proteção de Dados, Direitos da Personalidade, Autodeterminação Digital, Regulamento Geral de Proteção de Dados, RGPD, Stayaway Covid, Certificado Digital COVID-19 da UE

ABSTRACT

The present paper proposes an analysis of the impacts of certain measures adopted by public authorities in the context of the COVID-19 pandemic, especially in the European Union and in Portugal, regarding data protection rules.
The analysis is based upon legal concepts related to data protection law, guided by digital informational self-determination.
This paper explores specific topics such as processing of health data by public authorities regarding disclosure of information about infected people, the obligation to install and operate an application that leads to tracing of contacts of infected people and, also, the creation and operation of COVID-19 Digital Certificates. Examining such situations with regard to data protection law is important for the effectiveness test of statutory provisions for personal data concerning health in COVID-19 environment.

Keywords: Privacy, Data Protection, Personality Rights, Self-determination, General Data Protection Regulation, GDPR, Stayaway Covid e EU Digital COVID-19 Certificate - EUDCC

SUMÁRIO

INTRODUÇÃO

Na sua premiada obra intitulada *Ensaio sobre a Cegueira*[1], JOSÉ SARAMAGO narra a história de um homem que perde a visão, acometido de uma doença (cegueira branca). A doença transmite-se, em seguida, ao seu médico, a um ladrão (que lhe furta o carro) e, assim por diante, se alastra a toda a comunidade. Esse foi o início do que se transformou numa pandemia, combatida pelas autoridades dessa sociedade imaginária com extremo rigor e violência. Uma das consequências da pandemia, segundo SARAMAGO, seria a de desvendar a verdade sobre a sociedade, revelando os seus dramas e paradoxos intrínsecos.

Parece que se trata de uma lógica inegável que SARAMAGO, como bom conhecedor da alma humana, soube extrair da realidade: a propagação de uma doença em grande escala tem a especial aptidão para desorganizar a sociedade e trazer a lume o que subjaz, escondido, nas suas camadas mais internas, os seus íntimos dilemas.

Quase um quarto de século depois da publicação do livro, já em dezembro de 2019, a Comissão Municipal de Saúde da cidade de Wuhan, a cidade mais importante e populosa da China Central, comunicou ao mundo a ocorrência de 27 casos de pneumonia por síndrome respiratória aguda causada por uma nova variante do Coronavírus (que, posteriormente, se convencionou chamar COVID-19)[2]. Essa nova doença gerava manifestações clínicas severas, diferentes das que se viam nas pneumonias comuns, com um aspeto bastante especial: a resposta aos tratamentos convencionais não era satisfatória e muitos casos conduziam ao óbito. Destacava-se, além da mortalidade acentuada, a preocupante contagiosidade.

Em pouco tempo, o vírus ultrapassou fronteiras e alcançou muitos países, em todos os continentes. A Organização Mundial de Saúde – OMS, em 30 de janeiro de 2020, declarou emergência de saúde pública de âmbito internacional e, a 11 de março de 2020, classificou a situação de saúde como pandemia[3]. No dia seguinte, em Portugal, o Conselho de Ministros se

---

[1] SARAMAGO, José - **Ensaio sobre a Cegueira**. Lisboa: Livraria Lello e Porto Editora, 2021. ISBN 978-989-8939-97-5.

[2] A propósito das circunstâncias dessa descoberta, veja-se BARATA, Clara – **O que aprendemos sobre o covid-19 nos últimos dois anos** [Em linha]. *Jornal Público*, 31 de dezembro de 2021. Atual. [Consultado em 19 de março de 2022]. Disponível em https://www.publico.pt/2021/12/31/ciencia/noticia/aprendemos-covid19-ultimos-dois-anos-1990319..

[3] A propósito da evolução cronológica da COVID-19, consulte-se **European Center for Disease Prevention and Control Cfr. European Center for Disease Prevention and Control, «Event Background COVID-19»** [Em linha]. Atual. [Consultado em 21 de abril de 2022]. Disponível em https://www.ecdc.europa.eu/en/novel-coronavirus/event-background-2019) acesso em fevereiro de 2022.

reuniu para expedir um Comunicado com diversas medidas extraordinárias de resposta à pandemia do novo coronavírus.

Sem defesa contra esse novo vírus, a humanidade viu-se diante do que se tornou a maior e mais violenta pandemia dos últimos 100 anos, de consequências económicas, políticas e sociais muito mais terríveis do que aquelas vislumbradas por SARAMAGO.

A realidade e a ficção aproximam-se quando, tal como no flagelo do Ensaio, a pandemia da COVID-19 trouxe, além da insegurança social pelos riscos envolvidos para a saúde pessoal e coletiva, a urgência em encontrarem soluções mágicas para enfrentar a ameaça, sem o cuidado de serem perfeitamente compatíveis com o ordenamento jurídico vigente.

No campo jurídico, destaca-se a repercussão da pandemia nomeadamente em relação a um ponto de interesse que se vinha tornando cada vez mais objeto de preocupação e cuidado dos juristas, especialmente na União Europeia: o da proteção da privacidade dos dados pessoais, que molda e regulamenta as políticas de uso desses dados e que estabelece diretrizes para a segurança e privacidade das informações individuais.

Apesar de todo o arcabouço legal e regulamentar destinado à proteção dos dados pessoais, fundado e reforçado por uma legislação complexa e dotada de instrumentos preciosos à sua operacionalização, os interesses que se consideravam bem protegidos ficaram sob ameaça desde o surgimento da pandemia.

YUVAL NOAH HARARI[4] asseverou, já no início de 2020, no raiar dos novos tempos, que a tempestade passaria, mas as escolhas que se fizessem naquele momento poderiam moldar as nossas vidas no futuro, especialmente aquelas situadas entre a supervisão totalitária e a cidadania fortalecida ou entre o isolamento nacionalista e a solidariedade global.

---

[4] HARARI, Yuval Noah – **O mundo após o do coronavírus** [Em linha]. *Financial Times,* 20 de março de 2020. Atual. [Consultado em 30 de fevereiro de 2022]. Disponível em https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75. O autor destaca, ainda: : "*Humankind is now facing a global crisis. Perhaps the biggest crisis of our generation. The decisions people and governments take in the next few weeks will probably shape the world for years to come. They will shape not just our healthcare systems but also our economy, politics and culture. We must act quickly and decisively. We should also take into account the long-term consequences of our actions. When choosing between alternatives, we should ask ourselves not only how to overcome the immediate threat, but also what kind of world we will inhabit once the storm passes. Yes, the storm will pass, humankind will survive, most of us will still be alive — but we will inhabit a different world*". https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

Preocupava-lhe o risco de que os tempos anormais fossem pretexto para contramedidas extremas pelas autoridades, com o objetivo de permitir ou ampliar o monitoramento da população, por meio da aplicação de técnicas de rastreamento digitais que avançassem sobre conquistas civilizacionais relativas aos direitos à intimidade e às garantias de proteção dos dados dos cidadãos.

Esta ideia foi compartilhada por muitos[5] e naturalmente conduz à indagação inevitável quanto à real efetividade das medidas legislativas, princípios e instrumentos jurídicos concebidas para a proteção dos interesses dos cidadãos num cenário não pandémico, quando postas em causa ante situações extremas tais como as que se impuseram em todos os campos.

Quando os riscos que a propagação do coronavírus trouxe para a sociedade se agigantaram e diante de toda a incerteza que passou a existir a partir do início do ano de 2020, com a possibilidade de colapso estrutural, medidas extremas, concernentes à utilização de dados pessoais como parte de medidas de impacto empregadas no combate da pandemia, que não eram antes sequer cogitadas, passaram a ser efetivamente consideradas e, em alguns casos, foram aplicadas.

No presente estudo, algumas dessas medidas serão examinadas, com abordagem do conflito de interesses jurídicos que resulta dessa situação, em especial sob o prisma do direito à privacidade e da proteção dos dados sensíveis. Procurar-se-á analisar o conjunto de riscos envolvidos em relação à autodeterminação informativa digital e aos institutos jurídicos que a procuram proteger, essenciais para o desenvolvimento da sociedade do presente e do futuro.

Sem qualquer intenção de esgotar o tema, faremos uma abordagem inicial sobre a autodeterminação digital, o conceito, evolução e abrangência atual, bem como a sua aplicação no âmbito da proteção de dados pessoais de saúde, tendo em consideração a normatização da matéria, especialmente no Direito da União Europeia e português. Em seguida, examinaremos o impacto da pandemia na autodeterminação informativa, nomeadamente quanto às ameaças que surgiram com os diversos instrumentos tecnológicos de monitorização digital.

---

[5] De entre tantos outros, veja-se TIFFANY C. LI - **Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis,** 52-3 Loyola University, *Chicago Law Journal* 767 (2021) [Em linha]. Atual. [Consultado em 18 de julho de 2022]. Disponível em https://scholars.unh.edu/cgi/viewcontent.cgi?article=1459&context=law_facpub.

A partir dessas premissas, procuraremos enfrentar o caso específico dos passaportes vacinais, a sua adoção como forma de viabilizar o retomar das atividades numa sociedade impactada pela pandemia, constituindo alternativa às medidas de *lock down.*

Nesse ponto, é bom registar, o presente trabalho não cuidará das polémicas sociais e éticas geradas pela legislação que favorece, estimula e em alguns casos impõe às pessoas a vacinação contra a COVID-19; limitar-nos-emos ao âmbito do impacto dessas medidas na autodeterminação informativa e aos princípios que a presidem.

1. AUTODETERMINAÇÃO INFORMATIVA NUM MUNDO DIGITAL - OS DADOS PESSOAIS DE SAÚDE E A SUA PROTEÇÃO NO DIREITO DA UNIÃO EUROPEIA E PORTUGUÊS

Vive-se uma era digital. Os recentes progressos tecnológicos transformam profundamente a sociedade, constituindo o divisor de águas que sinaliza o início de um tempo em que a transmissão de informações se dá em velocidade e quantidade nunca vistas.

A tecnologia desenvolvida renova-se a cada dia, à medida que se populariza e leva toda a sociedade a participar, queira-se ou não, dessa teia de comunicação chamada internet. É a sociedade da comunicação.

As tecnologias digitais de informação e comunicação (chamadas TDICs, ou, em inglês, ICT, acrónimo para *Information Communication Technologies*) amplamente difundidas, não mais exclusivas de alguns e já quase totalmente portáteis, assumem novas dimensões, públicas e privadas, ocupam espaços antes inimagináveis; são o principal meio para realizar a interatividade e a interconectividade, promover a globalização e ampliar a velocidade de acesso aos dados. Por outro lado, as informações são armazenadas numa 'memória coletiva' cujos limites tendem ao infinito. Estabelecem-se novas relações entre as pessoas, absolutamente desvinculadas de tempo e espaço e experiências inauditas na sociedade e práticas sociais. Enfim, está em curso, e com a perspetiva de cada vez mais se acentuar, a revolução da informação (também conhecida como era tecnológica ou terceira revolução industrial).

Todo este movimento e os seus efeitos na vida da sociedade e do cidadão não são ignorados pelo Direito, que precisa tutelar as relações jurídicas nascidas sob o pálio dessa nova realidade. No campo do Direito Privado, há reflexos notáveis no Direito Laboral, nos Direito dos Contratos, no Direito Bancário e assim por diante.

Ainda no campo do Direito Privado, merecem especial destaque os chamados direitos da personalidade, que são a projeção concreta do princípio constitucional da dignidade da pessoa humana[6] [7].

---

[6] **Artigo 1.º da Constituição da República Portuguesa** [Em linha]. Atual. [Consultado em 16 de fevereiro de 2022]. Disponível em https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx

[7] Sobre o princípio constitucional da dignidade da pessoa humana, veja-se MIRANDA, Jorge – **A Constituição e a dignidade da pessoa humana**. Lisboa: Didaskalia, 1999. ISSN 0253-1674. 29:1-2 (1999) 473-485. e, OLIVEIRA, Fernando António Rodrigues da Silva Coutinho **- Breves considerações a respeito do princípio da**

1.1 Direitos da Personalidade, Direito à Privacidade e Direito da Proteção de Dados

M.R. Guimarães e M.R. Redinha[8] salientam que o aumento exponencial do uso da Internet, com o surgimento das redes sociais, criou novos desafios "ao arcabouço jurídico em relação à privacidade". E acrescentam, distinguindo bem o direito de personalidade geral (fundamental) dos demais direitos da personalidade, que sobre aquele se apoiam:

> No âmbito jurídico português, esses instrumentos envolvem direitos fundamentais previstos tanto no direito constitucional quanto no penal. Os direitos de personalidade, destinados a proteger os interesses da personalidade nas relações privadas, pertencem particularmente ao direito civil, mas também protegem os indivíduos nas áreas do trabalho e do direito penal. As diferentes camadas de proteção oferecidas por esses instrumentos legais funcionam de forma complementar, muitas vezes sobrepostas a fim de proteger os diversos níveis de intrusão que afetam os interesses da personalidade. Este intrincado conjunto de ferramentas inclui um "direito de personalidade geral", uma cláusula geral que estabelece o direito ao livre e pleno desenvolvimento da personalidade, um direito fundamental onde todos os interesses conhecidos e desconhecidos, previsíveis e imprevisíveis da personalidade humana podem estar envolvidos, com base no artigo 70 do Código Civil. Esta norma permite uma atualização permanente do direito civil no contexto em evolução e dinâmica dos direitos da personalidade, esticando sua capacidade de enfrentar novos desafios e crises imprevisíveis em um mundo em mudança. Ao mesmo tempo, o Código também introduz um direito especial de personalidade, protegendo expressamente a "intimidade da vida privada", afirmando que a extensão da proteção depende da natureza do caso e da condição da pessoa.

Orlando de Carvalho pondera que o direito geral da personalidade não deve ser confundido com mera ferramenta para superar as possíveis lacunas decorrentes da previsão dos direitos de personalidades especiais; e nem mesmo admite a condensação desses direitos em um só dispositivo. O direito geral da personalidade serve como fundamento axiológico para as demais disposições legais, como referencial interpretativo. [9]

---

dignidade da pessoa humana [Em linha]. Tese de mestrado da FDUP em 1.07.2013. Atual. [Consultado em 10 de junho de 2022]. Disponível em https://sigarra.up.pt/fdup/pt/pub_geral.pub_view?pi_pub_base_id=24817.

[8] GUIMARÃES, M.R. e REDINHA, M.R. - A Portuguese Approach to Privacy in COVID-19 Times: Through the Keyhole. In E. Hondius, M. Santos Silva, A. Nicolussi, P. Salvador Coderch, C. Wendehorst and F. Zoll (eds.), **Coronavirus and the Law in Europe** [Em linha]. *Intersentia Online*, 2021. Atual. [Consultado em 15 de janeiro de 2022]. Disponível em https://www.intersentiaonline.com/permalink/1fac1271118a21090498ddef1399707b.

[9] CARVALHO, Orlando de - **Teoria Geral do Direito Civil**. 3ª ed. Coimbra: Coimbra Editora, 2012, p. 26.

Para CAIO MÁRIO DA SILVA PEREIRA, a personalidade não constitui propriamente um direito, senão um ponto em que se apoiam os direitos e obrigações[10]. ELIMAR SZANIAWSKI, por outro lado, aceita o conceito de direitos da personalidade, que qualifica como os "direitos primeiros", que tutelam a pessoa humana, individualmente considerada, representando a defesa dos atributos da personalidade[11].

Sobre os direitos da personalidade, Jorge Miranda[12], sob outra perspetiva, pontifica:

> Os direitos da personalidade remontam, em Portugal, aos "direitos originários" do Código de Seabra, uma das expressões da visão antropocêntrica ou "individuocêntrica" que o enformava, e adquirem hoje consagração formal e nominal no Código Civil de 1966. Não traduzem meras conquistas doutrinárias à margem da lei. Eram "direitos originários" o direito de existência, o direito de liberdade, o direito de associação, o direito de apropriação e o direito de defesa (arts. 359.º e segs. do Código de 1867). E atualmente preveem-se, além da tutela geral da personalidade (art. 70.º do Código de 1966), a proteção contra a ofensa a pessoas já falecidas (art. 71.º), o direito ao nome e ao pseudônimo (arts. 72.º e 74.º) a reserva do conteúdo de cartas-missivas e outros escritos confidenciais (arts. 75.º, 76.º e 77.º), o direito à imagem (art. 79.º) e a reserva sobre a intimidade da vida privada (art. 80.º) – a que podem ainda ser aditados outros direitos.

Enuncia o jurista, em seguida, sobre os direitos da personalidade:

> II – Para lá do postulado primordial do respeito da dignidade da pessoa humana (art. 1.º da Constituição), com tudo quanto implica, eles dir-se-iam corresponder a direitos como o direito à vida (arts. 24.º e 33.º, n.º 4), o direito à integridade pessoal (art. 25.º), os direitos ao desenvolvimento da personalidade, à capacidade civil, ao bom nome e reputação, à imagem, à palavra e à reserva da intimidade da vida privada (art. 26.º, n.º 1), o direito à liberdade e à segurança (art. 27.º), certas garantias relativas à informática (art. 35.º), o direito de resposta (art. 37.º), a liberdade de consciência, de religião e de culto (art. 41.º), a liberdade de criação cultural (art. 42.º), a liberdade de aprender e ensinar (art.43.º), a liberdade de escolha de profissão (art. 47.º, n.º 1), o direito ao trabalho (art. 58.º), o direito ao ambiente (art. 66.º), o direito à educação e à cultura (art. 73.º) e o direito à cultura física e ao desporto (art. 79.º). Não obstante largas zonas de coincidência, não são, contudo, assimiláveis direitos fundamentais e direitos de personalidade. Basta pensar nos demais direitos inseridos no texto constitucional que extravasam dali: o direito de acesso aos tribunais (art. 20.º, n.º1), o direito à cidadania (art. 26.º, n.º 1), as garantias da liberdade e da segurança (arts. 28.º e segs.), a grande maioria dos direitos, liberdades e garantias e dos direitos econômicos, sociais e culturais (arts. 58.º e segs.) ou os direitos fundamentais dos administrados (art. 268.º). Mas, sobretudo, são distintos o sentido, a projeção, a perspetiva de uns e outros direitos. Os direitos fundamentais pressupõem relações de poder, os direitos de personalidade relações de igualdade. Os direitos fundamentais têm uma incidência publicística imediata, ainda quando ocorram efeitos nas relações entre particulares (como prevê o art. 18.º, n.º 1, a ser estudado a seu tempo); os direitos de personalidade uma incidência privatística, ainda quando sobre ou subposta à dos direitos fundamentais. Os direitos fundamentais pertencem ao domínio do Direito constitucional, os direitos de personalidade aos do Direito civil.

---

[10] - PEREIRA, Caio Mário da Silva - **Instituições de Direito Civil**. 19ª ed. Rio de Janeiro: Forense, 2002, p. 154.

[11] - SZANIAWSKI, Elimar - **Direitos de personalidade e sua tutela**. São Paulo: Revista dos Tribunais, 1993, p.11

[12] MIRANDA, Jorge - **Curso de Direito Constitucional.** Lisboa: Universidade Católica Editora, 2016, 2, p. 58.

No direito da personalidade geral, estão abrangidos, assim, os direitos especiais à reserva da intimidade da vida privada[13], ao bom nome, à reputação, à imagem, e a um conjunto de "garantias relativas à informática". Esses direitos e garantias, intimamente vinculados ao princípio da Dignidade da Pessoa Humana[14], previstos e protegidos na Declaração Universal dos Direitos do Homem, de 10.12.1948 (art. 12.º) e na Convenção Europeia dos Direitos do Homem, de 04.11.1950 (art. 8.º), assim como na Carta dos Direitos Fundamentais da União Europeia (arts. 7.º e 8.º) e no Tratado sobre o Funcionamento da União Europeia (art. 16.º - ex artigo 286 TCE), dão amplo respaldo, na perspetiva do mundo informático, a um novo ramo do direito, que se passou a denominar Direito da proteção de dados. Essa denominação é sujeita a muitas e pertinentes críticas, uma vez que não se trata apenas de se protegerem os dados, mas também de regular o seu tratamento.[15]

Menezes Cordeiro[16] afirma:

> A expressão Direito da proteção de dados aponta, como acima referido, para uma funcionalização originária deste ramo jurídico dirigida à proteção da posição jurídica dos titulares dos dados e dos seus respetivos direitos. Todavia não é assim: tanto numa perspetiva história, como numa perspetiva dogmática atual, a produção legislativa relativa aos dados pessoais justificou-se não para acautelar os interesses individuais dos titulares dos dados – esses seriam sempre protegidos através da invocação de normas gerais relativas ao direito da personalidade – mas para regular o seu tratamento. Não se nega, naturalmente, que o direito à autodeterminação informacional e a sua proteção desempenham um papel nuclear, somente se contesta: (i) que este se encontre funcionalizado a esse único propósito; e (ii) que foram essas as *rationes* subjacentes à sua emergência e autonomia, enquanto ramo jurídico próprio."

---

[13] O direito à privacidade foi destacado, talvez pela primeira vez, num artigo publicado em 15 de dezembro de 1890, por Samuel D. Warren e Louis Brandeis. Nesse artigo, os autores destacaram que o direito da *common law*, que antes se preocupava apenas com a proteção física do indivíduo e dos seus bens (terra e rebanho), deveria abranger também o direito de aproveitar a vida (*enjoy life*) e o "direito de ser deixado em paz" (*right to be let alone*), em resposta às práticas da época, de fotografia e jornalismo. WARREN, Samuel D. e BRANDEIS, Louis - **O Direito à Privacidade** [Em linha]. *Harvard Law Review,* Vol. IV*,* 15 de dezembro de 1890. Atual. [Consultado em 28 de fevereiro de 2022]. Disponível em https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.ht ml.

[14] Sobre a fundamentação do direito à proteção de dados e sua ligação com a Declaração Universal dos Direitos do Homem, veja-se ALVES, Lurdes Dias - **Proteção de Dados Pessoais no Contexto Laboral**. Coimbra: Almedina, 2020. ISBN 978-972-40-8581-4. Pp. 13-14.

[15] Nesse sentido é a lição de CORDEIRO, A. Barreto Menezes - **Direito da proteção de dados: à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020. ISBN 978-972-40-8304-9. p. 32: "Apesar da sua rápida consolidação, a locução *Direito da proteção de dados* foi criticada por parte relevante da primeira doutrina especializada. Smitis e Bull descrevem o termo como sendo enganador, por transmitir uma ideia incorreta do seu objeto de estudo. Steinmüller, igualmente crítico da nomenclatura, sugere uma alternativa: o Direito da proteção da informação (*Informationsshutz*).

[16] Op. cit., p. 33.

Seja qual for a denominação que se queira dar a esse novo ramo do direito, o que releva é a sua proposta de regulamentar o tratamento dos dados das pessoas singulares[17], com a segurança da obediência ao direito à privacidade[18],, à imagem e ao livre desenvolvimento da personalidade, entre outros, estimulando o titular dos dados a exercer o controlo, tanto quanto possível, do uso que tais informações possam sofrer, para concretização da autodeterminação informacional a que se refere Menezes Cordeiro. Colima-se, assim, impedir que o acesso indevido aos dados possa ser causa de discriminação[19], sem opor demasiados obstáculos à circulação desses dados, essencial à fruição dos benefícios decorrentes do avanço da tecnologia.

A questão é relevante pois envolve, não apenas aspetos pessoais, mas uma riqueza em patamares inéditos, que move interesses transnacionais poderosíssimos.

Segundo Jorge M. Carvalho, "os dados pessoais são, atualmente, considerados o novo ouro ou o novo petróleo, sendo um importante bem transacionável" (…).[20]

---

[17] Segundo o artigo 4.º, inciso 2, do RGPD, a definição jurídica de Tratamento é "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição" Em linha. Atual Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32021R0953&from=PT

[18] Paulo Mota Pinto defende que a privacidade assegura o desenvolvimento da individualidade e das relações humanas de confiança, motivo pelo qual é comumente associada a um aspeto da dignidade humana. PINTO, Paulo Mota - **Direitos de Personalidade e Direitos Fundamentais: estudos**. Coimbra: Gestlegal, 2018. p. 508.

[19] "Privacidade como autodeterminação informativa/existencial e reconhecimento da construção dinâmica da identidade pessoal conjugam-se, assim, como novas formas de manifestação da proteção jurídica da pessoa humana contra as ameaças e estigmatização e discriminação oriundas do desenvolvimento tecnológico. Com efeito, a principal preocupação com relação ao armazenamento e circulação de informações relativas à pessoa humana diz respeito à sua utilização para submetê-la a estigmas, viabilizando sua discriminação perante as demais. Entre os diversos dados relativos à pessoa, alguns são especialmente idôneos a facilitar processos sociais de exclusão e segregação, razão pela qual seu controle deve ser ainda mais rigoroso. Essa é a chave de leitura adequada para compreender a qualificação de dados pessoais como sensíveis". KONDER, Carlos Nelson - O tratamento de dados sensíveis à luz da Lei 13.709/2018. In TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coordenação) - **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. 1ed. São Paulo: Thomson Reuters Brasil, 2019. P. 451.

[20] Já em 2017, a revista *The Economist* noticiava que os dados passaram a ser a nova "*commodity*", destacando a sua importância como fonte de riqueza para a era digital: "*A NEW commodity spawns a lucrative, fast-growing industry, prompting antitrust regulators to step in to restrain those who control its flow. A century ago, the resource in question was oil. Now similar concerns are being raised by the giants that deal in data, the oil of the digital era. These titans—Alphabet (Google's parent company), Amazon, Apple, Facebook and Microsoft—look unstoppable. They are the five most valuable listed firms in the world*". **The worlds most valuable resource is no longer oil but data** [Em linha]. *The Economist*, 6 de maio de 2017. Atual. [Consultado em 28 de janeiro de 2022]. Disponível em https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

Diante de interesses financeiros e empresariais poderosos é que se contrapõe o direito do cidadão de exercer o controlo do uso de suas informações, a autodeterminação informacional. Em tempos de pandemia, todo esse tema entra em ebulição em vista do tratamento, em larguíssima escala, das informações pessoais relativas à saúde.

Dados muito valiosos e em quantidade incalculável são obtidos diretamente dos seus titulares a todo o momento e sujeitos a tratamento, sob a justificativa de se fazer necessário o combate à disseminação do vírus. É claro o risco para os titulares desses dados e quase inevitável verificar-se o cenário antevisto por HARARI, de que tais dados deem ensejo a um monitoramento da população, seja por autoridades ou empresas, ou mesmo por empregadores em relação a seus empregados, avançando sobre conquistas caras da sociedade.

1.2 Autodeterminação Informativa Digital- conceito, evolução e abrangência

Conforme esclarece Menezes Cordeiro[21], o termo ´autodeterminação informacional` designa, na Alemanha, a subjetivação da posição jurídica do titular de dados pessoais e teria sido cunhado, pela primeira vez, por Steinmüller e lá consagrada pelo Tribunal Constitucional Federal. [22]

Segundo o jurista, a discussão que gerou a definição desse conceito jurídico teria ocorrido em acórdão do *BVerfG* sobre uma lei alemã que tinha por objetivo permitir a coleta de informações pessoais de variadas naturezas - a Lei dos Censos, de 1983 – *Volkszählungsgesestzes*. A Suprema Corte germânica teria examinado a referida lei sob o enfoque da sua constitucionalidade e em especial perante os princípios da dignidade da pessoa humana e o livre desenvolvimento da personalidade, presentes na constituição alemã e concluído que o direito ao livre desenvolvimento da personalidade pressupõe: (i) que o titular dos dados saiba quais informações suas são detidas por terceiros, em que momento e contexto; (ii) liberdade de agir, sem que haja um controlo constante das suas ações e decisões. O direito então reconhecido não seria absoluto, pois não haveria um controlo total sobre os dados[23].

---

[21] Op. cit. p. 257

[22] *Bundesverfassungsgericht* ou simplesmente *BVerfG*.

[23] A respeito deste tema, veja-se a premissa estabelecida pelo TJUE no acórdão proferido no julgamento dos processos apensos C-92/09 e C 93/09 (itens 47 e 48), *verbis*: "A este respeito, sublinhe-se que o artigo 8.°, n.º 1, da Carta estabelece que «[t]odas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam

Menezes Cordeiro considera que esse seria um *novo direito* e afirma que o Tribunal assim procedeu à sua concretização: "(i) em princípio, cabe ao próprio titular determinar em que termos os seus dados pessoais podem ser divulgados e tratados; (ii) as restrições ao direito à autodeterminação informacional apenas podem ocorrer quando fundadas no interesse público e encontrarem suporte constitucional bastante – o princípio da proporcionalidade deve a todo tempo ser respeitado; e (iii) a utilização dos dados pessoais deve ser limitada por lei". As dúvidas que teriam seguido à referida decisão eram sobre se esse direito à autodeterminação seria ou não oponível contra todos os terceiros ou somente no âmbito do direito público.

Esclarece-nos, o jurista, ainda, que "os desenvolvimentos viriam a demonstrar a amplitude e transversalidade desse *novo* direito"[24].

Sobre a autodeterminação informativa, merece destaque a posição adotada pelo Supremo Tribunal de Justiça de Portugal no julgamento, pela 5.ª Secção, do recurso no proc. 679/05.7 TAEVR.E2.S1, Relatora Cons. Helena Moniz (16 de outubro de 2014), "o que aqui está em causa, para além da privacidade, é o direito (fundamental) à autodeterminação informativa. Assim sendo, o simples facto de os dados poderem ser públicos não é suficiente para afastar aquela lesão. Neste sentido, constituindo a proteção concedida pelo art. 47.º, da LPDP, uma decorrência do direito à autodeterminação informativa, previsto no art. 35.º, da CRP, este protege uma amplitude de direitos fundamentais para lá do direito à privacidade. O direito à autodeterminação informacional dá "a cada pessoa o direito de controlar a informação disponível a seu respeito, impedindo-se que a pessoa se transforme em «simples objeto de informação»" (Gomes Canotilho e Vital Moreira)".[25]

A autodeterminação informacional "pode impedir que o "eu" seja objeto de apropriação pelos outros, como matéria de comunicação na esfera pública. Nela conjuga –se o direito ao segredo (à intromissão dos outros na esfera privada, com tomada de conhecimento de aspetos a ela referentes) e um direito à reserva (proibição de revelação)".[26]

---

respeito». Este direito fundamental está indissociavelmente relacionado com o direito ao respeito da vida privada consagrado no artigo 7.° desta mesma Carta. Todavia, o direito à protecção dos dados pessoais não é uma prerrogativa absoluta, mas deve ser tomado em consideração relativamente à sua função na sociedade (v., neste sentido, acórdão de 12 de junho de 2003, Schmidberger, C-112/00, Colect., p. I-5659, n.° 80 e jurisprudência aí referida)."

[24] Op cit p. 259

[25] - Em relação à citação doutrinária de CANOTILHO, Gomes e MOREIRA, Vital - **Constituição da República Portuguesa Anotada**. 4.ª ed. Coimbra: Coimbra Editora, 2007. ISBN: 9789725405413. Vol. 1, pp. 551.

[26] SOUSA Ribeiro, J. - A tutela de bens da personalidade na Constituição e na jurisprudência constitucional portuguesas. In **Estudos de Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho.** Coimbra: Coimbra

O Tribunal Constitucional português, no julgamento da constitucionalidade dos artigos 2.º e 3.º Decreto n.º 139/X da Assembleia da República, proferiu o acórdão n.º 442/2007[27] (processo n.º 815/07), sendo Relator o Conselheiro Joaquim de Sousa Ribeiro, em que ficou assente que:

> Das três manifestações em que se fracciona o conteúdo do direito à reserva da intimidade da vida privada e familiar – direito à solidão, direito ao anonimato, e autodeterminação informativa – é esta última a sua expressão cimeira e mais relevante, e aquela que particularmente nos interessa quando está em causa o estatuto constitucional do sigilo bancário. Por *autodeterminação informativa* poderá entender-se o direito de subtrair ao conhecimento público factos e comportamentos reveladores do modo de ser do sujeito na condução da sua vida privada. Compete a cada um decidir livremente quando e de que modo pode ser captada e posta a circular informação respeitante à sua vida privada e familiar.

E em recente acórdão daquela mesma Corte Constitucional sobre a polêmica questão dos metadados[28], ficou assente o respeito à autodeterminação informativa, decorrente do direito ao sigilo de dados pessoais e inerente ao livre desenvolvimento da personalidade, como se vê do seguinte trecho do voto do Relator:

"Ademais, mesmo fora do domínio das comunicações, o direito ao livre desenvolvimento da personalidade abrange o direito ao sigilo dos dados pessoais — que, como se viu, não compreende somente aqueles que diretamente identificam uma pessoa, mas também aqueles que, sem esforço excessivo, permitam chegar a essa identificação — como se concluiu no Acórdão n.º 464/2019: *«Pode, na verdade, afirmar-se que o segredo dos dados pessoais e o poder de controlo do sujeito sobre os mesmos constituem uma garantia do direito ao livre desenvolvimento da personalidade enquanto possibilidade de «interiorização autónoma» da pessoa ou o direito a «autoafirmação» em relação a si mesmo, contra quaisquer imposições heterónomas (de terceiros ou dos poderes públicos). Este direito à "autoafirmação" dá guarida a vários «direitos de personalidade inominados mesmo que não especificamente positivados na Constituição, como por exemplo, o direito aos documentos pessoais e o direito à autodeterminação informativa quanto a dados pessoais constantes de ficheiros manuais ou informáticos, o direito à confidencialidade de dados pessoais constantes de atos ou decisões públicas respeitantes ao estado civil, o direito de não ser espiado no desenvolvimento de atividades lícitas (cf. Gomes Canotilho/Vital Moreira, Vol. I, ob. cit., pp. 464-465».*"

Editora. ISBN 9789723220537. Vol. III, "Direitos e Interconstitucionalidade: entre Dignidade e Cosmopolitismo", p. 853.

[27] Disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20070442.html

[28] Tribunal Constitucional, Processo n.º 828/2019, acórdão n.º 268/2022, Plenário, Relator Conselheiro Afonso Patrão, julgado em 04.2022. O Tribunal declarou a inconstitucionalidade das normas dos artigos 4.º e 6.º da Lei n.º 32/2008, de 17 de julho, que determinam a conservação, pelos fornecedores de serviços de telecomunicações e comunicações eletrónicas, de todos os dados de tráfego e de localização relativos a todas as comunicações ou sua tentativa, pelo período de um ano, com vista à sua eventual futura utilização para prevenção, investigação e repressão de crimes graves.

Interessa-nos especificamente a autodeterminação informativa (ou informacional) que se realiza no mundo digital onde atualmente estão, como já visto, os maiores riscos para a privacidade e o desenvolvimento da personalidade dos cidadãos, até por estar aí armazenada eletronicamente uma quantidade de informações pessoais que nem mesmo os próprios cidadãos supõem e que, muitas vezes, lhes são completamente desconhecidas. É a autodeterminação digital, da qual cuida o presente estudo.

1.3 União Europeia e Portugal – Ou RGPD e a legislação portuguesa

O direito à proteção dos dados pessoais, como se viu em cima, é considerado um direito fundamental na União Europeia e está previsto na Carta dos Direitos Fundamentais da União Europeia (CDFUE), especificamente no seu artigo 8.°, assim como no artigo 16.°, n.° 1, do Tratado sobre o Funcionamento da União Europeia (TFUE). Vincula-se intimamente ao próprio direito à privacidade, previsto no artigo 7.º da CDFUE.

Merece ainda ser mencionada a Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981, que foi o primeiro instrumento internacional no domínio da proteção de dados[29] e tinha por objetivo "garantir [...] a todas as pessoas singulares [...] o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de caráter pessoal".[30]

No campo do direito derivado[31], a partir da década 90, a Comunidade Europeia passou a adotar novos mecanismos legais para a proteção dos dados pessoais; destaca-se a Diretiva 95/46/CE (Diretiva do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa

[29] Informação constante em https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf (acedido em janeiro de 2022)

[30] A Convenção foi recentemente modernizada com a adoção do Protocolo de Modificação CETS n.º 223 a 18 de abril de 2018. Com acesso em março de 2022 (https://rm.coe.int/16808ade9d)

[31] - O Direito derivado ou secundário é "o corpo legislativo que decorre dos princípios e objetivos consagrados nos Tratados" e "inclui regulamentos, diretivas, decisões, recomendações e pareceres". Definição encontrada no site institucional da Comissão Europeia - https://ec.europa.eu/info/law/law-making-process/types-eu-law_pt

à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados), que estabeleceu as condições para o tratamento dos dados pessoais e os direitos dos titulares e previu a criação de órgãos independentes para o controlo nos Estados-Membros[32].

Já no século XXI, adotou-se a Diretiva 2002/58/CE de 12 de julho de 2002[33], relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, a complementar as regras da Diretiva 95/46. Em 2008, veio a Decisão-Quadro 2008/977/JAI que regulamentou a proteção dos dados pessoais no domínio da cooperação judiciária em matéria penal e policial.

Em 2016, todo a regulamentação jurídica relativa à proteção de dados na União Europeia foi revisto e os conceitos consolidados em Regulamento (Regulamento UE 2016/679, conhecido como Regulamento Geral sobre Proteção de Dados – RGPC)[34] [35]. O RGPD entrou em vigor no dia 25 de maio de 2016 simultaneamente, em todos os Estados Membros da União Europeia. Como se trata de um Regulamento, não houve necessidade de transposição para o direito interno, impondo-se a disciplina uniformizada para os Estados Membros em maio de 2018, data em que terminou o período transitório de dois anos para que se desse a necessária conformação com as obrigações ali previstas (muitas das quais, é bom que se diga, já existiam sob a égide da Diretiva 95/46/CE).

O RGPD é um instrumento para a unificação do direito da proteção de dados nos Estados-Membros, com o objetivo de possibilitar uma aplicação homogénea do direito no limite territorial da União, para assim consolidar o Mercado Único. De lembrar que, de acordo com o artigo 288.ª do TFUE, "(...) O regulamento tem caráter geral. É obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.", o que lhe permite unificar o direito regulado de uma só vez em todos os Estados-Membros, independentemente de se abrir

---

[32] A Diretiva95/46/CE foi revogada a partir de 25 de maio de 2018, pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[33] Essa Diretiva foi alterada pela Diretiva2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006. Porém, esta última Diretiva veio a ser considerada inválida pelo Tribunal de Justiça, por violação grave do princípio da proporcionalidade, à luz dos artigos 7.º, 8.º e 52.º n.º1 da Carta (Tribunal de Justiça da UE, Grande Secção, acórdão de 8 de abril de 2014, - processos apensos C-293/12 e C-594/12, disponível em https://curia.europa.eu/juris/liste.jsf?language=pt&num=C-293/12).

[34] - Revogou a Diretiva95/46, a Diretiva (UE) 2016/680 e a Decisão-Quadro 2008/977/JAI, sendo aplicável a partir de 25 de maio de 2018.

[35] Quanto às instituições e órgãos da União vinculados especificamente à proteção de dados, situação que era regida pelo Regulamento (CE) n.° 45/2001[35], foi criado novo cenário, com a edição do Regulamento (UE) 2018/1725, que revogou o anterior desde 11 de dezembro de 2018 e procurou harmonizar a matéria com o RGPD.

espaço, no próprio RGPD, para que o legislador de cada Estado-Membro possa atuar nas chamadas cláusulas de abertura que vão concretizar o Regulamento e permitir a sua adaptação às características e necessidades locais.

Também merece ser destacado o Regulamento UE 2018/1725, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados. O RGPD previa a adaptação do Regulamento (CE) n.º 45/2001 a fim de garantir um regime de proteção de dados sólido e coerente na União e de permitir a sua aplicação em paralelo com o RGPD. Foi esse o objetivo concretizado pelo Regulamento 2018/1725.

E é nessa perspetiva que atua o legislador português, editando regras de execução do RGPD no âmbito nacional, sempre nos limites das cláusulas de abertura estabelecidas pelo Regulamento e com respeito aos princípios ali estabelecidos[36] [37].

No âmbito do direito interno, é bom destacar que o tema da proteção de dados, como já visto, tem fundamento constitucional. Segundo Menezes Cordeiro,[38] "o Direito constitucional português tem uma longa tradição na regulamentação dos dados pessoais e do seu tratamento. A Constituição da República Portuguesa terá sido, à luz dos elementos recolhido, a primeira Lei Fundamental a reconhecer, diretamente, alguma proteção constitucional aos titulares de dados pessoais. O núcleo embrionário do Direito da proteção de dados contemporâneos surgia já na versão original do artigo 35.º da CRP".

Segundo o jurista, a atual redação do artigo 35.º, a partir da Revisão Constitucional de 1997, teria sido motivada pelo conteúdo da Diretiva n.º 95/46[39]. Seja como for, a norma constitucional é bastante clara ao assegurar o direito ao conhecimento das informações pessoais pelo seu titular, à sua retificação e atualização, ao remeter à lei o estabelecimento das condições

---

[36] Em caso de contradição entre o Regulamento e a lei interna dos Estados-Membros, deve prevalecer o direito europeu, como ficou assente no julgamento pelo TJUE do processo C-106/77 (acórdão de 09.03.1978 – Simmenthal), *verbis*, "O juiz nacional responsável, no âmbito das suas competências, por aplicar disposições de direito comunitário tem obrigação de assegurar o pleno efeito de tais normas, decidindo, por autoridade própria, se necessário for, da não aplicação de qualquer norma de direito interno que as contrarie, ainda que tal norma seja posterior, sem que tenha de solicitar ou esperar a prévia eliminação da referida norma por via legislativa ou por qualquer outro processo constitucional".

[37] Disso decorre a especial relevância aos 173 considerandos (*consideranda*), que ajudam a interpretar os artigos do Regulamento, expressando-se em todas as suas 24 versões.

[38] Op cit. p. 73

[39] - Op cit p. 75

para o tratamento automatizado, conexão, transmissão e utilização desses dados, garantindo a sua proteção.

No plano da legislação ordinária portuguesa, a primeira menção se faz ao artigo 70.º, n. 1.º, do Código Civil de 1966, que institui uma cláusula geral para assegurar os direitos da personalidade e proteger seu titular contra qualquer ofensa ilícita ou ameaça de ofensa à sua personalidade física ou moral. Segundo Paulo Mota Pinto[40], este direito confere uma tutela geral que, além e se ajustar melhor à complexidade da personalidade humana, pode abranger bens da personalidade não tipificados em lei. Por isso mesmo, o direito da personalidade seria "aberto, sincrônica e diacronicamente, permitindo a tutela de novos bens, e face a renovadas ameaças à pessoa humana".

Além do Código Civil, destaca-se a Lei n.º 2/73, de 10 de fevereiro, e o Decreto-Lei n.º 555 /73, de 26 de outubro[41]. No início da década de 90, foi publicada a Lei 10/91, de 29 de abril, voltada especificamente para a "proteção de dados pessoais face à informática". Essa lei foi revogada pela Lei n.º 67/98 (Lei de Proteção de Dados Pessoais) que, por sua vez, veio a ser substituída pela lei que hoje disciplina a matéria no âmbito do direito interno – a Lei n.º 58/2019, de 08 de agosto, também conhecida como a Lei de Execução do RGPD[42].

Por fim, também merece referência a Lei n.º 27/2021 de 17 de maio, que institui a Carta Portuguesa de Direitos Humanos na Era Digital e que contém regras aplicáveis ao direito da proteção de dados digitais. Essa Lei contém muitas regras programáticas, repete princípios e direitos fundamentais já consagrados (liberdade de expressão, sigilo das telecomunicações, proteção de dados, identidade e bom nome, ciber segurança, entre outros); trazendo parca inovação ao ordenamento jurídico português. Os temas ali tratados já o haviam sido e de forma exaustiva pela Constituição da República, pelos Regulamentos e Diretivas da União e pela própria legislação nacional.[43]

---

[40] PINTO, Paulo Mota. *Op. Cit*. p. 493/494.

[41] Ambos os diplomas tratavam do Registo Nacional de Identificação e já cuidavam da proteção de dados pessoais.

[42] - Há outros diplomas mais específicos, mas que também cuidam da proteção de dados pessoais, como a Lei n.º 41/2004 (dados pessoais e privacidade nas telecomunicações), Lei n.º 1/2005, de 10 de janeiro e diplomas subsequentes (videovigilância), Lei n.º 12/2005 (informação genética pessoal e dados de saúde), Lei n.º 59/2019, de 08 de Agosto (prevenção, deteção, investigação ou repressão a infração penal).

[43] A Comissão Nacional de Proteção de Dados - CNPD, em parecer produzido a respeito do Projeto de Lei n.º 473/XIV/1.ª da AR (parecer 2020/116 de 28 de setembro de 2020), que veio dar origem à Lei n.º 27/2021, apresentou severas críticas ao projeto e destacou que "não obstante a invocação de um extenso conjunto de instrumento jurídicos, a maior parte deles de cariz internacional ou europeu, e de outras iniciativas de debates sobre a matéria, no articulado do Projeto parece esquecer-se que muitos dos direitos, aqui consagrados como digitais, já estão reconhecidos, e com um âmbito bem delimitado, em instrumentos jurídicos vinculativos para o

Todos esses diplomas tiveram como uma das suas principais finalidades dar efetividade ao direito fundamental à proteção de dados pessoais, incorporando ao ordenamento jurídico os meios e instrumentos jurídicos próprios para garantir que fosse alcançado tal objetivo.

A proclamação de princípios jurídicos, como se fez no artigo 5.º do RGPD, o estabelecimento de regras específicas para autorizar o tratamento lícito de dados, inclusive no que respeita ao consentimento para esse tratamento, quando exigível, como está bem disciplinado nos artigos 6.º a 11.º do RGPD, a enunciação de direitos do titular dos dados nos artigo 12.º a 23.º do RGPD, bem como de obrigações para aquele responsável pelo tratamento dos dados pessoais previstas nos artigos 24.º a 31.º, tudo isto gera concretude e municia o titular de dados pessoais de instrumentos para que seus direitos sejam respeitados e, tanto quanto possível, possa exercer, na forma prevista na lei, a autodeterminação informativa digital.

Parece importante relevar o direito de informação e de acesso (arts. 13.º, 14.º e 15.º do RGPD), assim como o direito de retificação, de apagamento e de oposição (arts. 16.º, 17.º e 21.º do RGPD). São direitos subjetivos fundamentais para o exercício da autodeterminação informativa, em conformidade com o conceito empregado pelo Tribunal Constitucional Português no acórdão acima citado, que envolveria o "direito de subtrair ao conhecimento público factos e comportamentos reveladores do modo de ser do sujeito na condução da sua vida privada".

1.4 Conceito de Dados Pessoais de Saúde no RGPD e na legislação portuguesa

O conceito de dados pessoais está claro no artigo 4.º, 1) do RGPD: "«Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".

Estado português. E, portanto, consagrados e delimitados em termos tais que não podem agora, no plano legislativo nacional, ser alterados, mesmo que num sentido expansivo das posições subjetivas dos titulares dos dados."

A definição é bastante clara, não obstante possa suscitar, concretamente, diversas questões sobre a extensão dos seus elementos conceituais.

O primeiro elemento adotado pelo RGPD merece especial reflexão: que tipo de informação seria abrangida pelo instituto jurídico? MENEZES CORDEIRO[44] defende que a aceção a ser atribuída à expressão seja a mais ampla, ultrapassando os limites adotados pelo direito de personalidade, de tal forma que abranja todas as informações relativas à pessoa singular. O jurista se apoia em decisão do Tribunal Constitucional alemão, de que não haverá informação pessoal, "por muito insignificante ou fútil que possa parecer" que não mereça a proteção jurídica. E conclui o argumento ao referir-se a várias decisões do Tribunal Europeu dos Direitos Humanos, em que se consideram abrangidas no conceito de dados pessoais as informações relativas à vida privada bem como as que concernem a vida profissional e social.

De entre todas essas decisões do TEDH acima referidas, merece especial destaque a proferida no julgamento do caso AMANN v. SWITZERLAND (Application n.º 27798/95), de 16 de fevereiro de 2000, em que o Tribunal definiu a extensão a ser dada ao conceito de "vida privada", conforme expresso no artigo 8.º, 1, da Convenção Europeia dos Direitos do Homem, e apontou que esse instituto abrange o direito de estabelecer e desenvolver relações com outras pessoas e que não haveria razões que justificassem a exclusão de atividades de índole profissional ou de negócios daquele conceito, com apoio em precedente daquela mesma corte de justiça. Essa interpretação é correspondente à que se atribui ao artigo 1.º da Convenção n.º 108, de 28 de janeiro de 1981, do Conselho da Europa (Convenção para a Proteção de Indivíduos Relativamente ao Tratamento Automático de Dados Pessoais) e que, já então, definia informação pessoal como "qualquer informação relativa a uma pessoa identificada ou identificável" (artigos 1.º e 2.º). [45] Essa posição ajuda a definir a extensão de dados pessoais, para abranger todos os dados pertinentes a uma pessoa, não importa qual seja a relevância de tais dados.

---

[44] Op. Cit. Pág. 107 e 108.

[45] "The Court reiterates that the storing of data relating to the "private life" of an individual falls within the application of Article 8 § 1 (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 22, § 48). It points out in this connection that the term "private life" must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life" (see the Niemietz v. Germany judgment of 16 December 1992, Series A no. 251-B, pp. 33-34, § 29, and the Halford judgment cited above, pp. 1015-16, § 42)."

Também outro aspeto deve ser destacado. Os dados pessoais compreendidos na proteção do RGPD são os relativos às pessoas singulares, independentemente da sua nacionalidade ou residência. Não abrangem os dados de pessoas coletivas[46]. Igualmente não envolvem aqueles relativos a pessoas falecidas[47], os quais, entretanto, no âmbito de Portugal, são dotados de mecanismos de proteção previstos na lei portuguesa de execução do RGPD[48].

Porém ao presente estudo não interessam todos os dados pessoais, senão uma categoria, que merece mais elevada proteção; os chamados dados especiais ou sensíveis, que, "pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais".[49] São, conforme definição objetiva do artigo 9.º, os dados que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, os dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

---

[46] Não assim as pessoas coletivas, conforme Considerando n.º 14 do RGPD "(14) A proteção conferida pelo presente regulamento deverá aplicar-se às pessoas singulares, independentemente da sua nacionalidade ou do seu local de residência, relativamente ao tratamento dos seus dados pessoais. O presente regulamento não abrange o tratamento de dados pessoais relativos a pessoas coletivas, em especial a empresas estabelecidas enquanto pessoas coletivas, incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva."

[47] Considerando n.º 27 – "O presente regulamento não se aplica aos dados pessoais de pessoas falecidas. Os Estados-Membros poderão estabelecer regras para o tratamento dos dados pessoais de pessoas falecidas".

[48] A Lei n.º 58/2019, de 08 de agosto, cuida do tema no seu artigo 17.º, *in verbis*: 1 - Os dados pessoais de pessoas falecidas são protegidos nos termos do RGPD e da presente lei quando se integrem nas categorias especiais de dados pessoais a que se refere o n.º 1 do artigo 9.º do RGPD ou quando se reportem à intimidade da vida privada, à imagem ou aos dados relativos às comunicações, ressalvados os casos previstos no n.º 2 do mesmo artigo. 2 - Os direitos previstos no RGPD relativos a dados pessoais de pessoas falecidas, abrangidos pelo número anterior, nomeadamente os direitos de acesso, retificação e apagamento, são exercidos por quem a pessoa falecida haja designado para o efeito ou, na sua falta, pelos respetivos herdeiros. 3 - Os titulares dos dados podem igualmente, nos termos legais aplicáveis, deixar determinada a impossibilidade de exercício dos direitos referidos no número anterior após a sua morte."

[49] Transcrição de parte do Considerando 51 do RGPD – "Tais dados pessoais não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que o direito dos Estados-Membros pode estabelecer disposições de proteção de dados específicas, a fim de adaptar a aplicação das regras do presente regulamento para dar cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento. Para além dos requisitos específicos para este tipo de tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. Deverão ser previstas de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der o seu consentimento expresso ou para ter em conta necessidades específicas, designadamente quando o tratamento for efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais."

É clara a posição de maior fragilidade, pela possível exposição a situações de discriminação ou preconceito (princípio da não discriminação - artigo 21.º da Carta dos Direitos Fundamentais da União Europeia – CDFUE), com possível perturbação dos direitos fundamentais da personalidade, que os titulares de tais dados ostentam, o que justifica plenamente a preocupação do legislador europeu. Para Canotilho e Moreira, quanto mais os dados refiram-se à personalidade, à dignidade, e à autodeterminação, maior a necessidade de se restringir a recolha e utilização[50].

Os dados pessoais de saúde encaixam-se nesse perfil e, assim, são tratados pelo artigo 4.º, 15, do RGPD que os conceitua como aqueles "relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde".[51] Para Sérgio Deodato, "os dados pessoais de saúde incluem toda a informação relativa à saúde de uma pessoa que é usada pelos profissionais de saúde na sua relação assistencial e que geralmente é registada nos denominados processos clínicos".[52]

Patrícia Cardoso Dias[53], ao tratar dos dados especiais de saúde, leciona que "a especial sensibilidade desta categoria de dados pessoais convoca uma tutela qualificada atendendo aos impactos negativos que se podem produzir na esfera jurídica pessoal do titular" e que a informação de saúde está "sujeita a um regime de proteção reforçado por corresponder a uma categoria de dados pessoais que é suscetível de gerar ou promover a estigmatização e a discriminação dos respetivos titulares por via da revelação de aspetos da sua fisiologia orgânica que enformam o reduto máximo da privacidade".

---

[50] Op. cit. p. 557.

[51] A Lei n.º 12/2005 de 26 de janeiro no artigo 2.º conceitua do seguinte modo dados de saúde: "todo o tipo de informação direta ou indiretamente ligada à saúde, presente ou futura, de uma pessoa, quer se encontre com vida ou tenha falecido, e a sua história clínica e familiar". A Lei 58/2019 de 8 de agosto, até pela sua própria natureza (de execução de um Regulamento), não contém uma definição de dados especiais de saúde. Porém trata desses dados especificamente nos seus artigos 29.º e 30.º.

[52] - DEODATO, Sérgio - **A proteção dos dados pessoais de Saúde**. Lisboa: Universidade Católica Editora. 2017 .ISBN 9789725405789. p. 13.

[53] DIAS, Patrícia Cardoso - **Proteção de dados pessoais no contexto da pandemia provocada pelo novo coronavírus SARS-COV-2: aspetos ético-jurídicos relevantes da proteção de dados de saúde no âmbito da emergência de saúde pública** *Revista Julgar Online* [Em linha]. Janeiro de 2021-1, Atual. [Consultado em 28 de abril de 2022]. Disponível em http://julgar.pt/protecao-de-dados-pessoais-no-contexto-da-pandemia-provocada-pelo-novo-coronavirus-sars-cov-2-aspetos-etico-juridicos-relevantes-da-protecao-de-dados-de-saude-no-ambito-da-emergencia-de-saude-publica/ (acesso em junho de 2022).

São dados sensíveis e por isso mesmo os que sujeitam o seu titular aos maiores riscos de discriminação ou estigmatização, especialmente no ambiente de crise da pandemia.

2 A COVID-19 E A PROTEÇÃO DOS DADOS PESSOAIS DE SAÚDE

2.1 A pandemia da COVID-19 e seu impacto no direito à proteção de dados

Como foi mencionado previamente, um dos impactos relevantes da COVID-19 no sistema jurídico do mundo ocidental deu-se no campo do direito da proteção de dados. A pandemia mostrou-se desafiadora neste ponto, uma vez que, para contenção da doença, os governos deram ênfase à digitalização dos serviços públicos e lançaram mão dos dados de saúde dos cidadãos, necessários para pôr em prática as medidas sanitárias, em quantidade impressionante. Também as empresas privadas desenvolveram novas tecnologias, inclusive de rastreamento de contatos, que proporcionaram a captação cada vez maior de informações (sensíveis) de saúde e, assim, colocaram-se como forças auxiliares dos órgãos públicos, no combate à pandemia.

Com a justificativa, por vezes aceitável e até adequada, de que atuavam com esse objetivo de cooperação, promoveram a captação de dados de saúde e o seu tratamento em níveis que ainda não tinham sido vistos.

Vejam-se os seguintes exemplos:

Em abril de 2020, foi anunciada uma parceria entre a Google e a Apple com o objetivo de disponibilizar uma plataforma, operável tanto no ambiente Android como IOS, que deveria viabilizar o conhecimento dos contatos do usuário (*contact tracing platform*), com a utilização da tecnologia Bluetooth.[54] No comunicado, as empresas destacaram a necessidade de observarem a privacidade e a segurança dos titulares dos dados, assim como respeitar o seu consentimento; anunciaram, também, que as informações do projeto seriam públicas, a viabilizar o controlo por terceiros.

[54] No anúncio da parceria, foi esclarecido o seguinte: "*Across the world, governments and health authorities are working together to find solutions to the COVID-19 pandemic, to protect people and get society back up and running. Software developers are contributing by crafting technical tools to help combat the virus and save lives. In this spirit of collaboration, Google and Apple are announcing a joint effort to enable the use of Bluetooth technology to help governments and health agencies reduce the spread of the virus, with user privacy and security central to the design. Since COVID-19 can be transmitted through close proximity to affected individuals, public health officials have identified contact tracing as a valuable tool to help* ***contain its spread*****".** https://www.apple.com/ br/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracingtechnology/ Acesso em Janeiro 2022.

A despeito dessas premissas e compromissos, é inegável que a quantidade de dados de saúde que uma solução tecnológica dessas, , desenvolvida com o propósito de combater a pandemia, acaba por absorver é enorme, proporcional ao risco que decorre para a privacidade das pessoas, especialmente no ambiente pandémico. A conjugação de dados de geolocalização com dados sensíveis de saúde em tal magnitude representa um enorme risco para a privacidade.

A Organização Mundial de Saúde (OMS), em manifestação sobre a utilização desse tipo de tecnologia para o combate à pandemia, já ponderava, em 28 de maio de 2020, que:

> Through their products, services or platforms, some private companies capture as much data as governments gather. Such companies may develop or are even sharing their own digital proximity tracking applications with governments and, in some cases, are given the responsibility for collecting and analysing the data thus harvested. Moreover, there is a broader concern that private companies may permanently integrate their commercial products, services and architecture within public health infrastructures.[55]

O *The Washington Post*, em 20 de abril de 2020, publicou uma carta aberta do CEO do *Facebook*, MARK ZUCKERBERG, em que este reconheceu que, com bilhões de usuários, a plataforma reunia as condições para obtenção de dados pessoais em escala mundial, dispondo-se, assim, a utilizar essa situação para captar as informações e fornecê-las aos governos, com o objetivo de ajudar a estruturar estratégias de combate à pandemia. A propósito, veja-se o trecho seguinte da referida carta aberta:

> *Getting accurate county-by-county data from across the United States is challenging, and obtaining such focused data from across the whole world is even harder. But with a community of billions of people globally, Facebook can uniquely help researchers and health authorities get the information they need to respond to the outbreak and start planning for the recovery*.[56]

Em reforço dos seus argumentos, ZUCKERBERG acrescentava:

> *Data like this can unlock a lot of good. Since we're all generating data from apps and devices every day, there will likely be many more opportunities to use the aggregate data to benefit public health. But it's essential that this is done in a way that protects people's privacy and respects human rights. It's important that organizations involved in this work commit to doing it in a way that protects people's information and that any data collected is used solely for responding to public health emergencies and for other crisis response efforts. Fighting the pandemic has required taking unprecedented measures across society, but it shouldn't mean sacrificing our privacy.*

---

[55] Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing, Interim guidance, de 28.05. 2020 (acedido em junho 2022): https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1

[56] A carta de Mark Zuckerberg está inteiramente disponível em: (https://www.washingtonpost.com/opinions/2020/04/20/how-datacan-aid-fight-against-covid-19/)

Estes são, pois, bons e claros exemplos, como nunca, de como as informações pessoais de saúde foram e continuam a ser usadas por empresas e pelos agentes governamentais, por vezes em interação, em quantidade massiva nos momentos de ameaça.

A afirmação de valores e boas intenções, como aquela do FB, de que "*data like this can unlock a lot of good*" ou de que a utilização das informações se deve dar com respeito à privacidade do cidadão, por si só, não são bastantes para afastar os gravíssimos riscos inerentes à opção político-jurídica de se abrirem as portas que protegem os dados pessoais de saúde. Não se pode ser ingénuo a ponto de considerar que tais dados pessoais não possam ser desviados para outras finalidades ou mesmo que sejam objeto de tratamento sem os cuidados que as normas exigem.

Dúvidas existirão sempre sobre os destinos da enorme quantidade de dados coletados, a finalidade da sua utilização (que deve ser exclusivamente o atendimento às medidas de saúde pública emergentes da pandemia) assim como a observância ao princípio da proporcionalidade, que procura afastar os abusos. Assim, também haverá incertezas quanto ao controlo a ser exercido sobre tais condutas e projetos, às medidas para eventual reajuste e ao tratamento dos dados no período pós-pandemia.

Algumas medidas, como a anonimização de dados, sabe-se bem, não são sempre efetivas. Dados anonimizados muitas vezes podem ser "desanonimizados" [57] e até com certa facilidade, com ocorreu em 2006 em relação a dados anónimos fornecidos à NETFLIX[58]. As novas tecnologias e o desenvolvimento assombroso das capacidades informáticas e da inteligência artificial (IA) reduzem a eficácia das medidas de proteção da privacidade, uma vez que os dados pessoais sejam inseridos na *internet*. Por isso o risco enorme que corremos quando os dados disponibilizados dizem respeito à saúde, por mais justificáveis que sejam os propósitos. E tudo se amplia quando os dados são utilizados pelos governos e por grandes plataformas da *internet*.

---

[57] VÉLIS, Carissa - **Privacidade é Poder, por que razão e como devemos recuperar o controle dos nossos dados, Temas e Debates**. Lisboa: Bertrand Editora Ltda., 2022. ISBN 978-989-644-688-8.

[58] Segundo VÉLIS, *op. cit*. p. 32, "em 2006, a Netflix publicou 10 milhões de classificações de filmes de meio milhão de clientes como parte de um desafio às pessoas para conceberem um melhor algoritmo de recomendações. Os dados eram supostamente anónimos, mas os investigadores da Universidade do Texas, em Autin, provaram que conseguiram reidentificar as pessoas comparando classificações e registos data/hora com a informação na Internet Movie Database (IMBb). Por outras palavras, se vir um filme numa detemrinada noite na Netflix que gostou dele e depois também o classificar na IMDb, os investigadores poderão inferir que foi o leitor o autor das duas classificações."

Numa situação como a anteriormente descrita, é claro o risco de as informações chegarem às pessoas (singulares ou coletivas) interessadas em fazer delas o comércio de dados que tanto assusta, pela invasão da privacidade e capacidade para gerar discriminações, fraudes, extorsões, além de outras consequências conhecidas. Além disso, há sempre o risco de as próprias autoridades utilizem esses dados, durante ou depois da pandemia, para fins não estritamente ligados às atividades de saúde pública.

A armazenagem de informações pelas autoridades estatais pode, pois, fazer-se de tal forma que permita o seu uso para outros fins, como se verá mais adiante neste estudo.

HARARI, no seu texto já referido, descreveu as medidas drásticas adotadas pela China nos primeiros dias da pandemia com o objetivo de controlar a propagação do vírus. Destacou que, pela monitorização dos *smatphones*, juntamente com centenas de milhões de câmaras de reconhecimento facial e a partir de informações obtidas dos próprios cidadãos sobre a sua temperatura corporal e as condições médicas, as autoridades chinesas puderam, não apenas identificar suspeitos de serem portadores do vírus, como rastrear os seus movimentos e até os seus contatos, enquanto aplicativos alertavam a população contra a proximidade de infetados.

HARARI esclarece que esse tipo de tecnologia não estava limitado à Ásia Oriental. Em Israel, o então primeiro-ministro Benjamin Netanyahu autorizou a Agência de Segurança a empregar tecnologia de rastreamento, normalmente dedicada ao combate de terroristas, para vigiar pessoas infetadas por coronavirus, medida que se adotou sob os efeitos de um decreto de emergência[59].

Como se constata, as medidas para enfrentar a pandemia podem, facilmente, prestar-se a desviar os dados de saúde para outros fins perseguidos pelas autoridades estatais ou pelas

[59] Para compreensão da extensão das restrições impostas em Israel, veja-se o artigo da professora Tamar Hostovsky Brandes, intitulado :Israel's Perfect Storm: Fighting Coronavirus in the Midst of a Constitutional Crisis – no sítio eletrónico de Verfassungsblog on mattrers constitucional. Ressalta-se o seguinte trecho impressionante: *The Knesset Service Affairs Committee approved the employment of military cellular tracking technology pursuant to article 7(B)(6), of the General Security Service Law, 5762-2002, which allows the service to perform "activities in any other area determined by the Government, with the approval of the Knesset Service Affairs Committee, which is designed to safeguard and promote State interests vital to the national security of the State". The authorization includes a sunset clause which determines that it will end on April 30th, 2020.The committee required the state to examine less invasive alternatives during this period, and to present them to the committee. The information the Service is allowed to share with the Ministry of Health includes real-time locations of confirmed Covid-19 patients in the 14 days that preceded diagnosis and the personal details of individuals who came into "close contact" with such patients. The Ministry of Health will use this information to inform those who came in contact with a Covid -19 patient that they are required to enter isolation.*

empresas privadas. O risco é enorme, ainda mais sob a perspetiva proposta por HARARI, relativa à realização de monitoramento "*under the skin*".[60]

2.2 Fundamentos Jurídicos para a proteção de dados pessoais - Aplicação das regras que estabelecem direitos e garantias dos titulares de dados no ambiente da COVID-19

Para se antecipar a situações que suscitavam dúvidas sobre a proteção da privacidade, no âmbito das medidas de combate à pandemia, e diante do que dispunha o RGPD em matéria de tratamento de dados pessoais e utilização de dados de localização, assim como relativamente a aspetos inerentes ao ambiente de trabalho, em 19 de março de 2020, o Comité Europeu para a Proteção de Dados expediu uma Declaração sobre o tratamento de dados pessoais no contexto do surto de COVID-19.[61]

A Declaração pretendeu destacar como os dados pessoais estariam protegidos pelas normas vigentes, em especial o RGPD, ante as medidas que se tomavam para evitar a propagação do vírus.

No introito, já se dizia que

> Os governos, assim como as organizações públicas e privadas de toda a Europa, têm estado a tomar medidas para conter e atenuar o surto de COVID-19, que podem implicar o tratamento de vários tipos de dados pessoais. As normas em matéria de proteção de dados (como o Regulamento Geral sobre a Proteção de Dados) não obstam a que sejam adotadas medidas para combater a pandemia de coronavírus. A luta contra as doenças transmissíveis é um objetivo primordial partilhado por todas as nações, devendo ser apoiada da melhor forma possível. A humanidade tem interesse em travar a propagação de doenças e em utilizar técnicas modernas na luta contra os flagelos que afetam grande parte do mundo. Ainda assim, o Comité Europeu para a Proteção de Dados gostaria de sublinhar que, mesmo nestes tempos de exceção, os responsáveis pelo tratamento dos dados e os subcontratantes devem assegurar a proteção dos dados pessoais dos respetivos titulares.

Destacou igualmente que "há que ter em conta uma série de considerações para garantir o tratamento lícito dos dados pessoais e ter sempre presente que qualquer medida tomada neste contexto deve respeitar os princípios gerais de direito, não podendo ser irreversível."

---

[60] HARARI, no texto, pondera que, no momento em que os estados estão a combater o coronaíirus, pode ocorrer a normalização da utilização de instrumentos de vigilância em massa como representar uma transição da vigilância "*over the skin*" (incidente sobre o comportamento exterior, como localização, hábitos, compras, etc) para a "*under the skin*" (capaz de monitorar dados biológicos, como temperatura corporal, pressão arterial, batimentos cardíacos, respiração, etc). A segunda permitiria aos algoritmos saber a condição de saúde antes dos sintomas, antes do próprio cidadão. E, mais ainda, os dados poderiam ser utilizados para avaliação do estado emocional do ser humano, e até, quiçá, dos seus sentimentos, o que representaria uma invasão à privacidade inaudita, podendo gerar discriminações, influências ou manipulações.

[61] Disponível em https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/statement-processing-personal-data-context-covid-19_pt (consulta em junho de 2022)

O Comité assinalou, também, que a situação de emergência legitimava a imposição de restrições às liberdades, "desde que sejam proporcionadas e limitadas ao período de emergência." E defendeu, ainda, a aplicação do RGPD, "um diploma legislativo genérico que prevê regras aplicáveis igualmente ao tratamento de dados pessoais num contexto como o do surto de COVID-19", e que "permite que as autoridades competentes em matéria de saúde pública e os empregadores procedam ao tratamento de dados pessoais no contexto de uma epidemia, em conformidade com o direito nacional e nas condições nele estabelecidas". A título de exemplo desse tratamento de dados permitido pelo RGPD, apontou a necessidade "por motivos de interesse público importante no domínio da saúde pública", situação que torna desnecessário obter o consentimento dos particulares.

O entendimento do Comité, ali manifestado, é de que as previsões dos artigos 6.º e 9.º do RGPD são bastantes para autorizar as autoridades públicas competentes, mesmo diante de dados especiais (como os de saúde) a promoverem o respetivo tratamento, para desempenho do mandato legal. Além disso, esclareceu que nas relações laborais o empregador pode, se necessário para cumprir obrigação legal, nomeadamente em matéria de saúde e segurança no local de trabalho, ou por razões de interesse público como o controlo de doenças e outras ameaças à saúde pública, realizar o tratamento dos dados pessoais dos empregados. A base legal referida no texto é o artigo 9.º, n.º 2.º, alíneas *c)* e *i*), apesar de parecer mais correto, no que concerne o tratamento de dados pelo empregador, a aplicação da autorização prevista na alínea *b*), que se refere especificamente ao cumprimento de obrigações da legislação laboral.

Outro ponto que merece especial atenção é o relativo aos riscos inerentes ao tratamento dos dados de localização, os quais, quando atrelados aos dados de saúde, podem permitir ao responsável pelo tratamento exercer grande controlo sobre os titulares dos dados. Este aspeto é de grande relevância por nos remeter anos cenários, descritos na introdução, de monitoramento e vigília constantes sobre os cidadãos, podendo culminar com a quebra das resistências ao estabelecimento de uma sociedade da vigilância e, assim, atingir profundamente a autodeterminação informativa digital. Para essas situações, o Comité defendeu a aplicação da Diretiva Privacidade Eletrónica e ressaltou que, em princípio, os dados de localização somente podem ser utilizados pelo operador se forem tornados anónimos ou se for obtido o consentimento. Estas limitações, contudo, segundo o Comité, podem ser superadas em caso de lei excecional que possa ser editada por algum Estado-membro com o objetivo de salvaguardar

a segurança pública, tendo por fundamento o artigo 15.º da Diretiva Privacidade Eletrónica[62] [63].Por fim, destacou o Comité que os dados pessoais, no ambiente do combate à pandemia, podem ser tratados, mas desde que com finalidade específica e explícita, fornecendo, aos respetivos titulares, informações transparentes sobre as atividades de tratamento, as suas principais características, período de conservação dos dados e a finalidade. Recomenda a adoção de medidas de segurança adequadas e políticas de confidencialidade para evitar que os dados sejam divulgados a pessoas não autorizadas.

Extrai-se da referida Declaração a sinalização da preocupação do Comité quanto aos riscos que a pandemia fez recair sobre a proteção dos dados pessoais, enfatizando três vetores, sendo os de maior preocupação: o tratamento dos dados pelas autoridades públicas, o tratamento dos dados no ambiente de trabalho e o tratamento dos dados de localização para fins de rastreio.

O Comité procurou ressaltar os limites à atuação dos governos dos Estados-Membros impostos pela legislação de proteção de dados. Afirmou que os artigos 6.º e 9.º do RGPD e os princípios estabelecidos no Regulamento seriam bastantes para assegurar o devido respeito dos direitos dos titulares de dados. E, ao enfrentar a questão dos dados de localização, referiu-se ao artigo 15.º da Diretiva 2002/58/CE, de 12 de julho, que admite exceção às regras limitativas antes referidas e submete a disciplina da questão à lei nacional em situações de risco para a segurança.

A Declaração antecipa as principais questões que se anunciavam e indica os principais fundamentos para a defesa dos interesses e direitos dos titulares de dados pessoais, fazendo alusão aos artigos 6.º e 9.º do RGPD e salientando a possível aplicação do artigo 15.º da Diretiva 2002/58/CE, de 12 de julho.

---

[62] A regra a que se refere o Comité está no c*aput* do artigo 15.º da Diretiva 2002/58/CE, de 12 de julho: "Artigo 1. Os Estados-Membros podem adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos n.os 1 a 4 do artigo 8.º e no artigo 9.º da presente Directiva sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a detecção e a repressão de infracções penais ou a utilização não autorizada do sistema de comunicações electrónicas, tal como referido no n.º 1 do artigo 13.º da Directiva 95/46/CE. Para o efeito, os Estados-Membros podem designadamente adoptar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito comunitário, incluindo os mencionados nos n.ºs 1 e 2 do artigo 6.º do Tratado da União Europeia".

[63] Para a interpretação do artigo 15.º da Diretiva, veja-se o acórdão do Tribunal de Justiça da União Europeia (TJUE) de 29 de janeiro de 2008, Productores de Música de España (Promusicae)/Telefónica de España SAU, C-275/06, ECLI:EU:C:2008:54. Em https://curia.europa.eu/juris/liste.jsf?language=en&num=C-275/06 (acedido em janeiro de 2022).

Convém aqui examinar as situações destacadas na Declaração, em especial no que tange ao tratamento dos dados de saúde pelas autoridades, em vista ao direito à privacidade do cidadão, assim como no ponto relativo aos dados de localização, ou dados de tráfego, que se pretenderam utilizar para o rastreio de indivíduos. São pontos sensíveis relativamente à autodeterminação informativa no ambiente digital.

2.2.1 Tratamento de dados de saúde pelas autoridades públicas portuguesas, com base no interesse público – artigo 9.º, 2, *i)* do RGPD

O primeiro ponto relativo ao tratamento dos dados de saúde pelas autoridades públicas envolve vários aspetos, entre os quais a divulgação de informações nos relatórios e comunicados ao público em geral. O Estado deve atender ao princípio da transparência e publicidade, especialmente numa situação de crise sanitária, que lhe impõe prestar contas à sociedade das medidas adotadas para conter o aumento de casos, assim como dos resultados alcançados. Não foi por outro motivo que, em Portugal, a Autoridade Nacional de Saúde disponibilizou, sistematicamente, informações sobre o número de casos suspeitos de infeção, de casos confirmados, de recuperados e de óbitos. Informava, também, a distribuição desses casos pelo território português, apontando as regiões e os números da incidência, inclusive por concelho.

Alguns municípios portugueses divulgaram também os quantitativos e chegam a informar dados por freguesia. Em alguns casos, deram a conhecer os dados de identificação e contatos de alguns infetados, nas suas páginas na *internet* ou redes sociais. Noutros casos, as informações dadas, apesar de anonimizadas, foram suficientes para conduzirem à identificação dos doentes, em situações verificadas em pequenas localidades, com poucos residentes.[64] São casos de evidente desrespeito ao sigilo que protege os dados pessoais de saúde.

É, pois, indubitável que os dados pessoais, inclusive os de saúde, podem ser objeto de tratamento pelas autoridades públicas.[65]

---

[64] A respeito desses casos, veja-se o relato da Comissão Nacional de Proteção de Dados na orientação sobre divulgação de informações relativas a infetados por COVID-19 em https://www.cnpd.pt/media/4i4hmccv/orientacoes_divulgacao_informacao_infetados_covid-19.pdf (acedido em 15.01.22)

[65] É sempre bom lembrar que os *consideranda* prestam auxílio à interpretação do Regulamento, motivo pelo qual se deve atentar para o (46) que se refere aos tratamentos de dados que conciliam o interesse público e os interesses

O tratamento dos dados pessoais é regulado, conforme conceito jurídico firmado no artigo 4.º, 2, do RGPD. Isso decorre do artigo 6.º, 1, alíneas c), d) e e) do RGPD, seja para cumprir uma obrigação jurídica[66], para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular ou para o exercício de funções de interesse público ou para o exercício de autoridade pública de que está investido o responsável pelo tratamento.[67]

Quanto aos dados especiais de saúde, além das hipóteses em que haja consentimento do respetivo titular, do que aqui não se cogita, a autorização do RGPD para o tratamento vem clara na alínea *i)* do inciso 2, do artigo 9.º do RGPD, que estabelece tal exceção à proibição genérica constante no inciso 1 desse mesmo artigo. Poder-se-ia considerar que o disposto na alínea *g*) também tivesse de ser aplicável, uma vez que é inegável a presença do interesse público. Porém, parece que a existência de um item específico destinado a tratar dos temas de saúde pública afasta a incidência de dispositivos mais genéricos. E é claro que "interesse público no domínio da saúde pública" se encaixa na perfeição na situação da pandemia, considerada como a prestação de cuidados de saúde e o acesso universal aos mesmos[68]. A referência, que o legislador faz a título de exemplo, a uma situação de "proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde" é mais do que suficiente para que se reconheça a aplicabilidade do inciso, uma vez caracterizado o interesse público ínsito a uma tal situação.

---

vitais "para fins humanitários, incluindo a monitorização de epidemias e da sua propagação ou em situações de emergência humanitária, em especial situações de catástrofes naturais ou de origem humana", assim como o (54) que esclarece que "o tratamento de categorias especiais de dados pode ser necessário por razões de interesse público nos domínios da saúde pública, sem o consentimento do titular dos dados."

[66] Melhor seria ter-se adotado a expressão 'obrigação legal', tal como se fez no artigo 7.º, c) da Diretiva 95/46/CE, de 24 de outubro de 1995, em que a mesma regra já constava. É que neste caso, a obrigação que pode justificar o tratamento é aquela decorrente de lei, pois a obrigação contratual já está contemplada na alínea b). Aliás, na versão do RGPD em inglês consta a expressão mais adequada - *legal obligation*; na versão em francês - *obligation légale*.

[67] Segundo o que consta no Considerando (46) "O tratamento de dados pessoais também deverá ser considerado lícito quando for necessário à proteção de um interesse essencial à vida do titular dos dados ou de qualquer outra pessoa singular. Em princípio, o tratamento de dados pessoais com base no interesse vital de outra pessoa singular só pode ter lugar quando o tratamento não se puder basear manifestamente noutro fundamento jurídico. Alguns tipos de tratamento podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo, se o tratamento for necessário para fins humanitários, incluindo a monitorização de epidemias e da sua propagação ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana."

[68] O conceito jurídico de saúde pública encontra-se no Regulamento (CE) n.º 1338/2008 de 16 de Dezembro de 2008, relativo às estatísticas comunitárias sobre saúde pública e saúde e segurança no trabalho, no seu artigo 3.º/1, c) que assim a define: «Saúde pública», todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade.

A exigência que faz o RGPD é que o direito da União ou dos Estados-Membros prevejam medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional.

O sigilo profissional aí referido tem como destinatários os profissionais de saúde, sujeitos a essa regra jurídica e deontológica. Mas também o encarregado da proteção de dados está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, em conformidade com o que dispõe o artigo 38.º, 5, do RGPD, assim como os responsáveis pelo tratamento de dados e todas as pessoas que intervenham em qualquer operação de tratamento de dados, os quais estão cobertos pelo dever de confidencialidade, de acordo com o artigo 10.º, 2, da Lei de Execução (LE). No que diz respeito aos dados de saúde, o legislador nacional foi além e estabeleceu regras que protegem o titular dos dados, impondo sigilo e confidencialidade àqueles que, por necessidade, participarem do tratamento desses dados. É o que se observa no artigo 29, incisos 1, 2, 3, 4 e 5.

Aliás, parece claro que o intuito do legislador português de atender à exigência de previsão de medidas - específicas e adequadas com vista à defesa dos direitos fundamentais e dos dados pessoais das pessoas singulares - posta na parte final do permissivo da alínea *i*) do inciso 2 do artigo 9.º do RGPD se expressou no artigo 29 da LE, que disciplinou conjuntamente o tratamento dos dados de saúde e genéticos.

MENEZES CORDEIRO[69] defende que o disposto no artigo 29 não seria suficiente para atender às "exigências legais genéricas" do RGPD que alcançariam:

> Identificação dos dados objeto do tratamento e fim em concreto prosseguido, previr medidas adequadas e específicas que salvaguardem os direitos e as liberdades do titular dos dados – direitos e deveres de informação, possibilidade de recorrer da decisão de tratamento, faculdade de acompanhar o processo de tratamento e, em particular, o sigilo profissional.

Diz ainda, no ponto, no mínimo sujeito a controvérsia, que

> Não nos parece que o artigo 29.º da LE cumpra estas exigências legais: as medidas de salvaguarda aí previstas não podem ser descritas como sendo específicas. Nesse sentido e porquanto não sejam introduzidas medidas adicionais, não cremos que possam ser realizados tratamentos motivados pelo interesse público no domínio da saúde.

Não parece ter razão o jurista. O artigo 29 da LE, mesmo não sendo um exemplo da boa técnica legislativa, é suficiente para tratar da confidencialidade e refere-se ao sigilo profissional,

---

[69] Op. cit. p. 251

que, naturalmente, é tratado igualmente em outros diplomas nacionais que preexistiam ao RGPD, das quais destacam-se as Leis n.º 12/2005 de 26 de janeiro, que trata da informação genética pessoal e informação de saúde, e n.º 26/2016, de 22 de agosto, que aprova o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos. São diplomas legais que, em complemento do artigo 29 da LE, atendem às exigências acima referidas, estabelecidas pela alínea *i*) do inciso 2, do artigo 9.º do RGPD. Inegavelmente, nessas leis se disciplinam o sigilo e a confidencialidade, impõem-se sanções a serem aplicadas em decorrência do seu incumprimento, regulamenta-se o direito de acesso do titular de dados, permitindo-lhe acompanhar o tratamento dos seus dados, formular reclamações e pedir a reforma das decisões, respeitada a estrutura administrativa existente no estado português.

Criou-se, inclusive, uma entidade administrativa independente, que funciona junto da Assembleia da República, a quem cabe zelar pelo cumprimento das disposições da referida lei, com funções disciplinares e decisórias: a Comissão de Acesso aos Documentos Administrativos - CADA.

Todo este arcabouço de leis e essa estrutura administrativa complexa servem o propósito, definido no RGPD, de viabilizar a concretização dos direitos assegurados aos titulares de dados. Além disso, não se pode deixar de destacar a Comissão Nacional de Proteção de Dados, uma entidade de controlo independente, prevista no capítulo VI do RGPD (artigos 51.º e seguintes), cuja organização e funcionamento são regulados pela Lei n.º 43/2004, de 18 de agosto, republicada como anexo à LE. A CNPD visa assegurar a execução do RGPD na ordem jurídica interna, controlando e fiscalizando-lhe o cumprimento, bem como das demais disposições legais e regulamentares em matéria de proteção de dados pessoais.

A referida jurídico-administrativa anteriormente referida permite reconhecer a aplicabilidade do disposto na alínea i) do inciso 2 do artigo 9.º do RGPD quanto à possibilidade jurídica do tratamento de dados de saúde motivado pelo interesse público no domínio da saúde pública em Portugal.

Fixada esta premissa, convém destacar que a confidencialidade e o sigilo impostos sobre os dados de saúde, no RGPD ou na LE impedem a adoção da conduta das autarquias locais, relatada pela CNPD acima referida, de permitir a divulgação de dados pessoais dos infetados ou disponibilizar informações capazes de conduzir a essa identificação. É bom destacar que o

tratamento dos dados em conformidade com o RGPD atrai a necessidade de atendimento aos princípios estabelecidos no artigo 5.º, *i*)[70] e inclusive ao da proporcionalidade.

Sobre a aplicação do princípio da proporcionalidade em relação à divulgação de dados pessoais para efeitos de transparência no setor público, o Grupo de Trabalho de Proteção de Dados do artigo 29.º da Diretiva 95/46/CE[71] pronunciou-se no Parecer n.º 02/2016[72]: "O princípio de proporcionalidade deve ser respeitado no decurso de cada operação de tratamento e, em especial, na fase de recolha dos dados e na sua eventual publicação subsequente". E acrescenta, ainda, que "a publicação em linha de informações que revelem aspetos irrelevantes da vida privada de uma pessoa singular não se justifica à luz dos princípios da equidade e da proporcionalidade". O parecer refere-se a decisões do TJUE nos processos apensos C-465/00, C-138/01 e 139/01, no sentido de que o tratamento de dados pessoais deve dar-se de forma proporcionada e, quanto à publicidade de dados pessoais, os órgãos jurisdicionais nacionais competentes devem «verificar se tal publicidade é, simultaneamente, necessária e proporcionada» ao objetivo prosseguido e apreciar se tal objetivo não poderia ter sido alcançado de forma igualmente eficaz por formas alternativas que fossem menos suscetíveis de afetar a privacidade das pessoas em causa.

A lição aplica-se à situação acima tratada, que envolveu divulgação de dados sensíveis de saúde pelas autoridades públicas portuguesas.

PATRÍCIA CARDOSO DIAS [73] defende que se acrescente

> Aos princípios gerais vertidos no artigo 5.º a necessidade de qualquer tratamento de dados pessoais de saúde encontrar-se subsumido a uma base jurídica legitimadora nos termos do artigo 6.º coordenada com alguma das derrogações previstas no n.º 2 do artigo 9.º do RGPD para efeitos de licitude do tratamento de categorias de dados sensíveis.

E sustenta, ainda, que

> As pessoas singulares devem, para cumprimento integral do conteúdo dos princípios vertidos no artigo 5.º, receber informações transparentes, redigidas em linguagem facilmente apreensível, em relação às operações de tratamento de dados pessoais e as suas principais caraterísticas, período de conservação e finalidades do tratamento. Os dados pessoais tratados devem ser objeto de medidas de segurança adequadas e políticas de confidencialidade que assegurem que não sejam divulgados a pessoas não autorizadas.

---

[70] Princípios da licitude, lealdade e transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade e confidencialidade e responsabilidade.

71 O grupo de trabalho foi criado ao abrigo do artigo 29.º da Diretiva 95/46/CE, constituindo-se num órgão consultivo independente europeu sobre a proteção de dados e a privacidade, cujas atribuições estão descritas no artigo 30.º da Diretiva 95/46/CE e no artigo 15.º da Diretiva 2002/58/CE.

[72]https://www.uc.pt/site/assets/files/475840/20160608_parecer_02_2016_publicacao_de_dados_pessoais_para_efeitos_de_tranparencia_no_setor_publico_wp239_pt.pdf (acedido em janeiro 2022)

[73] Artigo citado, p. 18.

Parece ser correta a posição adotada. O atendimento a todos esses requisitos é, portanto, rigoroso para que se legitime o tratamento dos dados pessoais de saúde, com fundamento no artigo 9.º, 2, *i*) do RGPD.

2.2.2 – Dados de localização e contato – Plataforma Stayaway Covid – a experiência portuguesa

Outro ponto abordado pelo Comité e que deve merecer especial atenção refere-se à utilização dos dados de telecomunicações como ferramenta de rastreio de pessoas infetadas. Na Declaração anteriormente referida, o Comité manifestou-se no sentido de que "as medidas mais invasivas, como o «rastreio» de indivíduos (ou seja, o tratamento de dados históricos de localização não anonimizados), poderão ser consideradas proporcionais em determinadas circunstâncias e em função das modalidades concretas do tratamento dos dados." Portanto, deixou claro que, naquele momento, concordava com a possibilidade de se utilizarem desses meios de rastreio, não se pronunciando, entretanto, sobre se uma tal medida poderia ou não ser compulsória.

A utilização de *contact tracing systems*[74] pode representar graves riscos à autodeterminação digital e tem potencial para gerar atitudes discriminatórias. A propósito desta questão essencial, veja-se o pronunciamento da Organização Mundial de Saúde [75] em que, após destacar as possíveis vantagens de se utilizar a tecnologia em prol do combate à pandemia, adverte, com razão:

> *Yet such uses of data may also threaten fundamental human rights and liberties during and after the COVID-19 pandemic. Surveillance can quickly traverse the blurred line between disease surveillance and population surveillance. Thus, there is a need for laws, policies and oversight mechanisms to place strict limits on the use of digital proximity tracking technologies and on any research that uses the data generated by such technologies*.

---

[74] De acordo com a OMS, *"contact tracing is the process of identifying, assessing, and managing people who have been exposed to a disease to prevent onward transmission. When systematically applied, contact tracing will break the chains of transmission of an infectious disease and is thus an essential public health tool for controlling infectious disease outbreaks".* Em Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing, Interim guidance, de 28.05. 2020: https://www.who.int/publications/i/item/WHO-2019-nCov-Ethics_Contact_tracing_apps-2020.1 (acedido em junho 2022)

[75] ob. cit.,

O tema veio a ser tratado, em Portugal, no Decreto-Lei n.º 52/2020 de 11 de agosto que definiu o responsável pelo tratamento dos dados e regulou a intervenção do médico no sistema Stayaway Covid. Tratava-se, em poucas palavras, de aplicação capaz de armazenar dados de contato, e notificar aos portadores de aparelho telemóvel em que essa aplicação estivesse instalada, sobre situação capaz de representar risco de contágio, pela proximidade ocorrida em relação a outro aparelho em que tenha sido inserido código representativo de infeção do seu portador pelo vírus da COVID-19.

O referido Decreto-Lei estabeleceu, no artigo 2.º, que tal aplicação deveria "respeitar a legislação europeia e nacional aplicável à proteção de dados pessoais, nomeadamente o Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, a Lei n.º 58/2019, de 8 de agosto, e demais legislação aplicável".

O Decreto-Lei fez referência expressa às "Diretrizes n.º 4/2020, do Comité Europeu para a Proteção de Dados, sobre a utilização de dados de localização e meios de rastreio de contactos no contexto", nas quais o Comité se manifestara do seguinte modo: "o CEPD já tomou posição sobre o facto de a utilização de aplicações de rastreio de contactos dever ser voluntária e não dever depender do rastreio de movimentos individuais mas sim de informações sobre a proximidade dos utilizadores".[76]

É de estranhar que o Governo de Portugal, adotando posição divergente da que fora manifestada no Decreto-Lei 52/2020, uma vez que ali se colhera a manifestação do EDPB (*European Data Protection Board*) no sentido de a utilização da aplicação dever ser voluntária, apresentou uma proposta de Lei (n.º 62/XIV/2ª GOV) na qual se previa, além de outras medidas, a utilização compulsória da tecnologia.[77] No artigo 4.º da referida proposta, determinava-se a "obrigatoriedade da utilização da aplicação Stayaway Covid em contexto laboral ou

---

[76] Leia-se na íntegra as Diretrizes do CEPD em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf (acedido em junho de 2022). Destaca-se que, não obstante firmar a premissa de que a utilização da aplicação exigia o consentimento do titular de dados, o Comité acrescentou: "No entanto, são permitidas derrogações dos direitos e das obrigações previstas na diretiva nos termos do artigo 15.º, sempre que as mesmas constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para alcançar determinados objetivos

[77] Em 15.10.2020, o Diário de Notícias *online* informava sobre uma proposta de lei do governo que previa multas de até 500 euros para quem não tivesse a app Stayaway Covid. A fiscalização do cumprimento da obrigação competiria à Guarda Nacional Republicana, à Polícia de Segurança Pública, à Polícia Marítima e às polícias municipais. Conferir https://www.dn.pt/pais/lei-propoe-multas-ate-500-euros-para-falhas-no-uso-de-mascara-e-stayaway-covid-12922740.html

equiparado, escolar e académico", "em especial os trabalhadores em funções públicas, funcionários e agentes da Administração Pública, incluindo o setor empresarial do Estado, regional e local, profissionais das Forças Armadas e de forças de segurança." A proposta criava o dever de o utilizador "proceder à inserção na aplicação do código de legitimação pseudoaleatório, que deve figurar do relatório que contenha o resultado do teste laboratorial de diagnóstico"

A Ordem dos Advogados de Portugal, ouvida, opôs-se à referida proposta por fundamentos jurídicos relevantes (artigos 32.º, n.º 8,10 e 34.º, n.º4 da Constituição).[78]

Especial destaque merece a posição adotada pela Comissão Nacional de Proteção de Dados - CNPD que, num parecer bem fundamentado de 27.10.2020 (parecer 2020/129)[79], destacou, inicialmente, a tensão existente, naquele momento, entre o direito à vida e à saúde e o direito à privacidade[80]:

> A CNPD compreende a necessidade de definição de medidas adequadas a acautelar o interesse público de saúde pública e a salvaguardar os direitos fundamentais à vida e à integridade física, os quais podem implicar restrições de outros direitos fundamentais, como o direito à liberdade e à privacidade. Não pode deixar de sublinhar, contudo, que tais restrições têm de refletir um equilíbrio entre os diferentes direitos e valores constitucionalmente protegidos, não podendo ultrapassar o limite último do respeito pelo conteúdo essencial dos direitos, liberdades e garantias, no quadro do Estado de Direito democrático em que nos movemos.

Feita esta introdução ao tema, a Comissão prosseguiu, esclarecendo que a aplicação em questão (Stayaway Covid) assentava num sistema descentralizado de tratamento de dados, o que significava que os dados de contato ficavam armazenados no próprio aparelho e

---

[78] Veja-seo parecer da Ordem dos Advogados de Portugal sobre a referida proposta de lei, parcialmente transcrito: "No caso concreto, a restrição que o Governo pretende impor através da consagração da obrigatoriedade da aplicação ao direito da reserva da intimidade da vida privada e familiar, ao direito à inviolabilidade dos meios de comunicação privada e à proibição da utilização da informática para tratamento de dados referentes à vida privada, não é claramente adequada (por não ser eficaz para prevenir e deter a epidemia, uma vez que só poderá ser utilizada pelos cidadãos que sejam portadores de equipamento compatível com a aplicação), não é exigível (porque o legislador dispõe de outros meios menos restritivos para alcançar o mesmo fim) e é excessiva e desproporcional. A par disso, a CRP proíbe a ingerência das autoridades públicas nas telecomunicações, sendo nulas todas as provas obtidas mediante abusiva intromissão na vida privada, no domicílio ou nas telecomunicações, aplicando-se essa proibição ao processo contra-ordenacional, o que, no caso concreto, impossibilitaria o sancionamento dos utilizadores com a aplicação de coima (cf. Artigos 32.º, n.º8, 10 e 34.º, nº. 4)."

[79] O parecer pode ser encontrado no site da CNPD https://www.cnpd.pt/covid-19/ e é intitulado - Parecer sobre a obrigatoriedade do uso de máscara para acesso ou permanência nos espaços e vias públicas e a obrigatoriedade de utilização da aplicação Stayaway Covid (acedido em janeiro de 2022).

[80] Para Paulo Mota Pinto, a privacidade se baseia numa *tensão entre o social e o individual*. Op. Cit. p. 509.

pseudonimizados[81] "uma vez que permitem, por relacionamento com outra informação, identificar a pessoas a que dizem respeito".

E com base em informações técnicas, relativas ao funcionamento da aplicação, concluiu que

> A Google e a Aple criaram uma interface (GAEN) para habilitar o funcionamento de aplicações de rastreamento de proximidade, disponibilizando o acesso a funcionalidades ao nível do sistema operativo do dispositivo móvel, como sejam o acesso à componente *Bluetooth*, a geração de chaves de identificadores pseudoaleatórios e o seu cruzamento para cálculo do risco, as quais não são executadas pela aplicação. Com isto, uma parte substancial do tratamento de dados não é controlada pelo responsável pelo tratamento (a Direção-Geral de Saúde), mas, sim, por uma parceria de duas das maiores empresas privadas de tecnologia. Esta é também uma das razões porque a utilização da aplicação só foi considerada legítima no ordenamento jurídico nacional se dependesse exclusivamente da vontade dos cidadãos a sua utilização, o mesmo se aplicando à introdução do código de legitimação, que desencadeia o alerta de risco de contágio junto dos utilizadores da aplicação e que tenham ficado registados como tendo estado próximos do utilizador que é portador do vírus.

Em seguida, a Comissão asseverou que "pelo menos quanto aos dispositivos Android, a interface GAEN implica a recolha permanente do dado 'localização', uma vez que deixa de ficar ao critério de cada um poder desativar essa funcionalidade se e quando o desejar, permitindo à Google rastrear as deslocações e movimentos dos cidadãos utilizadores desta aplicação para outras finalidades".

Além disso, e com razão, a Comissão considerou que a imposição das obrigações concernentes à utilização da aplicação geraria impacto nos direitos fundamentais à liberdade, à reserva ou respeito pela vida privada, à inviolabilidade das comunicações eletrónicas e à proteção dos dados pessoais (artigos 26.º, 27.º, 34.º, e 35.º da CRP e artigos. 6.º, 7.º e 8.º da CDFUE), direitos que somente poderiam ser afetados excecionalmente, desde que respeitado o princípio da proporcionalidade (adequação, necessidade e caráter não excessivo da restrição e sem afetar o conteúdo essencial dos direitos (artigo 18.º, n.os 2 e 3, e artigo 52.º, n.º 1 da CRP).

A Comissão mostrou-se francamente contrária à proposta. E tinha toda a razão em assim se posicionar, pois, a medida, se aprovada, representaria uma violação grave dos direitos fundamentais dos cidadãos, absolutamente desproporcionada e afrontaria o artigo 18.º, 2, da

---

[81] CORDEIRO, A. BARRETO MENEZES, ob. cit. p. 149 ensina: "A pseudonimização consiste, nos termos do artigo 4.º, 5), (i) num tratamento efetuado sobre dados pessoais (ii) que impossibilita a identificação do titular de determinados dados, sem a utilização da informação suplementar. A estes dois critérios estruturais acresce um (iii): a informação suplementar deve ser conservada separadamente, de forma a impedir a identificação do titular dos dados. (…) A pseudonimização incentivada pelo legislador, permitir reduzir os riscos de divulgação da identidade do titular dos dados pessoais, acautelando os seus interesses, e facilitar o cumprimento, pelos responsáveis pelo tratamento ou pelo subcontratante, dos deveres impostos pelo RGPD."

CRP e o artigo 5.º, 1, do RGPD. A imposição, ainda que por lei, da utilização de tecnologia de compartilhamento de dados pessoais de localização estaria próxima dos piores cenários temidos no texto de HARARI, citado no início deste estudo.

Não se trata somente de uma violação das regras de proteção de dados (o que já seria bastante para rejeitar a proposta); a intenção do Governo era de que o cidadão se submetesse a uma série de obrigações que violavam por completo a sua liberdade. Estaria obrigado a instalar a aplicação (se compatível com o seu aparelho) e, diante de uma fiscalização (por agentes de segurança), seria obrigado a desbloquear o aparelho, permitir ao agente a verificação de pelo menos o seguinte: (i) da compatibilidade do aparelho com a aplicação; (ii) do descarregamento da aplicação; (iii) da ativação do *Bluetooth*.

A compulsoriedade de que se reveste a medida, como se vê, não é somente quanto ao fornecimento da informação pessoal à autoridade (e, quiçá, ao terceiro com quem o titular dos dados possa ter tido contato)[82], mas envolve uma série de condutas por parte do cidadão, titular dos dados, que representa uma devassa na sua vida privada, uma exposição da sua intimidade, podendo resultar na autoincriminação, constituindo absurdos inaceitáveis, que mostram quão desproporcionada é a proposta.

Nem tudo se permite, mesmo com o objetivo de atender aos interesses maiores da saúde pública. Segundo ALICE DONALD E PHILIP LEACH [83]:

> *If a state takes far-reaching steps to protect life and health, it is highly likely that this will result in the restriction of other rights. However, as Mavronicola explains, while the pandemic may justify or even require exceptional emergency measures, it does not give carte blanche to states to take actions that are impermissible under international human rights law.* [84]

A proposta lei n.º 62/XIV/2ª GOV não foi adiante e a aplicação foi admitida em Portugal, com base no DL 52/2020, de 11 de agosto, dependente de um ato voluntário, de

---

[82] É natural que, em muitas situações, por serem poucos os contatos pessoais, especialmente em tempos de pandemia, seja possível identificar-se aquela pessoa que, preenchendo as características exigidas para acionar o alarme de risco de contágio (proximidade por determinado período de tempo), seja o provável infetado. Se não houvessem outros defeitos, este, por si só, já importaria em quebra da obrigação de confidencialidade.

[83]DONALD, Alice e LEACH, Phillipe - **Human Rights – The Essential Frame of Reference in the Global Response to COVID-19** [Em linha]. 2020/5/12. Atual. [Consultado em 10 de abril de 2022]. Disponível em https://verfassungsblog.de/humanrights-the-essential-frame-of-reference-in-the-global-response-to-covid-19/ (acedido em junho de 2022).

[84] No mesmo artigo, os autores concluem que: "*In other respects, too, measures adopted by states which comply with a human rights framework are likely to be more effective in protecting life and health, than ones that restrict other rights disproportionately. For example, voluntary contact tracing apps (installed onto smart phones) which rely on a critical mass of public uptake will not be effective if there are concerns about a disproportionate invasion of privacy".*

consentimento do titular de dados. A rejeição da proposta, em função da resistência que encontrou na sociedade, em especial nos órgãos que se dedicam à proteção dos dados pessoais, representa a prevalência do direito e, neste caso, revela que o ordenamento jurídico foi eficaz na prevenção contra o arbítrio.

3. O CERTIFICADO DIGITAL COVID DA UE (OU CERTIFICADO VERDE) – CRIAÇÃO, FINALIDADE, TRATAMENTO LEGAL

Com o objetivo de combater a propagação do vírus SARS-COV-2, os países adotaram, com base no princípio da precaução, medidas de isolamento, cada qual com um determinado nível de restrições, que tiveram grande impacto na liberdade e especialmente no direito de livre circulação. Foram impostas restrições severas a locomoção, viagens transfronteiriças, exigindo-se o cumprimento de medidas de quarentena, isolamento e realização de testes para despistagem da infeção.[85] [86]

Essas medidas, além de implicarem graves restrições ao direito de livre circulação, dentro e fora dos países, acarretavam uma enorme perda económica, com especial ênfase nos campos do turismo e transportes.

Com o advento das vacinas contra o SARS-COV-2, a verificação da sua eficácia na produção de resposta imunológica e, consequentemente, na produção de resultados positivos para auxílio no objetivo de contenção da pandemia, passou-se a considerar fortemente a hipótese de se voltar a permitir a livre circulação de pessoas imunizadas, que se mostraram menos propensas a transmitir a doença. Neste conjunto ideal de pessoas, e de acordo com dados científicos, incluem-se os vacinados, dentro do prazo de eficácia da vacina, assim como os que obtiveram um resultado negativo em teste de despistagem à COVID-19, bem como as pessoas que recuperaram da doença nos seis meses anteriores.

Foi considerado que a livre circulação de tais pessoas não representava risco significativo para a saúde pública, motivo pelo qual as restrições em relação a esse grupo específico poderiam ser afastadas, ainda que temporariamente, pois o objetivo das limitações era, exatamente, impedir a propagação do vírus, que não ocorreria, significativamente, com a circulação de pessoas alegadamente imunes.

---

[85] Na União Europeia, foi adotada a Recomendação (UE) 2020/1475 de 13 de outubro de 2020 sobre uma abordagem coordenada das restrições à liberdade de circulação em resposta à pandemia de COVID-19, com critérios a serem adotados pelos Estados-Membros para evitar a discriminação e para alcançar, tanto quanto possível, uma ação harmoniosa no tema da circulação no território europeu.

[86] Para um relatório detalhado sobre as medidas de restrição impostas por diversos países nos primeiros meses da pandemia, incluindo medidas de limitação à imigração e supressão de direitos humanos, veja-se o Verfassungsblog symposium organizado por Joelle Grogan no endereço eletrónico https://intr2dok.vifa-recht.de/receive/mir_mods_00008563 (acedido em junho de 2022)

Muitos países começaram a adotar medidas tendentes à criação de documentos capazes de atestar essa situação, fosse em relação à vacinação, fosse em relação à recuperação ou testagem, o que originou a ideia de se emitirem certificados com tais informações, que rapidamente viriam a ser denominados certificados de vacinação.

No âmbito da União Europeia, tais certificados de vacinação possibilitariam a retoma da livre-circulação entre países, ajudando a reativação da economia. Para isso, os certificados teriam que ser interoperáveis, compatíveis, seguros e verificáveis, de forma a que pudessem ser reconhecidos e utilizados por todos os Estados-membros, assim como pelas empresas de transporte e demais agentes económicos envolvidos. Era necessária uma abordagem uniforme da questão, para evitar que cada Estado-membro criasse o seu certificado, o que dificultaria a aceitação em todo o território da União.

Ficou decidido, então, que seria estabelecido um regime comum para a emissão, verificação e aceitação pelos Estados-membros, de certificados interoperáveis de vacinação, teste e recuperação da COVID-19 (Certificado Digital COVID da UE[87]), em formato digital ou em papel (ou em ambos).

Como a questão envolvia o tratamento de dados especiais de saúde em larguíssima escala, foram ouvidos a Autoridade Europeia para a Proteção de Dados e o Comité Europeu para a Proteção de Dados, nos termos do artigo 42.º do Regulamento (UE) 2018/1725. Essas entidades emitiram um parecer conjunto em 31 de março de 2021. [88] Em 14 de junho de 2021, foi editado o Regulamento (EU) 2021/953, cujo objeto era o estabelecimento de um regime para a emissão, verificação e aceitação de certificados interoperáveis de vacinação, teste e recuperação da COVID-19 («Certificado Digital COVID da UE»), para facilitar o exercício do direito de livre circulação dos seus titulares durante a pandemia e contribuir, também, para facilitar o levantamento gradual das restrições à livre circulação adotadas pelos Estados-membros, em conformidade com o direito da União, para limitar a propagação do SARS-CoV-2, de forma coordenada (art. 1.º).

[87] Também conhecido como Certificado Verde Digital.

[88] Joint Opinion EDPB and EDPS 04/2021 na versão em língua portuguesa pode ser encontrado em https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042021-proposal_pt (acedido em janeiro de 2022).

3.1 Questões polémicas e riscos para a autodeterminação digital

O tema do Certificado Digital COVID da UE envolve um debate intenso sobre questões ético-jurídicas, muitas das quais estão além dos limites do presente estudo. Isso decorre, desde logo, das consequências de se adotar o Certificado como passaporte para a retoma da livre-circulação.

No próprio parecer conjunto EDPB/EDPS acima referido, há menção expressa a essa situação, com especial ênfase para a manifestação da Organização Mundial da Saúde (OMS), no seu «*Interim position paper: considerations regarding proof of COVID-19 vaccination for international travellers*», de 5 de fevereiro de 2021, em que declarou: "(...) as autoridades nacionais e os operadores de transporte não devem introduzir requisitos de prova de vacinação contra a COVID-19 aplicáveis às viagens internacionais como condição para a partida ou para a entrada, dado que ainda existem incógnitas críticas a respeito da eficácia da vacinação na redução da transmissão".

O parecer conjunto EDPB/EDPS também mencionava o estudo desenvolvido pelo Instituto Ada Lovelace, intitulado "*What place should COVID-19 vaccine passports have in society*?".[89] Neste estudo leem-se as conclusões de pesquisas sobre o tema da adoção da vacinação contra a COVID-19 como elemento para discriminação entre pessoas, com o objetivo de imposição de limitações mais severas à liberdade individual, considerado o alegado risco de transmissão do vírus. O trabalho do Instituto Ada Lovelace foi desenvolvido por *experts* nas áreas de imunologia, epidemiologia, sociologia, desenvolvimento internacional, direito, história da medicina, saúde pública, ética e *design* de sistemas. De entre as conclusões a que chegou o grupo multidisciplinar, destaca-se a seguinte: *"At present, vaccination status does not offer clear or conclusive evidence about any individual's risk to others via transmission, so cannot be a robust basis for risk-based decision making, and therefore any roll-out of a digital passport is not currently justified".*

O próprio parecer conjunto destaca esse ponto, no seu item 14, quando assevera: "A este respeito, observamos que, no momento da elaboração do presente parecer conjunto,

[89] Ada Lovelace Institute - **What place should COVID-19 vaccine passports have in society? Findings from a rapid expert deliberation chaired by Professor Sir Jonathan Montgomery.** [Em linha]. Atual. [Consultado em 12 de maio de 2022]. Disponível em https://www.adalovelaceinstitute.org/summary/covid-19-vaccine-passports/

parecem existir poucos dados científicos que corroborem o facto de que a toma de uma vacina contra a COVID-19 (ou a recuperação da COVID-19) conceda imunidade e a duração dessa imunidade". O parecer data de 31 de março de 2021[90].

É este o primeiro ponto da marcante polémica gerada com a utilização do certificado vacinal como elemento de discriminação de pessoas não vacinadas (e não submetidas ao teste ou recuperadas da doença). A base ético-jurídica para o estabelecimento do discrímen pressupunha que se estabelecesse, solidamente, a premissa de que aqueles vacinados seriam incapazes de transmitir o vírus; ao contrário, não se poderia justificar o tratamento diferenciado.

Este tema tem óbvia relação com a proteção de dados, uma vez que o certificado digital não é outra coisa senão um repositório de dados pessoais de saúde, armazenados digitalmente ou em papel. A necessidade de se exibir um conjunto desses dados como condição para se obter maior liberdade, numa sociedade moderna, envolve claramente a autodeterminação informativa, que se define, relativamente a cada pessoa, como "o direito de controlar a informação disponível a seu respeito, impedindo-se que a pessoa se transforme em «simples objeto de informação»" na feliz expressão de Gomes Canotilho e Vital Moreira.[91]

Em qualquer situação que envolva um tratamento diferenciado entre cidadãos da UE, ainda que respaldada no interesse público, deve-se sempre ter em mente o princípio da proporcionalidade e o que dispõe o artigo 52.º da CDFUE:

> Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efectivamente a objectivos de interesse geral reconhecidos pela União, ou à necessidade de protecção dos direitos e liberdades de terceiros.

Especificamente sobre essa questão, OSKAR JOSEF GSTREIN, ANDREJ ZWITTER E DIMITRY KOCHENOV[92] chegam a referir uma "onda de *apartheid*" a ser evitada, destacando que

---

[90] Sobre o tema da propagação do vírus pelos vacinados, Andrew Lee, professor de saúde pública na Universidade de Sheffield, na Inglaterra, manifesta-se num artigo publicado em janeiro de 2022 no *site The Conversation* (https://theconversation.com/faroe-islands-superspreader-event-why-transmission-among-the-triple-vaxxed-shouldnt-alarm-you-174301) (acedido em julho de 2022): *"There is now ample evidence that shows the vaccines are not very effective at stopping a vaccinated person from getting infected or from spreading infection. This was graphically illustrated by a superspreading event that took place in the Faroe Islands where 21 out of 33 triple-vaccinated healthcare workers who attended a private gathering caught omicron. This was also despite the fact that several had done a PCR or lateral flow test in the 36 hours before the event".*

[91] Op. cit. p. 557.

[92] GSTREIN, Oskar Josef, ZWITTER, Andrej e KOCHENOV, Dimitry - **A Terrible Great Idea? COVID-19 'Vaccination Passports' in the Spotlight**, [Em linha]. Atual. [Consultado em 9 maio de 2022]. Disponível em https://www.compas.ox.ac.uk/2021/a-terrible-great-idea-covid-19-vaccination-passports-in-the-spotlight/

a questão do passaporte vacinal não envolve tantos problemas técnicos (*privacy by design*) mas, sim, questões sociais, de integração: *"the technical design to make vaccination passports 'private by design', secure and usable are relatively minor. (…) Ultimately, what counts is not the technical fix, but the implementation in society. There is no way to hack oneself out of this pandemic. In order to avoid that the next wave of the COVID-19 pandemic will be the 'wave of apartheid', we need thoughtful, feasible and practical solutions that are widely accessible and work for everyone*".[93]

A implantação do passaporte vacinal, conjugado com a paulatina liberação de algumas atividades para os portadores, e só para eles, pela pluralidade de situações que envolve, é capaz de gerar polémicas infindáveis, além de lançar os não vacinados em situação de inegável prejuízo no que concerne as suas liberdades. A medida pode ter a sua proporcionalidade em relação ao objetivo de interesse público prosseguido posta em causa, tendo em vista o princípio da dignidade da pessoa humana, assim como diante da incerteza quanto à sua efetividade.

3.2 Desvio da Finalidade Determinada – A utilização do Certificado Digital pelos Estados-Membros para objetivos não previstos no REGULAMENTO (UE) 2021/953 de 14 de junho de 2021

O Certificado Digital, como destacado, foi concebido para garantir o direito fundamental de livre circulação, especialmente no território dos Estados-Membros da União Europeia, e superar as restrições à entrada ou a exigência, para os viajantes transfronteiriços, de cumprimento de autoisolamento ou testagem para despistagem da infeção por SARS-CoV-2.

A sua criação decorreu do facto de, naquele momento (primeiro semestre de 2021), muitos Estados-Membros terem lançado ou tencionavam lançar iniciativas para a emissão de certificados de vacinação, cumprindo à União regulamentar e uniformizar a medida, com o

[93] Considerem-se, também, neste contexto, as advertências de Steven Greenberg, no artigo *online* "*I'm triple-vaxxed. The Green Pass system is bankrupt. The system marginalizes and publicly humiliates the unvaccinated, punishing rather than reforming, and creating even greater rifts in Israeli society".* Em (https://blogs.timesofisrael.com/im-triple-vaxxed-the-green-pass-system-is-bankrupt/) (acedido em Janeiro de 2022); "*The unvaxxed will continue to live and work among us. They will continue to be our neighbours, parents in the schools our children attend, shoppers in the supermarkets we frequent. Demonization and public humiliation of the unvaxxed serve nothing but the most base of our instincts".*

objetivo de impedir perturbações significativas no exercício do direito de livre circulação que pudessem ser causadas pelos Estados-Membros, em iniciativas unilaterais capazes de prejudicar o bom funcionamento do mercado interno, nomeadamente do turismo.

Foi esse o intuito declarado do legislador da União ao adotar o Regulamento (UE) 2021/953 de 14 de junho de 2021 relativo a um regime para a emissão, verificação e aceitação de certificados interoperáveis de vacinação, teste e recuperação da COVID-19 (Certificado Digital COVID da UE), a fim de facilitar a livre circulação durante a pandemia de COVID-19. [94]

O artigo 10.º, 2, do Regulamento é claro sobre a finalidade para a qual os dados pessoais são inseridos no Certificado:

> Para efeitos do presente regulamento, os dados pessoais contidos nos certificados emitidos nos termos do presente regulamento são tratados apenas para efeitos de acesso e verificação das informações constantes do certificado, a fim de facilitar o exercício do direito de livre circulação na União durante a pandemia de COVID-19.

Interessante notar que o Regulamento 2021/953 reconhece que o RGPD é aplicável ao tratamento de dados necessário para a emissão, verificação e aceitação do Certificado Digital e estabelece como fundamento jurídico para o tratamento, além do artigo 6.º, n.º 1, alínea *c*), do RGPD, o artigo 9.º, 2, alínea *g*) daquele Regulamento. Este aspeto demonstra que a finalidade ali declarada não é a da alínea *i*), como parece, à primeira vista, ser a mais apropriada. O interesse público, em questão, a partir dessa premissa fixada pelo Regulamento, seria permitir a livre circulação mais do que algum interesse público no domínio da saúde pública.

Como decorre do artigo 9.º, 2, alínea *g*), do RGPD, o tratamento desses dados deve: *i*) respeitar o princípio da proporcionalidade diante do objeto visado; *ii*) respeitar a essência do direito à proteção de dados pessoais; iii) prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados.[95]

Segundo MENEZES CORDEIRO, respeitar a essência do direito à proteção de dados significa que "do tratamento não pode resultar um total esvaziamento da intrínseca relação pessoal e individual existente entre os dados tratados e o seu titular."[96] Isto importa em que

---

[94] Veja-se, a este respeito, o considerando n.º 12: "A fim de facilitar o exercício do direito de livre circulação e residência no território dos Estados-Membros, deverá ser estabelecido um regime comum para a emissão, verificação e aceitação de certificados interoperáveis de vacinação, teste e recuperação da COVID-19 (Certificado Digital COVID da UE)".

[95] Destaque-se o facto de que a alínea *g*) não contém qualquer referência ao sigilo profissional, diferentemente do que acontece com a alínea *i*) do mencionado dispositivo.

[96] Op. cit. p. 249

qualquer limitação à privacidade deva dar-se no limite do necessário[97], fazendo-se a ponderação equilibrada dos interesses em questão, sendo que tal não pode ir ao ponto de atingir os elementos essenciais do direito subjetivo à proteção de dados.

Porém, como se constatou logo em seguida, a finalidade para a qual foi concebido o Certificado e que é a justificativa para o tratamento dos dados pessoais nele contidos acabou por ser alargada indevidamente pelos Estados-Membros, criando-se uma situação de facto em que a exposição dos dados sensíveis de saúde passou a ser necessária como condição para o exercício de outros direitos, não apenas de livre circulação, o que levou a que esses dados fossem objeto de generalizada exposição e consulta.

É bom destacar que a consulta aos dados, por si só, caracteriza tratamento, conforme o artigo 4.º, 2, do RGPD.

Tal situação, em que os dados sensíveis de saúde são tornados públicos, como requisito para praticamente toda e qualquer atividade social, desde o comparecimento em festas, a frequência em restaurantes ou salas de espetáculo, inegavelmente representa o esvaziamento completo do direito à proteção desses dados, à autodeterminação informativa. É clara a violação ao próprio artigo 9.º, 2, alínea *g*) do RGPD, em que se fundamenta o Regulamento 2021/953, de 14 de junho de 2021. Mais ainda se há de considerar ilegal a situação ao ter como fundamento legal do tratamento a alínea *i*), do mencionado inciso, que parece ser a pertinente. Isto porque tal alínea menciona expressamente o sigilo profissional que estaria impossibilitado numa situação destas, de ampla exposição dos dados de saúde.

O Parecer Conjunto EDPB/EDPS acima referido já manifestava o receio de que os certificados tivessem a sua destinação indevidamente expandida pelos Estados-Membros, para além dos limites objetivos declarados pela União, de permitir a livre-circulação. O seguinte trecho do parecer é indicativo desse risco que já então se antecipava:

> O CEPD e a AEPD consideram que, dado o caráter da ingerência das medidas apresentadas pela proposta, qualquer outra eventual utilização do quadro e do Certificado Verde Digital com base no direito dos Estados-Membros, outra que não a facilitação do direito de livre circulação entre os Estados-Membros da UE, não é abrangida pelo âmbito de aplicação da proposta nem se insere, por conseguinte, no parecer conjunto do CEPD e da AEPD. Não obstante, o CEPD e a AEPD consideram que se os Estados-Membros persistirem na implementação do Certificado Verde Digital com base no direito dos Estados-Membros para qualquer outra eventual utilização que não a utilização prevista de facilitar a livre circulação entre os Estados- Membros da UE, tal poderá acarretar consequências e riscos indesejados para os direitos fundamentais dos cidadãos da UE.

[97] TJUE, acórdão Schecke, processos apensos C-92/09 e C-93/09, item 77: "as derrogações à protecção dos dados pessoais e as suas limitações devem ocorrer na estrita medida do necessário".

No mesmo parecer, advertia-se: "Ao abrigo de uma base jurídica nacional, qualquer outra utilização do Certificado Verde Digital e do quadro conexo não deveria ser suscetível, jurídica ou factualmente, de comportar discriminação baseada em ter (ou não) sido vacinado ou ter recuperado da COVID-19".[98]

Já era expectável que os Estados-Membros pudessem pretender criar legislações nacionais que autorizassem a utilização do Certificado Digital como um requisito de facto para a prática de atividades triviais, como acesso a bares e restaurantes, salas de espetáculos, cultos, lojas, ginásios, e outras atividades assemelhadas, e assim tentar impulsionar as próprias economias, aliviando os seus cidadãos das restrições decorrentes da pandemia. Tal alívio, entretanto, não seria extensível a todos, senão aos que tivessem consigo os certificados digitais, repletos de dados sensíveis, verdadeiras insígnias sem as quais não se abriam as portas para o 'novo normal'.

Porém, tal medida, é impossível negar, representaria um avanço aos limites da finalidade declarada na criação do Certificado e traria, segundo o parecer, "riscos indesejados para os direitos fundamentais dos cidadãos da UE". Em outras palavras, poderia representar o que GSTREIN, ZWITTER E KOCHENOV chamaram "*wave of apartheid*".

Em Portugal, o Decreto-Lei n.º 54-A/2021, de 25 de junho, cujo objeto era executar, na ordem jurídica interna, o Regulamento (EU) 2021/953, logo no seu introito, revelou o desvio da finalidade. Com efeito, no Decreto-Lei, prevê-se que os Certificados Digitais possam ser utilizados, para além dos fins previstos no Regulamento, também "em matéria de acesso a eventos de natureza cultural, desportiva, corporativa ou familiar."[99] Nenhuma dessas finalidades se encontra ou mesmo sequer é sugerida no Regulamento 2021/953 de 14 de junho de 2021.

Deve ser enfatizado que nem mesmo se cuidou de incluir, no Decreto-Lei, com base no artigo 4.º, 2, *g*) do RGPD, disposições específicas sobre as categorias de entidades que

---

[98] O parecer conjunto menciona ainda que "a inclusão de tal base jurídica no direito dos Estados-Membros deve, no mínimo, incluir disposições específicas que identifiquem claramente o âmbito e a extensão do tratamento, a finalidade específica subjacente, as categorias de entidades que podem proceder à verificação do certificado, bem como as garantias relevantes para evitar o abuso, tendo em conta os riscos para os direitos e as liberdades dos titulares dos dados."

[99] O *site* do Diário da República eletrónico em que é publicado o DL, na parte relativa ao resumo em linguagem clara (sem valor legal), contém o seguinte: "este decreto-lei permite que quem tenha um Certificado Digital COVID da UE não fique sujeito a restrições em matéria de viagens aéreas e marítimas com destino a Portugal, em matéria de circulação pelo território nacional e em matéria de acesso a determinados eventos."

pudessem proceder à verificação do certificado, e nem se previram garantias para os titulares de dados com o objetivo de se evitarem os abusos, como reputavam necessário tanto o CEPD como a AEPD no parecer conjunto anteriormente mencionado.

Repise-se que o simples ato de consulta aos dados constantes no Certificado Digital já representa tratamento e não há um regime jurídico que garanta aos titulares de dados o respeito ao sigilo que é devido por parte daqueles que tenham contato com o Certificado, conforme exigido na alínea *i*) do n.º 2 do artigo 9.º do RGPD.[100]

Além disso, a submissão dos dados sensíveis de saúde à exposição generalizada, para os fins mais comezinhos e triviais, reverte na completa aniquilação da privacidade que deve permear o tratamento desses dados.

Diante de um cenário com tais características, que a reação dos Estados à pandemia acabou por criar, é mesmo difícil cogitar a previsão de medidas "adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados". É irrecusável o atentado que se comete contra a autodeterminação informativa digital, pois os titulares dos dados, em tal situação, não exercem qualquer controlo sobre a sua divulgação e nem sequer detêm meios para fazerem prevalecer o conjunto dos seus direitos previstos no RGPD (capítulo III).

3.3 Utilização dos Dados do Certificado para fins não ligados à situação de Saúde Pública

OSKAR JOSEF GSTREIN,[101] ao examinar a proposta de texto para o regulamento do Certificado Digital manifesta a sua preocupação com situações em que os dados sensíveis possam ser utilizados para outras finalidades, diversas da que justificou a sua coleta. Traz exemplos de casos que revelaram quebra do compromisso em que a utilização dos dados de saúde seria feita apenas para situações de combate à doença.

---

[100] Não obstante o facto de se ter feito referência à alínea *g*) do inciso 2.º do artigo 9.º do RGPD, no Regulamento 2021/953, tratando-se de dados sensíveis de saúde tratados para os fins de interesse público no domínio da saúde pública, parece mais adequado convocar-se a aplicação da alínea *i*) e não há razão para se dispensar a exigência do sigilo. O RGPD refere-se a sigilo profissional, o que conduz à ideia de que aqueles que devem tratar dados de saúde, nas hipóteses da citada alínea *i*), devem ser profissionais de saúde e não terceiros sem essa qualificação.

[101] GSTREIN, Oskar Josef "The EU Digital COVID Certificate: A Preliminary Data Protection Impact Assessment" European Journal of Risk Regulation , Volume 12 , Special Issue 2: Symposium on COVID-19 Certificates and Special Issue on the Global Governance of Alcohol, June 2021 , pp. 370 – 381 DOI: https://doi.org/10.1017/err.2021.29 Cambridge University Press

Este ponto é da maior relevância. OSKAR JOSEF GSTREIN, num artigo que produziu com comentários e críticas ao Parecer Conjunto,[102] destaca:

> While the DPAs acknowledge that the Commission does not plan to establish a central database, questions have emerged about the oversight of data storage at the national level. In addition, even if the EUDCC is suspended at the EU level, it might be possible that nation states will continue to use their respective systems, which might also contain data originating from other Member States. The question not only relates to how such data could be updated, revised or deleted. Even more concerning is a scenario where nation states adopt dedicated national laws to keep the systems originally intended for the EUDCC running and start to use them for other purposes such as national security. The updated draft addresses this issue in Article 9 paragraphs 3 and 3a but there is no comprehensive guarantee that one or more Member State(s) will not use the data from the EUDCC in other contexts based on national laws.

E, no mesmo artigo, GSTREIN menciona casos que motivam a sua preocupação, a saber: i) a polícia de Singapura acedia aos dados dos aplicativos de rastreamento de contato apesar de promessas do governo local de que tal não seria admitido[103]; ii) a polícia alemã utilizou informações extraídas desses aplicativos de rastreamento, obrigatórios em *pubs* e restaurantes, para fins de investigação criminal; iii) as autoridades austríacas pretendiam inserir as informações obtidas com o certificado numa base abrangente de dados para vincular as informações com dados estatísticos relativos a histórico no trabalho, receitas, licenças de doença e educação, medida que teria sido bastante criticada.[104]

São situações que revelam o perigo, para autodeterminação digital, que envolve a coleta de dados pessoais de saúde para viabilização do Certificado Digital, e o risco para a efetividade do princípio da limitação da finalidade prevista no artigo 5.º, i, *b*) do RGPD.

3.4 Fiscalização – acesso a dados sensíveis por particulares – Da Sociedade da Informação para a Sociedade da Vigilância

Segundo SHOSHANA ZUBOFF,[105] o capitalismo de vigilância inicia-se

---

[102] GSTREIN, Josef Oskar, The EU Digital COVID Certificate: **A Preliminary Data Protection Impact Assessment**, [Em linha]. Atual. Consultado em 10 de julho de 2022. Disponível em https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/eu-digital-covid-certificate-a-preliminary-data-protection-impact-assessment/F51BABA3959C62E1EE9EFDB26D21EBB9#fn16

[103] A esse respeito, veja-se a abordagem de Mia Sato em MIT Technology Review, em: https://www.technologyreview.com/2021/01/05/1015734/singapore-contact-tracing-police-data-covid/.

[104] *Op cit*. pp 379/380

[105] ZUBOFF, Shoshana - **A era do Capitalismo da Vigilância – A disputa por um Futuro Humano na Nova Fronteira do Poder**.: Lisboa Relógio D´Água Editores, 2019. ISBN 978-989-783-090-7, p.374.

> Com a descoberta do *excedente comportamental* mais ou menos à-mão-de-semear no ambiente online, quando se percebeu que o «exaustor de dados» que entupia os servidores da Google podia ser combinado com suas potentes capacidades analíticas e com eles produzir previsões do comportamento dos utilizadores. Estes *produtos preditivos* seriam a base de um processo anormal de vendas lucrativas que criou novos *mercados de comportamento futuro*. A inteligência automática da Google foi melhorando à medida que o volume de dados aumentava, criando melhores produtos preditivos. Esta dinâmica determinou o *imperativo de extração*, o qual exprime a necessidade de *economias de escala na acumulação de excedentes* e que depende de sistemas automatizados que rastreiam, perseguem e induzem implacavelmente mais excedentes comportamentais. A Google impôs uma lógica da conquista, definindo a experiência humana como livre para recolher, disponível para renderizar na forma de dados e reivindicar como um ativo de vigilância. A empresa aprendeu a utilizar uma variedade de estratégias retóricas, políticas e tecnológicas para ofuscar esses processos e suas implicações.

A autora desenvolve o seu pensamento, descrevendo as fases mais avançadas de desenvolvimento desse processo e sustentando que os "capitalistas de vigilância são empurrados do mundo virtual para o mundo real, com oportunidades de abastecimento ubíquo", para que "os produtos preditivos se aproximem da certeza e garantam resultados comportamentais", para em seguida "intervirem na situação corrente e moldarem de forma ativa o comportamento da própria fonte".

É assustador este cenário que vai da vigilância à interferência no mundo real.

Mas os capitalistas não estão sozinhos neste processo apesar de serem inegavelmente o seu principal vetor. Assim, também os governos, cada vezmais, se assenhoreiam dos dados pessoais dos cidadãos, para controlo e interferência na sociedade.

E, com a pandemia da COVID-19, essa vigilância passou a ser largamente exercida, em nome dos interesses do Estado, pelos próprios cidadãos.

Como bem disse ZUBOFF,

> Seria incorreto assumir que o capitalismo da vigilância se consegue entender apenas pelo prisma da sua ação económica, ou que os desafios defrontados se restringem a discernir, conter ou transformar os seus mecanismos fundamentais. As consequências desta nova lógica de acumulação já ultrapassaram e continuarão a ultrapassar as práticas comerciais, influenciando a textura das nossas relações sociais, transformando o relacionamento connosco e com os outros. Estas transformações são o chão no qual o capitalismo de vigilância floresceu: uma espécie invasiva que cria a sua própria fonte de nutrição. Ao transformar-nos, alimenta a sua própria marcha.[106]

A medida adotada pelos Estados-membros, de atribuir a particulares a fiscalização e verificação doCertificado nas situações enquadradas no largo espectro previsto na lei, como o

[106] *Op. cit*. p. 384

acesso a eventos de natureza cultural, desportiva, corporativa ou familiar, representa mais um passo no sentido da vigilância das pessoas pelos seus pares.

Em certa medida, a situação revela como a sociedade tem optado por soluções jurídicas que restringem, cada vez mais, a liberdade individual, esvaziando o conteúdo dos direitos à privacidade. A sociedade da informação transforma-se progressivamente na sociedade da vigilância, com a participação disseminada de indivíduos nessa tarefa, estejam ou não munidos de poder estatal.

A situação que decorreu das medidas de combate à pandemia provocou a banalização da função de fiscalizar o atendimento a requisitos escolhidos pela lei para o exercício de direitos e liberdades. Patrões, empregados, empregados de lojas, restaurantes, salas de espetáculo, e toda uma coletividade de pessoas sem qualquer preparação ou responsabilidade legal passaram a exercer a função que deveria ser pública, de fiscalizar, impedir ou autorizar o exercício de direitos e de operar o tratamento de dados sensíveis, em auxílio ao Estado na tarefa de controlar o cidadão. E mais grave ainda é a tarefa de verificação da temperatura corporal (que também configura tratamento de dados de saúde) para fins de controlo de acesso ao local de trabalho, acesso a serviços ou instituições públicas, estabelecimentos educativos e espaços comerciais, culturais ou desportivos, meios de transporte, em estruturas residenciais, estabelecimentos de saúde, estabelecimentos prisionais ou centros educativos, como chegou a ser previsto no artigo 4.º do Decreto do Conselho de Ministros n.º 8/2020.

A reação das autoridades de proteção de dados diante dessa situação foi tíbia. A própria sociedade aceitou essas medidas e pô-las em prática. É de facto uma tarefa difícil a de impedir, por qualquer meio, a adoção de estratégias que aparentam ser, num determinado momento, essenciais para o combate à pandemia e para o alívio das medidas rigorosas de *lock down*.

CONCLUSÃO

A crise causada pela pandemia, com a consequente necessidade de imposição de severas limitações sociais, sanitárias e pessoais à população mundial, em especial no seu direito de livre locomoção, acabou por gerar uma tendência nos governos para utilizar os dados especiais de saúde como instrumento de combate à propagação do vírus.

As empresas de tecnologia rapidamente desenvolveram aplicativos para rastreio dos infetados e dos seus contatos e estes passaram a ser uma ferramenta tentadora para se enfrentar a pandemia, controlando aqueles doentes ou suspeitos de estarem infetados, para concentrar sobre eles, e não sobre os demais, as restrições aos direitos e às liberdades de locomoção.

Outra forma de se atingir objetivo semelhante foi a criação de certificados sobre o estado de imunidade do cidadão, a partir de três vetores que indicavam o estado de vacinação, a recuperação recente da doença ou o teste de despistagem.

A discriminação entre portadores e não portadores do certificado, assim justificada pelo interesse público em se retomarem as atividades económicas, culturais e sociais, entretanto, acabou por pôr em causa a estrutura que fora criada para a defesa dos interesses dos titulares de dados pessoais, submetida a compreensível pressão para que a privacidade não fosse empecilho para a retoma das atividades económicas.

As entidades de defesa da proteção dos dados, alarmadas, advertiram sobre os riscos do que poderia vir a suceder. Primeiramente, tentou-se impor a utilização de aplicativos de geolocalização para controlo e rastreio dos infetados. Se a empreitada fosse bem-sucedida, o primeiro passo estaria dado para a verificação do temido cenário orwelliano de controlo da população. Mas a força do Direito foi intransponível e, pelo menos em Portugal, a medida não passou.

Mas nada foi capaz de impedir a adoção do certificado digital, inicialmente destinado a aliviar a população das restrições à livre circulação no âmbito da UE, e que teve o seu destino grandemente ampliado, para permitir a retoma das atividades daqueles que o tivessem.

Era expectável que tal ocorresse, diante do avanço da vacinação e do impacto que essa situação causou na redução dos casos e, especialmente, dos internamentos.

Mas isto não se deu sem que os direitos de privacidade dos titulares dos pessoais de saúde fossem atingidos. Admitir que se torne obrigatória ou quase-obrigatória a exposição de uma gama de informações de saúde a toda a hora e a quem quer que seja, para se poder entrar

num restaurante ou num café, transformando esses dados em passaporte para atos rotineiros da vida, é esvaziar o conteúdo do direito à confidencialidade desses dados.

A convocação da população, impreparada e desprevenida, sem vínculo formal com o Estado ou mesmo consciência da importância e responsabilidades que cercam o tratamento de dados sensíveis, para a tarefa de fiscalizar o cumprimento da lei representou mais um passo no sentido da consolidação da sociedade da vigilância, em detrimento do direito à autodeterminação.

A pandemia deve passar. Já se foram os dias mais agudos e o porvir é alvissareiro. Mas as escolhas feitas hão de moldar as nossas vidas no futuro.

REFERÊNCIAS BIBLIOGRÁFICAS

1 SARAMAGO, José - **Ensaio sobre a Cegueira**. Lisboa: Livraria Lello e Porto Editora, 2021. ISBN 978-989-8939-97-5.

2 BARATA, Clara – **O que aprendemos sobre o covid-19 nos últimos dois anos** [Em linha]. *Jornal Público*, 31 de dezembro de 2021. Atual. [Consultado em 19 de março de 2022]. Disponível em https://www.publico.pt/2021/12/31/ciencia/noticia/aprendemos-covid19-ultimos-dois-anos-1990319.

3 **European Center for Disease Prevention and Control Cfr. European Center for Disease Prevention and Control, «Event Background COVID-19»** [Em linha]. Atual. [Consultado em 21 de abril de 2022]. Disponível em https://www.ecdc.europa.eu/en/novel-coronavirus/event-background-2019) acesso em fevereiro de 2022.

4, 60, 61 HARARI, Yuval Noah – **O mundo após o do coronavírus** [Em linha]. *Financial Times,* 20 de março de 2020. Atual. [Consultado em 30 de fevereiro de 2022]. Disponível em https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75.

5 TIFFANY C. LI - **Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis,** 52-3 Loyola University, *Chicago Law Journal* 767 (2021) [Em linha]. Atual. [Consultado em 18 de julho de 2022]. Disponível em https://scholars.unh.edu/cgi/viewcontent.cgi?article=1459&context=law_facpub.

7 MIRANDA, Jorge – **A Constituição e a dignidade da pessoa humana**. Lisboa: Didaskalia, 1999. ISSN 0253-1674. 29:1-2 (1999) 473-485.

OLIVEIRA, Fernando António Rodrigues da Silva Coutinho **- Breves considerações a respeito do princípio da dignidade da pessoa humana** [Em linha]. Tese de mestrado da FDUP em 1.07.2013. Atual. [Consultado em 10 de junho de 2022]. Disponível em https://sigarra.up.pt/fdup/pt/pub_geral.pub_view?pi_pub_base_id=24817.

8 GUIMARÃES, M.R. e REDINHA, M.R. - A Portuguese Approach to Privacy in COVID-19 Times: Through the Keyhole. In E. Hondius, M. Santos Silva, A. Nicolussi, P. Salvador Coderch, C. Wendehorst and F. Zoll (eds.), **Coronavirus and the Law in Europe** [Em linha]. *Intersentia Online*, 2021. Atual. [Consultado em 15 de janeiro de 2022]. Disponível em https://www.intersentiaonline.com/permalink/1fac1271118a21090498ddef1399707b.

9 CARVALHO, Orlando de - **Teoria Geral do Direito Civil**. 3ª ed. Coimbra: Coimbra Editora, 2012, p. 26.

10 PEREIRA, Caio Mário da Silva - **Instituições de Direito Civil**. 19ª ed. Rio de Janeiro: Forense, 2002, p. 154.

11 SZANIAWSKI, Elimar - **Direitos de personalidade e sua tutela**. São Paulo: Revista dos Tribunais, 1993, p. 11.

12 MIRANDA, Jorge - **Curso de Direito Constitucional.** Lisboa: Universidade Católica Editora, 2016, 2, p. 58.

13 WARREN, Samuel D. e BRANDEIS, Louis - **O Direito à Privacidade** [Em linha]. *Harvard Law Review,* Vol. IV, 15 de dezembro de 1890. Atual. [Consultado em 28 de fevereiro de 2022]. Disponível em https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.ht ml.

14 ALVES, Lurdes Dias - **Proteção de Dados Pessoais no Contexto Laboral**. Coimbra: Almedina, 2020. ISBN 978-972-40-8581-4. Pp. 13-14.

15, 16, 22, 23, 25, 39, 40, 45, 70, 82 CORDEIRO, A. Barreto Menezes - **Direito da proteção de dados: à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020. ISBN 978-972-40-8304-9. p. 32.

18, 41, 81 PINTO, Paulo Mota - **Direitos de Personalidade e Direitos Fundamentais: estudos**. Coimbra: Gestlegal, 2018.

19 KONDER, Carlos Nelson - O tratamento de dados sensíveis à luz da Lei 13.709/2018. In TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coordenação) - **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. 1ed. São Paulo: Thomson Reuters Brasil, 2019. P. 451.

20 CARVALHO, Jorge Morais - **Manual de Direito do Consumo**. 6ª ed. Coimbra: Almedina, 2019. ISBN 978-972-40-7833-5. P.56.

26, 51 CANOTILHO, Gomes e MOREIRA, Vital - **Constituição da República Portuguesa Anotada**. 4.ª ed. Coimbra: Coimbra Editora, 2007. ISBN: 9789725405413. Vol. 1, pp. 551, 557.

27 SOUSA Ribeiro, J. - A tutela de bens da personalidade na Constituição e na jurisprudência constitucional portuguesas. In **Estudos de Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho.** Coimbra: Coimbra Editora. ISBN 9789723220537. Vol. III, "Direitos e Interconstitucionalidade: entre Dignidade e Cosmopolitismo", p. 853.

30 PARLAMENTO EUROPEU - Artigo sobre proteção de dados Atual. [Consultado em 28 de janeiro de 2022]. Disponível em https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf

31 CONSELHO DA EUROPA. Atual. [Consultado em 17 de março de 2022]. Disponível em março de 2022 (https://rm.coe.int/16808ade9d)

32 COMISSÃO EUROPEIA – esclarecimento sobre direito derivado. Atual. [Consultado em 30 de abril de 2022]. Disponível em https://ec.europa.eu/info/law/law-making-process/types-eu-law_pt

53 DEODATO, Sérgio - **A proteção dos dados pessoais de Saúde**. Lisboa: Universidade Católica Editora. 2017 .ISBN 9789725405789. p. 13.

54, 74 DIAS, Patrícia Cardoso - **Proteção de dados pessoais no contexto da pandemia provocada pelo novo coronavírus SARS-COV-2: aspetos ético-jurídicos relevantes da proteção de dados de saúde no âmbito da emergência de saúde pública** *Revista Julgar Online* [Em linha]. Janeiro de 2021-1, Atual. [Consultado em 28 de abril de 2022]. Disponível em http://julgar.pt/protecao-de-dados-pessoais-no-contexto-da-pandemia-provocada-pelo-novo-coronavirus-sars-cov-2-aspetos-etico-juridicos-relevantes-da-protecao-de-dados-de-saude-no-ambito-da-emergencia-de-saude-publica/ .

56 Organização Mundial de Saúde - OMS - Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing, Interim guidance, de 28.05. 2020 (acedido em junho 2022): https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1

58, 59 VÉLIS, Carissa - **Privacidade é Poder, por que razão e como devemos recuperar o controle dos nossos dados, Temas e Debates**. Lisboa: Bertrand Editora Ltda., 2022. ISBN 978-989-644-688-8.

84, 85 DONALD, Alice e LEACH, Phillipe - **Human Rights – The Essential Frame of Reference in the Global Response to COVID-19** [Em linha]. 2020/5/12. Atual. [Consultado em 10 de abril de 2022]. Disponível em https://verfassungsblog.de/humanrights-the-essential-frame-of-reference-in-the-global-response-to-covid-19/ (acedido em junho de 2022).

90 Ada Lovelace Institute - **What place should COVID-19 vaccine passports have in society? Findings from a rapid expert deliberation chaired by Professor Sir Jonathan Montgomery.** [Em linha]. Atual. [Consultado em 12 de maio de 2022]. Disponível em https://www.adalovelaceinstitute.org/summary/covid-19-vaccine-passports/

93, 102, 103 GSTREIN, Oskar Josef, ZWITTER, Andrej e KOCHENOV, Dimitry - **A Terrible Great Idea? COVID-19 'Vaccination Passports' in the Spotlight**, [Em linha]. Atual. [Consultado em 9 maio de 2022]. Disponível em https://www.compas.ox.ac.uk/2021/a-terrible-great-idea-covid-19-vaccination-passports-in-the-spotlight/

106 ZUBOFF, Shoshana - **A era do Capitalismo da Vigilância – A disputa por um Futuro Humano na Nova Fronteira do Poder**.: Lisboa Relógio D´Água Editores, 2019. ISBN 978-989-783-090-7, p.374.

CNPD

43, 64 , 79 Comissão Nacional de Proteção de Dados– **pareceres/orientações**

43 - parecer 2020/116 de 28 de setembro de 2020 em https://www.cnpd.pt/decisoes/pareceres/

64 -orientação sobre divulgação de informações relativas a infetados por COVID-19 em https://www.cnpd.pt/media/4i4hmccv/orientacoes_divulgacao_informacao_infetados_covid-19.pdf

79 – parecer 2020/129 da CNPD https://www.cnpd.pt/covid-19/ e é intitulado - Parecer sobre a obrigatoriedade do uso de máscara para acesso ou permanência nos espaços e vias públicas e a obrigatoriedade de utilização da aplicação Stayaway Covid

Referências bibliográficas do domínio da Jurisprudência [Em linha]. Atual. [Consultadas ao longo da execução do presente trabalho].

Notas 24, 28, 29, 34, 37

Tribunal de Justiça da União Europeia

Acórdão proferido no julgamento dos processos apensos C-92/09 e C 93/09 (itens 47 e 48), disponível em https://curia.europa.eu/juris/liste.jsf?num=C-92/09&language=en

Acórdão proferido no julgamento dos processo c-112/00 schmidberger, disponível em https://curia.europa.eu/juris/liste.jsf?num=C-112/00

Acórdão de 8 de abril de 2014, - processos apensos C-293/12 e C-594/12, disponível em https://curia.europa.eu/juris/liste.jsf?language=pt&num=C-293/12).

Acórdão de 09.03.1978 - processo C-106/77 (Simmenthal), disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:61977CJ0106&from=DA

Acórdão de 29.01.08, processo C- 275/06 Productores de Música de España (Promusicae)/Telefónica de España SAU, ECLI:EU:C:2008:54, disponível em https://curia.europa.eu/juris/liste.jsf?language=en&num=C-275/06

Tribunal Constitucional

Acórdão no Processo n.º 828/2019, acórdão n.º 268/2022, Plenário, Relator Conselheiro Afonso Patrão, julgado em 04.2022, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html

Tribunal Europeu dos Direitos Humanos

Acórdão Application n.º 27798/95 - caso AMANN v. SWITZERLAND), disponível em https://hudoc.echr.coe.int/fre#{%22fulltext%22:[%22Amann%20v.%20Switzerland%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58497%22]}