

ENTRE A SAÚDE PÚBLICA E TUTELA DOS DADOS PESSOAIS EM SITUAÇÃO DE CRISE
PANDÉMICA: O CONTACT TRACING SEGUNDO O REGIME JURÍDICO DE DIREITO DA
UNIÃO EUROPEIA E DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

*BETWEEN PUBLIC HEALTH AND THE PROTECTION OF PERSONAL DATA IN A
SITUATION OF PANDEMIC CRISIS: CONTACT TRACING UNDER EUROPEAN UNION LAW
AND THE GENERAL DATA PROTECTION REGULATION*

Luís Manuel Pica^A

 <https://orcid.org/0000-0002-0470-5732>.

^A Doutorando em Ciências Jurídicas-Públicas na Escola de Direito da Universidade do Minho (Portugal). Docente no Instituto Politécnico de Beja (Portugal). Investigador no JusGov – Centro de Governação e Justiça da Escola de Direito da Universidade do Minho (Portugal)

Correspondência: luispica280@gmail.com

DOI: 10.12957/rfd.2022.51436

Artigo submetido em 01/06/2020 e aceito para publicação em 04/11/2022.

Resumo: O artigo discute as implicações jurídicas que derivam do fenómeno tecnológico denominado por “*contact tracing*”, o qual consiste numa técnica de rastreio através do tratamento massivo de dados pessoais de um grande volume de sujeitos. O objetivo é que este tratamento permita descobrir situações patológicas ligadas ao novo SARS-CoV2, adotando posteriormente um conjunto de ações que procuram mitigar os efeitos negativos deste vírus. Mas, contudo, levantam-se um conjunto de questões que merecem resposta, designadamente sobre a necessidade dos dados pessoais dos sujeitos, a sua legitimidade no tratamento e quais os limites dos poderes estaduais? Assim, quais os contextos de legitimidade e de necessidade de tratamento dos dados pessoais? Será que a necessidade dos dados pessoais pressupõe a ablação da tutela dos dados pessoais necessários ao controlo dos efeitos derivados do surto pandémico? Traçando o processo de tutela dos dados pessoais objeto de tratamento pelos Estados, a fim de dar cumprimento aos desideratos de prevenção e mitigação dos efeitos negativos despoletados pelo novo SARS-CoV2, será possível concluir pelo interesse público em detrimento dos interesses egoístas dos titulares dos dados pessoais? Ou será necessário adotar as medidas garantísticas consideradas suficientes e que não desconfigurem a posição central e matricial que o homem deve assumir num Estado baseado no respeito pela dignidade da pessoa humana? Procuraremos, com o presente artigo, dar resposta a estas questões enunciando a nossa posição e abordando as mesmas segundo uma visão europeia e atendendo ao quadro normativo de Direito da União Europeia e atendendo ao Regulamento Geral de Proteção de Dados, em vigor desde 2018 em todos os Estados-Membros e países, espaços ou territórios que tenham ligações com sujeitos residentes em qualquer dos Estados-Membros da União Europeia.

Palavras-chave: COVID-19. Tutela Dados Pessoais. Saúde Pública. *Contact tracing*.

Abstract: The article discusses the legal implications arising from the technological phenomenon known as "contact tracing", which consists of a tracking technique through the massive processing of personal data of a large volume of subjects. The aim is that this processing allows the discovery of pathological situations linked to the new SARS-CoV2, subsequently adopting a set of actions that seek to mitigate the negative effects of this virus. However, a set of questions arise that deserve an answer, namely about the need for the subjects' personal data, their legitimacy in the processing and what are the limits of state powers? Thus, what are the contexts of legitimacy and necessity of the processing of personal data? Does the necessity of the personal data presuppose the abrogation of the protection of personal data necessary to control the effects derived from the pandemic outbreak? Tracing the process of protection of personal data being processed by States in order to meet the desiderata of prevention and mitigation of the negative effects triggered by the new SARS-CoV2, is it possible to conclude that the public interest prevails over the selfish interests of the holders of personal data? Or is it necessary to adopt the guarantee measures considered sufficient and that do not disfigure the central and central position that man must assume in a State based on the respect for the dignity of the human being? With this article, we will try to answer these questions by stating our position and addressing them from a European perspective and taking into account the legal framework of European Union law and the General Data Protection Regulation, in force since 2018 in all Member States and countries, areas or territories that have links with subjects residing in any of the Member States of the European Union.

Keywords: COVID-19. Protection personal data. Public health. Contact tracing.

INTRODUÇÃO

A atual crise pandémica assolada pela irrupção do SARS-CoV2 comprometeu o panorama mundial até aqui conhecido, desenvolvendo importantes palpitações no quotidiano da sociedade moderna, nas relações sociais, económicas, políticas e também tecnológicas. Os alicerces da sociedade moderna e que, até há bem pouco tempo, pareciam quase inquebrantáveis foram colocados em crise, sofrendo profundas intrusões e restrições aos valores axiológicos estruturantes da mesma.

As dimensões apresentadas num contexto de crise pandémica irradiam a necessidade de adotar instrumentos, técnicas e metodologias que permitam dar cumprimento aos desideratos de bem-estar social e de salvaguarda pelos direitos fundamentais matriciais da sociedade. Entre as várias técnicas e metodologias adotadas, a utilização das novas tecnologias permite enfrentar este novo surto pandémico através de medidas de controlo e de mitigação dos efeitos negativos e nocivos para a sociedade.

Os benefícios que derivam da utilização das novas tecnologias resultam num combate eficiente a este vírus e à sua capacidade de propagação. Através do tratamento massivo dos dados pessoais e do seu cruzamento é possível um controlo sobre a atividade dos seus titulares, sobre a sua situação de saúde e sobre a sua movimentação geográfica, conseguindo um controlo e mitigação na propagação do vírus na sociedade, alertando os usuários de possíveis contatos com pessoas que tenham apresentado sintomas e tenham testado positivo para o novo SARS-CoV2. A utilização de aplicações de controlo de pessoas, designado por *contact tracing*, permite, assim, combater os efeitos negativos da propagação do vírus SARS-CoV2. Daí que, atentos aos benefícios trazidos pela utilização destas aplicações móveis, países como Singapura, Coreia do Sul ou China conseguiram um controlo férreo a este vírus e à sua propagação.

No entanto, qual o custo? Até que ponto a tutela dos dados pessoais envolvidos não é colocada em crise? Mostrar-se-á necessário face a interesses de saúde pública restringir direitos fundamentais como o direito à tutela dos dados pessoais?

A partir deste cenário, o presente estudo problematiza a estruturação jurídica da utilização massiva dos dados pessoais pelos Estados, especialmente quando os mesmos se mostram tão necessários perante o assolamento de um surto pandémico que suscita um conjunto de interrogantes complexas e pluridimensionais. Encaminhando esta problemática, não poderemos deixar de adotar uma metodologia matricial sobre os dados pessoais, pois são estes que se mostram como centrais na utilização destas técnicas inovadoras, mas que também suscitam a intervenção do Direito enquanto limite face a atuações autoritárias, abusivas e desproporcionais que possam colocar em evidência a democracia e os pilares da liberdade e da dignidade da pessoa humana.

O método fenomenológico baseado na utilização massiva destes dados pessoais mostra-se satisfatório ao desenlace deste trabalho, autorizando aquilo que muitas das vezes se dá como assumido numa sociedade. Com efeito, se os benefícios são muitos, os custos da democracia, da liberdade e dos direitos fundamentais dos cidadãos merecem que adotemos um estudo baseado no direito fundamental à tutela dos dados pessoais, passando pela adoção de uma análise ponderativa entre a necessidade dos mesmos e a necessidade de adotar mecanismos de proteção dos seus titulares. A abordagem qualitativa, a técnica ponderativa e os procedimentos analíticos procurarão ser transversais a todo o presente trabalho.

O DIREITO FUNDAMENTAL À TUTELA DOS DADOS PESSOAIS: UM BREVE ESBOÇO NORMATIVO

O direito à tutela dos dados pessoais expressa a sua proeminência como a potestade que cada um tem de controlar a informação que lhe diz respeito, decidindo todos os aspetos privados que lhe digam respeito e permitindo um controlo sobre as mesmas. Configurando-se como informações que permitem, diretamente ou indiretamente, identificar o seu titular - de tal modo que permitem associar determinado facto, característica ou traço a certa pessoa singular -, conhecendo aspetos da sua vida privada e reservada de forma acutilante e, por vezes, preocupante, acabou o direito (obrigatoriamente) por intervir na regulação desta realidade que se mostrava cada vez mais preocupante e *in crescendo* na sociedade moderna.

Foi devido ao aumento no fluxo de transferência de dados que os Estados, enquanto Estados de Direito Democráticos, viram-se obrigados a intervir na tutela destes, verificando-se com maior frequência a criação de legislação com vista à tutela dos dados e informações, que aqui se configuravam como os sujeitos mais frágeis e desprotegidos face aos grandes agentes que tratavam estas informações.

Indispensável a esta preocupação, a tutela dos dados pessoais das pessoas singulares sofreu, desde finais do século transato, uma notória evolução, quer por parte institucional, como a nível jurídico interno, internacional e comunitário. Foi nesta senda axiológica que, num panorama comunitário, encontramos o preceituado no artigo 8.º da Convenção Europeia dos Direitos do Homem, procurando-se, através da instituição de uma norma basilar para os direitos fundamentais da União Europeia, tutelar a vida privada e íntima das pessoas singulares e por ingerência a tutela dos dados pessoais que integram a esfera mais privada e restrita dos seus titulares (RITA AMARAL CABRAL, 1989). Também, a regulamentação normativa originária da União Europeia veio consagrar esta proteção, tendo sido instituído no artigo 16.º do Tratado de Funcionamento da União Europeia que “[t]odas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito”, criando-se, assim, condições de base à sua tutela. Neste sentido, posteriormente, foi o direito derivado da União Europeia que, na senda do já iniciado anteriormente, veio concretizar a tutela dos dados pessoais das pessoas singulares, nomeadamente com a aprovação da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, instrumento normativo que procurou harmonizar e criar mecanismos uniformes de proteção dos dados pessoais das pessoas singulares na União

Europeia, bem como instrumentos de circulação desses mesmos dados pessoais, fomentando, assim, a concretização do mercado interno (MANUEL MASSENO, 2016). Esta legislação comunitária, ao ser uma diretiva de natureza comunitária, careceu de ser transposta para os Estados-Membros da União Europeia, uma vez que não tinha aplicabilidade direta e imediata nestes. No caso do ordenamento jurídico português, esta transposição foi feita pela Lei n.º 67/98, de 26 de outubro de 1998, a qual aprovou a Lei de Proteção de Dados Pessoais. A Lei de Proteção de Dados Pessoais teve como principal desiderato a “proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados”. Para além disso, a Lei de Proteção de Dados Pessoais veio delimitar as formas de recolha, tratamento, transmissão, registo e conservação dos dados pessoais das pessoas singulares, bem como a criação da entidade independente que visa a fiscalização do cumprimento deste normativo legal (nomeadamente a Comissão Nacional de Proteção de Dados). Por último, recentemente, foi aprovado em 2016 o tão aclamado Regulamento Geral de Proteção de Dados, diploma legislativo que procurou uniformizar as legislações dos vários Estados-Membros em matéria de tutela dos dados pessoais e da sua circulação entre os Estados, procurando diminuir as assimetrias existentes nos vários Estados-Membros e as limitações existentes em matéria de livre circulação destes.

Este novo Regulamento Geral de Proteção de Dados foi o resultado de um longo processo que se pode situar, do ponto de vista institucional, no ano de 2010 quando o Conselho Europeu, juntamente com a Comissão Europeia, avaliou o funcionamento dos instrumentos aprovados e que se encontravam em vigor na União sobre a tutela dos dados pessoais, podendo, em caso de ser necessário, apresentar iniciativas com vista a colmatar as deficiências existentes (LUÍS PICA, 2018). Procurava-se, essencialmente, uniformizar e homogeneizar toda a regulamentação existente nos Estados-Membros, de forma que a livre circulação dos dados pessoais não sofresse quaisquer entraves e, num domínio funcional, que os direitos dos titulares dos dados pudessem ser idênticos ou o mais semelhante possível nos vários Estados-Membros e que os direitos sobre estes pudessem ser exercidos de forma uniforme.

Dessarte, é ponto assente que o instrumento comunitário utilizado procura, a título principal, a harmonização na regulamentação de uma matéria tão importante e sensível como são os dados pessoais das pessoas singulares, sendo esta regulamentação concretizada através de um diploma legislativo homogêneo entre os Estados-Membros, menos flexível e

mais rígido para estes, sendo contudo concedida pequenas prerrogativas de regulamentação para adotarem, dentro da sua legislação interna, as medidas legais que considerem convenientes aos interesses dos seus cidadãos e à concretização deste diploma comunitário. Assim, este novo Regulamento Geral de Proteção de Dados, apesar de ser quase na sua generalidade auto-exequível, carece de execução por parte dos Estados-Membros em alguns aspetos que o legislador comunitário considerou que deveriam ser estes a regulamentar. Como exemplo de essas matérias que cabem aos Estados-Membros regulamentar, encontramos as situações expressamente mencionadas nos artigos 8.º n.º1 *in fine*, ou no artigo 84.º, todas do Regulamento Geral de Proteção de Dados.

Por isso, e devido a esta necessidade, os Estados-Membros gozam de um conjunto de prerrogativas legais que podem ou devem ser concretizadas, de modo que, certos direitos e possibilidades, sejam devidamente exequíveis nos vários ordenamentos jurídicos. Como desenvolvimento desta imperatividade, em Portugal foi aprovada a Lei n.º 58/2019, de 8 de agosto, a qual assegurou a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

OS DADOS PESSOAIS EM SITUAÇÃO DE CRISE PANDÉMICA: A TUTELA OU A NECESSIDADE DE TRATAMENTO?

Como referimos, os dados pessoais - como largamente tem sido já adjectivamente por várias pessoas e sociedades - constituem o ouro do século XXI, pois a sua recolha e tratamento vislumbra-se como uma mais-valia no processo de tomada de decisões. Com efeito, veja-se que os dados pessoais surgem como o recurso mais valioso na economia atual, pois a sua utilização compreende uma infinidade de aplicações em diversos setores, tais como o setor bancário, financeiro, jurídico, médico, etc.. Porém, sobejamente se encontra assente que os dados pessoais se caracterizam como um importante reflexo da privacidade e da intimidade dos seus titulares, sendo que este direito fundamental veio mostrar-se positivado nos vários diplomas jurídicos a partir do século XIX e cuja relevância começou a ter corpo no século XVIII (SAMUEL WARREN, LOUIS BRANDEIS, 1890).

A ascensão das novas tecnologias e a fragmentação de informação e de dados pessoais materializados em dados informatizados, vieram assaltar a necessidade de invocar novos instrumentos de tutela que o direito fundamental de reserva da vida privada e íntima não conseguia, com os recursos que disponibilizava, dar resposta. Foi nesta senda axiológica que o direito à autodeterminação informativa e da tutela dos dados pessoais avocou-se como um direito *ex novo* que procurou dar resposta aos novos desígnios que vinham assaltar os titulares destes dados pessoais e que careciam de instrumentos próprios que lhes permitisse salvaguardar a sua situação jurídica (ANA ORTIZ, 2002; JURGEN SCHWABE, 2005)

O direito à autodeterminação informativa, *prima facie*, pode ser compreendido como o direito potestativo que outorga ao seu titular o poder de controlar os dados pessoais que lhe dizem respeito. Como advoga o *Tribunal Constitucional Federal Alemão no seu aresto de 15 de dezembro de 1983, BvR n.º209/83*, a autodeterminação individual pressupõe, porém – mesmo sob as condições da moderna tecnologia de processamento de informação –, que ao indivíduo está garantida a liberdade de decisão sobre ações a serem procedidas ou omitidas e, inclusive, a possibilidade de se comportar realmente conforme tal decisão. O livre desenvolvimento da personalidade pressupõe, sob as modernas condições do processamento de dados, a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais. Na mesma senda axiológica, o *Tribunal Constitucional português, no seu acórdão n.º 442/2007, de 11 de setembro*, procurou seguir a mesma orientação jurídica, afirmando que “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”.

Com o desiderato facultar resposta a esta necessidade, vários diplomas jurídicos se invocaram como direito positivo que pretendiam dar resposta aos desígnios *supra* referidos, sendo que aquele que merece maior destaque para efeitos do presente estudo, num contexto europeu, é o novo Regulamento Geral de Proteção de Dados Pessoais, aprovado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Mas também a legislação brasileira se mostrou bastante prolifera neste campo, tendo, inclusive, sido aprovada a Lei de Proteção de Dados Pessoais, através da Lei nº 13.709, de 14 de agosto de 2018, aguardando, contudo, início de vigência.

No que concerne à sua qualificação enquanto direito fundamental, vieram vários diplomas atribuir ao direito à autodeterminação informativa a natureza de direito fundamental, nomeadamente o artigo 8.º, n.º1 da Carta dos Direitos Fundamentais da União Europeia e o artigo 35.º da Constituição da República Portuguesa. Configurando-se insofismavelmente como um direito de natureza fundamental de nova geração, é necessário invocar todos os recursos disponíveis num Estado de Direito contra eventuais ingerências por parte de terceiros, incluindo o próprio Estado.

Os dados pessoais, mostrando-se como um recurso axiomáticamente imprescindível para vários domínios como também será o domínio da saúde e do controlo sanitário, acabam por assumir uma importância enaltecida no atual contexto pandémico, já que permitem a coleta de informação para a identificação da pessoa infetada com o novo COVID-19, bem como os locais onde o mesmo esteve geograficamente, permitindo uma correlação entre estes para determinar com quem esteve em contato e durante quanto tempo (BETHANIA ALMEIDA, DANILO DONEDA, MARIA YURY ICHIHARA¹, GUSTAVO MATTA, MANOEL BARRAL-NETTO, ELAINE RABELLO, FABIO GOUVEIA, MAURICIO L BARRETO, 2020).

Neste sentido, a Apple e a Google vieram recentemente declarar o desenvolvimento tecnológico de uma ferramenta de rastreamento ao novo SARS-CoV2, permitindo aos utilizadores dos sistemas iOS e Android a descarga de uma aplicação móvel em que são recolhidos um conjunto de dados pessoais da pessoa relativa à sua georreferenciação, à sua identificação e posteriormente se testaram positivo ao novo SARS-CoV2, notificando os utilizados da aplicação que tenham estado em contato com este último para efeitos de prevenção e de assessoria. Este método designado por *contact tracing* tem vindo a ganhar relevância no atual contexto pandémico, permitindo através do recurso aos sensores existentes nos dispositivos móveis e à estrutura de rede existentes, identificar pessoas que possam ter entrado em contato com outras que contraíram o novo SARS-CoV2. O *contact tracing* acaba por ter relevância no sentido que permite uma luta eficiente contra uma doença infecciosa, permitindo reduzir ou mesmo interromper a transmissão do vírus, já que alerta os usuários sobre possíveis contatos com a infeção e oferece uma assessoria preventiva ou atenção para oferecer um diagnóstico.

É neste contexto que os dados pessoais solicitados por via de diversas fontes suscitam grandes desafios e representam riscos para a segurança dos seus titulares, pois estes dados e informações permitem alcançar detalhadamente um conjunto de elementos que colocam

seriamente em causa a reserva da vida privada do seu titular, configurando-se um risco acrescido em caso de terceiros adquirirem ilicitamente esta informação. Contrariamente, também se assumem como o meio de

Primo, deve-se partir do contexto que, *in casu*, estamos perante dados pessoais de diversa natureza, concretamente dados pessoais de natureza simples, na aceção dada pelo artigo 4.º, n.º1 do Regulamento Geral de Proteção de Dados, e, também, dados de natureza sensível e catalogados como dados de saúde, na definição dada pelos artigos 4.º, n.º15 e 9.º também do Regulamento Geral de Proteção de Dados. Recorde-se que estando perante dados de natureza sensível, a tutela destes acaba por ser fortalecida comparativamente aos dados pessoais de natureza simples, uma vez que os dados relativos à saúde mostram-se gravemente lesivos se partilhados com terceiros alheios à esfera jurídica do titular dos dados pessoais, sem o prévio consentimento deste.

Secundo, devemos trazer à colação que este direito fundamental não se pode mostrar ilimitado e rígido face à sua articulação com os demais direitos fundamentais do sistema jurídico, isto é, poderão sempre ser restringidos caso exista necessidade imperativa superior que legitime esta limitação (*v.g.* interesses do Estado ou do próprio titular dos dados). Alguns reflexos deste carácter limitado que se encontra subjacente a este direito, encontra-se plasmado logo nos artigos 6.º, n.º1 alínea e) e 9.º, n.º2 alínea g) do Regulamento Geral de Proteção de Dados, o qual consagra que o tratamento dos dados pessoais apenas é lícito se o tratamento for necessário por motivos de interesse público, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados.

Deste importante trecho normativo, denota-se importantes aspetos materiais que devem aqui ser devidamente mencionados. A primeira premissa revela-se na necessidade entre o interesse público, o qual deve estar legitimado pelas normas da União Europeia ou do Estado-Membro; em segundo lugar, o tratamento dos dados pessoais apenas deve ocorrer de modo estritamente proporcional e quando mostre necessário e adequado à salvaguarda do interesse a salvaguardar. Invocam-se assim os princípios plasmados no artigo 5.º do Regulamento Geral de Proteção de Dados, nomeadamente o da minimização dos dados pessoais e da finalidade.

Contudo, esta restrição ao prévio consentimento apenas legitima determinada entidade, *in casu* o Estado, a recolher e tratar os dados pessoais relativos à saúde do seu titular para determinada finalidade concreta. Tal permissão legislativa não legitima o Estado a revelar a informação a terceiros, não sendo este trecho legislativo legitimador de revelação dos dados a entidades terceiras alheias às finalidades visadas. Pelo contrário, deve-se enfatizar que esta permissão de revelação a terceiros, em determinadas situações, não poderia ser concedida pelo Regulamento Geral de Proteção de Dados, pois se o objeto deste diploma legislativo é concretamente a tutela dos dados pessoais, dotar o responsável pelo tratamento ou algum terceiro da legitimidade de revelar a informação e os dados a qualquer terceiro, seria este contrário aos desígnios prosseguidos por este diploma jurídico. Esta possibilidade, unicamente poderá ser invocada por via do instrumento previsto na Constituição da República Portuguesa, nomeadamente o instrumento de articulação e de restrição de direitos fundamentais quando os mesmos, numa determinada situação concreta, estejam em colisão.

A solução para a colisão entre direitos fundamentais deve passar pela harmonização equitativa entre ambos, a qual apenas pode ser concretizada através da restrição proporcional de algum destes, ou de ambos de forma equitativa, a qual apenas poderá ser feita na medida adequada ao fim que se pretende atingir, tendo como desiderato a prossecução do interesse estadual quando seja estritamente necessário e na medida proporcional (VITAL MOREIRA E GOMES CANOTILHO, 2006). Haverá assim que, para exercício do poder ablativo dos direitos fundamentais, preencher as três vertentes conhecidas, nomeadamente a adequação da restrição ao fim que se pretende atingir, a indispensabilidade da restrição relativamente ao desiderato a concretizar e a sua adequação a este mesmo fim, e, por último, a racionalidade do teor da restrição imposta (BACELAR GOUVEIA, 2001)

Para efeitos de publicitação de dados pessoais de pessoas em contexto de pandemia facilmente se poderia invocar a existência de um direito de saúde pública, o qual encontra consagração normativa no artigo 64.º da Constituição da República Portuguesa, ou ainda o direito à saúde e ao bem-estar previsto no artigo 25.º da Declaração Universal dos Direitos do Homem. Porém, a mera existência de um direito fundamental que entre em aparente conflito com o direito à tutela dos dados pessoais não legitima, *per si*, a restrição deste para efetivação do primeiro. Afirmar tal possibilidade seria contrariar o referido *supra* quanto ao preenchimento dos princípios da adequação, da proporcionalidade *stricto sensu* e da necessidade.

Questão que nos assalta relaciona-se em descortinar se a restrição do direito fundamental da tutela aos dados pessoais se mostra adequado e necessário aos desideratos de concretização de saúde pública e, em caso afirmativo, em que moldes deveria o mesmo ser restringido de modo a não se verificar discricionário e desproporcional, nomeadamente quanto à utilização de uma aplicação para dispositivo móvel que recolha e trate os dados pessoais do seu titular de modo a verificar e prevenir o possível contágio do vírus a terceiros. Na nossa humilde opinião e *data venia*, somos em crer que esta restrição se mostrará adequada e necessária aos fins pretendidos, contudo não na extremidade de restringir e revelar informação sensível a terceiros. Assim, somos em crer que sempre e quando seja executado de modo a alcançar certos limites que não poderão, aqui, ser extravasados sob pena de ofendermos gravemente os direitos dos titulares dos dados pessoais e afastar a possibilidade de tal restrição.

Em termos substantivos, a premissa da adequação e necessidade, mostrar-se-á cumprida, já que as medidas de confinamento se mostram de difícil implementação na sociedade e nem sempre aceites politicamente em todos os Estados, pelo que a medida que parece apontar-se mais adequada será a implementação de uma aplicação que controle certos aspetos do seu utilizador e para efeitos de prevenção de terceiros. Por último, a implementação desta medida apenas se legitima se não se ultrapassarem certos limites, nomeadamente a revelação do titular dos dados pessoais a terceiros, bem como a desnecessidade de armazenamento em grandes bases de dados que poderão colocar em sérios riscos os titulares dos dados armazenados. Deste modo, a revelação da informação apenas se encontraria legitimada se expurgada de identificadores que permitam, de alguma forma, relacionar a informação ao seu titular.

Dessarte, não se mostrando a revelação dos dados pessoais como um quesito a colocar em equação, não poderemos falar numa verdadeira restrição do direito fundamental à tutela dos dados pessoais vertido no artigo 35.º da Constituição da República Portuguesa, mas sim à faculdade prevista pelo legislador no artigo 9.º, n.º1 alíneas g) e i) do Regulamento Geral de Proteção de Dados. Veja-se, também, que se não houver forma de identificação do seu titular, acabamos por enquadrar a informação e os dados pessoais na categoria de “dados anonimizados” e, portanto, fora da alçada de tutela do Regulamento Geral de Proteção de Dados, pelo que a revelação dos dados apenas poderia ser feita se não houver forma de identificar o seu titular.

Em suma, poderemos assim que dizer que, *primo*, estamos perante situação em que o Estado poderá tratar as informações e os dados sensíveis ao estado de saúde do seu titular estando este legitimado a tratar as informações mencionadas, conforme o preceituado no artigo 9.º, n.º1 alíneas g) e i) do Regulamento Geral de Proteção de Dados. O fundamento que reside nesta permissão legal será a invocação do direito de saúde pública previsto no artigo 65.º da Constituição da República Portuguesa, permitindo, assim, o tratamento dos dados pessoais sem se mostrar necessário o prévio consentimento do seu titular. Porém, apesar desta permissão legislativa, não isenta o responsável pelo seu tratamento dos demais deveres que sobre este impende, nomeadamente os deveres de informação previstos nos artigos 13.º e seguintes do Regulamento Geral de Proteção de Dados. *Secundo*, estando o Estado, ou a entidade de saúde competente, legitimada à recolha e ao tratamento dos dados pessoais, esta permissão não se mostra, como consagra expressamente a norma legitimadora, ilimitada e discricionária, pautando um conjunto de requisitos que se mostram imperativos cumprir. Como refere o citado preceito legal, o tratamento dos dados pessoais de natureza sensível quanto legitimados num interesse superior da coletividade deve mostrar-se proporcional ao objetivo visado, ou seja, apenas se encontra possível o tratamento dos dados pessoais que se mostrem adequados e na medida do necessário para a prossecução do desiderato prosseguido; estando legitimado o tratamento dos dados pessoais de natureza sensível na medida do estritamente proporcional, devem ser consagradas medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados, nomeadamente em matéria de confidencialidade e de segurança das informações tratadas.

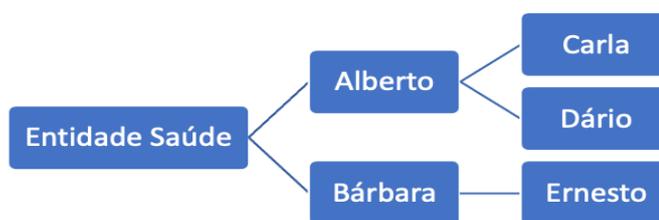
Por tudo o mencionado, se deve afirmar que em conjunturas de hercúlea necessidade, como é a atual necessidade de zelo pela saúde pública e pela sua salvaguarda, o tratamento dos dados pessoais, quer de natureza simples ou de natureza sensível, se encontram legitimados para concretização dos desideratos de conservação destes direitos fundamentais, não carecendo do consentimento do titular dos dados para que o seu tratamento seja lícito. Contudo, restringindo-se havendo uma certa limitação a uma componente importante do direito à tutela dos dados pessoais e da autodeterminação informativa, deve o legislador consagrar medidas que se mostrem adequadas e proporcionais a compensar esta restrição, procurando instituir mecanismos de proteção sobre os dados pessoais tratados e a instrumentos que permitam a sua segurança face à intromissão de terceiros não autorizados.

O TRATAMENTO DOS DADOS PESSOAIS ATRAVÉS DA UTILIZAÇÃO DE APLICAÇÕES MÓVEIS PARA CONTROLO DA PANDEMIA

No atual contexto pandêmico que tem vindo a assolar o planeta, várias tem sido as medidas instituídas pelos vários governos com o fim de controlar e mitigar a propagação do vírus, indo desde as medidas de confinamento até medidas de controlo eletrónico.

Vários Estados e países têm vindo, como uma importante medida de controlo de propagação do vírus, a instituir medidas eletrónicas, nomeadamente através da utilização de uma aplicação móvel, as quais permitem uma fiscalização geográfica do utilizador desta e um controlo no contato com outros utilizadores, o qual irá permitir que em caso de alguém, com contato prévio ao utilizador da aplicação, ficar infetado pelo novo COVID-19, seja o utilizador notificado da possibilidade de contágio em virtude do contato com alguém já infetado.

Esquemáticamente:



Em caso de o utilizador da aplicação Alberto, que esteve em contato com o Carla e Dário, vir estar infetado com o novo COVID-19, aplicação da entidade de saúde notificará estes dois do contato com alguém que se encontra atualmente com teste positivo, pelo que haverá uma certa probabilidade de estes vir a estar também infetados. Contudo, Bárbara e Ernesto que nunca tiveram contato com nenhum dos utilizados mencionados, nunca receberão nem terão conhecimento dos demais infetados.

A existência de uma aplicação móvel deste tipo, coloca *ab initio* uma questão que nos assalta e que merece aqui uma resposta, nomeadamente se a mesma deve impor-se como obrigatória por parte dos governos dos Estados afetados pela pandemia ou se, pelo contrário, a mesma deverá pressupor a voluntariedade dos cidadãos.

Conforme referimos *supra*, o tratamento dos dados pessoais encontra-se aqui legitimado com a invocação no interesse público da coletividade e com o desiderato de

manutenção da saúde pública, podendo o Estado ou a entidade de saúde competente pela gestão da aplicação de controlo da pandemia recolher e tratar os dados pessoais dos utilizadores mesmo sem o prévio consentimento destes. Contudo, esta recolha e tratamento deve encontrar subjacente importantes medidas de tutela, nomeadamente a obrigatoriedade de o responsável pelo tratamento dos dados pessoais informar dos direitos que o seu titular destes goza e de como os poderá exercer, bem como deverão encontrar-se salvaguardados a confidencialidade e segurança dos dados recolhidos e tratados, sob pena de importante e graves omissões por parte do responsável pelo tratamento dos dados pessoais. Neste aspeto será importante referir que não se mostrará adequado e necessário o armazenamento da informação tratada e guardada durante grandes períodos, ou seja, dever-se-á unicamente zelar pelo tratamento dos dados pessoais e guardá-los pelo tempo estritamente necessário à realização dos fins visados, *in casu*, 14 dias, devendo posteriormente proceder-se ao seu apagamento completo e sem qualquer registo dos mesmos.

Porém, estando os dados pessoais tratados de forma lícita sempre que se mostrem necessários à salvaguarda de direitos fundamentais como é o direito à saúde pública, encontrar-se-á mais idóneo para os Estados obter o consentimento prévio do titular dos dados, evitando-se, assim, redundâncias e medidas justificativas que poderão protelar um conjunto de conflitos entre as respetivas autoridades de controlo (*in casu* a Comissão Nacional de Proteção de Dados), as instituições europeias e, principalmente, o titular dos dados pessoais. Por este motivo, tem-se debatido nos vários Estados que as aplicações para controlo da pandemia devem residir no caráter voluntário das mesmas, beneficiando das suas potencialidades unicamente as pessoas que assim o desejem e apelando os governos à sua utilização voluntária para cumprimento de um interesse comum.

Por este motivo, não estamos perante aquelas situações em que são divulgadas informações sobre o estado de saúde de determinada pessoa individualizada e concreta, unicamente sobre a existência de uma pessoa que veio contrair esta nova doença e que cumulativamente este em contato durante um certo lapso temporal com o utilizar da aplicação móvel. A divulgação desta informação à pessoa que esteve em contato com a pessoa agora infetada não coloca complexificações jurídica, pois estaremos no campo dos denominados dados anonimizados, os quais acabam por ser expurgados de todos os identificadores que permitem, direta ou indiretamente, associar os dados aos seus titulares (MANUEL DAVID MASSENO, 2019). Referindo-nos a dados anonimizados, acabarão estes

por se encontrar excluídos dos princípios gerais da proteção de dados vertidos no RGPD, não carecendo, assim, de tutela por parte deste diploma.

Dessarte, invoca-se como uma das medidas mais adequadas em face do controlo da pandemia e de mitigação da sua expansão, pois a comunicação de dados anonimizados que apenas indiquem que determinado usuário com quem o utilizador da aplicação esteve recentemente em contato se encontre infetado com o novo COVID-19, não pressupõe a comunicação de dados pessoais sujeitos a tutela, mas sim de dados anonimizados. Assim, devemos realçar a desnecessidade de comunicação de dados identificáveis a terceiros, uma vez que não se mostram adequados e necessários aos fins visados.

Por último, em função desta medida adotada, deve-se afirmar-se que deverá o responsável pelo tratamento dos dados pessoais zelar pela confidencialidade dos mesmos, impedindo o acesso ilegítimo por terceiros alheios a esta relação jurídica, bem como a instituição de fortes medidas de segurança sobre a aplicação criada que impeçam o furto de informação que se encontrem tratados por parte da entidade responsável pelo tratamento dos dados e pela manutenção da aplicação móvel. Em caso de se mostrar tecnicamente possível e à luz do princípio da adequação, mostrar-se-ia idóneo que os dados pessoais tratados não fossem armazenados em bases de dados.

CONCLUSÃO

Configurando-se os dados pessoais como um importante objeto de combate à pandemia declarada pela Organização Mundial de Saúde, torna-se axiomático que a utilização destes através da partilha de informação de georreferenciação de pessoas infetadas com o novo COVID-19 e que tenham estado em contato com outros utilizadores, permitem um controlo férreo e bastante eficiente na mitigação da propagação do vírus.

Porém, o tratamento de um grande número de dados e de natureza diversa acarreta uma grande complexificação de questões jurídicas que merecem aqui destaque e que assumem uma importância inegável para os Estados modernos. É neste sentido que o tratamento sem o consentimento pode surgir para invocação de um superior interesse da coletividade como é o direito à saúde pública e à sua salvaguarda, bem como os instrumentos que devem ser adequados a este tratamento sem prévio consentimento.

Contudo, a restrição parcial ao direito à autodeterminação informativa, nomeadamente no que diz respeito ao tratamento apenas quando legitimado pelo titular dos dados, acaba por obrigar o responsável pelo tratamento a adotar mecanismos de salvaguarda destes dados e instrumentos de segurança que se mostrem idóneos a proteção dos dados pessoais objeto de tratamento.

REFERÊNCIAS BIBLIOGRÁFICAS

HERRÁN ORTIZ, Ana Isabel. El Derecho a la protección de datos personales en la sociedad de la información. *Cuadernos Desto De Derechos Humanos*, N.º26, Universidad de Bilbao, 2002.

ALMEIDA, Bethania; DONEDA, Danilo; ICHIHARA, Maria Yury; MATTA, Gustavo; BARRAL-NETTO, Manoel; RABELLO, Elaine; GOUVEIA, Fabio; BARRETO, Mauricio. Personal data usage and privacy considerations in the COVID-19 global pandemic. *SciELO - Scientific Electronic Library Online*, 2020.

GOUVEIA, Jorge Bacelar. Regulação e limites dos direitos fundamentais. *Dicionário Jurídico da Administração Pública*, 2º suplemento, Lisboa, 2001.

ANDRADE, José Carlos Vieira de. *Os Direitos Fundamentais na Constituição de 1976*, 4ª Edição, Almedina, 2009.

SCHWABE, Jürgen. *Fünfzig Jahre Des Deutschen Bundesverfassungsgerichts Rechtswissenschaft*, Konrad-Adenauer-Stiftung E. V., Berlim, 2005.

CANOTILHO, J.J. Gomes; MOREIRA, Moreira. *Constituição da República Portuguesa Anotada Vol. I*, Coimbra Editora, 2006.

PICA, Luís. As Avaliações De Impacto, O Encarregado de Dados Pessoais e a Certificação no Novo Regulamento Europeu de Proteção de Dados Pessoais. *Revista Científica Sobre Cyberlaw do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa*. *Revista nº 5 | MARÇO 2018*, Lisboa, 2018.

MASSENO, Manuel David. *O novo Regulamento Geral sobre proteção de dados pessoais da União Europeia*, 8º Congresso de Direito de Informática e Telecomunicações, setembro 2016.

MASSENO, Manuel David. “Da anonimização, pseudonimização e cifragem em tempos de 'Big Data' [no âmbito do Regulamento Geral sobre Proteção de Dados]”, *in Conferência Regulamento Geral de Proteção de Dados. Um ano depois*, 2019. Disponível em [https://www.academia.edu/39249969/Da_anonimiza%C3%A7%C3%A3o_pseudonimiza%C3%A7%C3%A3o_e_cifragem_em_tempos_de_Big_Data_no_ambito_do_Regulamento_Geral_sobre_Prote%C3%A7%C3%A3o_de_Dados](https://www.academia.edu/39249969/Da_anonimiza%C3%A7%C3%A3o_pseudonimiza%C3%A7%C3%A3o_e_cifragem_em_tempos_de_Big_Data_no_%C3%A2mbito_do_Regulamento_Geral_sobre_Prote%C3%A7%C3%A3o_de_Dados). Acesso em: jun.2020.

CABRAL, Rital Amaral. O Direito à Intimidade da Vida Privada. *Estudos em Memória do Prof. Doutor Paulo Cunha*, Lisboa, 1989.

WARREN, Samuel; BRANDEIS, Louis. The Right of Privacy. *Harvard Law Review* - Vol.IV, December, n.º5, 1890. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: mai.2020.