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

Patrícia Cardoso Dias ([1])

Sumário: 1. Considerações iniciais: Proteção multinível do direito à privacidade e à proteção de dados pessoais; 2. Do estado de epidemia a pandemia – Emergência de uma situação de saúde pública global; 3. Operações de tratamento de dados pessoais no contexto do controlo sanitário de propagação do contágio; 4. Tratamento de dados por motivos de interesse público no domínio da saúde pública: a ameaça transfronteiriça grave para a saúde; 4.1. Vigilância epidemiológica e alerta rápido de ameaças graves para a saúde; 4.2. Operações de tratamento de dados pessoais de saúde pela autoridade de saúde nacional; 4.3. Utilização de aplicações digitais para controlo sanitário da transmissão do SARS-COV-2; 4.3.1. Considerações éticas sobre sistemas digitais de rastreio de proximidade; 4.3.2. STAYWAY COVID: uma app instrumental a uma estratégia global de interrupção das cadeias de contágio; 5. Considerações finais.

[1] Professora convidada na Universidade Autónoma de Lisboa "Luís de Camões", doutoranda e Mestre em Direito pela Universidade Autónoma de Lisboa "Luís de Camões". padias@autonoma.pt. Um agradecimento especial à Senhora Professora Doutora Ana Roque pelo magistral rigor que a caracteriza nas suas valorosas contribuições para os meus trabalhos, em particular, no domínio da proteção de dados pessoais.

Resumo: no contexto do surto provocado pelo novo coronavírus, responsável pela infeção respiratória aguda designada COVID-19, ganharam expressão de valor reforçado diversas soluções tecnológicas com a precípua finalidade de auxiliar o controlo sanitário de transmissão do SARS-COV-2. As soluções tecnológicas, promotoras de benefícios para a salvaguarda dos valores superlativos da saúde pública e da saúde individual, não subjazem sem o tratamento de dados pessoais *stricto sensu*, e bem assim de dados pessoais de saúde (particularmente sensíveis), o que se pode observar por força do cumprimento de obrigações legais a que autoridades nacionais se encontrem sujeitas, mas de igual forma por razões de interesse público, tal como é o caso de patologias/doenças ou quaisquer outras ameaças à saúde que, de igual forma, se encontram amparadas em diversos dispositivos legais. Há, assim, que ter presente que a disciplina legal orientada para a proteção da saúde pública e individual, bem como a relativa à vigilância epidemiológica não produzem efeitos isoladamente, tendo necessariamente de ser apreciadas conjugadamente com a disciplina legal relativa à proteção de dados pessoais. No contexto de um dever geral de recolhimento e isolamento social, simultâneo com a necessária promoção das atividades económicas, a progressiva transição para uma "nova normalidade", impôs que diversas entidades implementassem medidas tendentes a prevenir e mitigar o contágio (*v.g.*, organização do espaço de trabalho ou dos espaços de utilização pública, aquisição de soluções alcoólicas de desinfeção, reforço dos serviços de limpeza e higienização), mas sobretudo ganharam particular relevância as que suportam aquela função em ecossistemas de partilha de dados através de soluções digitais que constituem marcadores de contato da infeção provocada pelo SARS-COV-2. Ora, estas operações implicam o tratamento de diversas categorias de dados pessoais, suscitando particulares cautelas os dados pessoais de saúde, não apenas por respeitarem diretamente a uma pessoa singular identificada ou identificável, mas em virtude da particular sensibilidade desta categoria de dado que enforma o reduto último da privacidade, estando por isso sujeita a um regime jurídico reforçado de proteção. Resulta do próprio princípio da proporcionalidade, adequação e necessidade, que a informação de saúde apenas pode ser objeto de tratamento na medida em que o direito europeu e nacional o permita, e assim sempre em conformidade com a legislação específica. Com efeito, atendendo à natureza do dado, revelador de aspetos de vida privada que pode potenciar a discriminação, o estado de exceção, em sentido estrito e em sentido lato, não pode *per se* legitimar a adoção de quaisquer medidas preventivas e de vigilância epidemiológica. Por conseguinte, a implementação de soluções tecnológicas com estas finalidades, seja sob égide das competências atribuídas às autoridades de saúde ou enquanto mecanismos de autorresponsabilização e auto monitorização, tem necessariamente de ser ponderada com o direito fundamental à privacidade e à proteção de dados pessoais.

Palavras-chave: privacidade; dados pessoais de saúde; saúde pública; novas tecnologias.

1. Considerações iniciais: proteção multinível do direito à privacidade e à proteção de dados pessoais

Importa distinguir o que verdadeiramente se tutela no contexto do recurso às novas tecnologias para efeitos de combate ao surto de COVID-19, a saber, o direito à reserva sobre a intimidade da vida privada e privacidade e o direito à proteção de dados pessoais que, pese embora se encontrem intrinsecamente ligados, são direitos distintos.

O direito à privacidade é reconhecido no artigo 8.º da Convenção Europeia dos Direitos Humanos (CEDH de 1950)[2] e no artigo 12.º da Declaração Universal dos Direitos Humanos (DHDH de 1948)[3] como direito humano fundamental sob a tutela do direito à reserva sobre a intimidade da vida privada.

Nestes artigos são repudiadas, através de proibições, quaisquer ingerências dos poderes públicos no exercício do direito ao respeito pela vida privada, salvo quando a respetiva ingerência se encontre prevista em lei e seja necessária no contexto de uma sociedade democrática, designadamente, para proteção de interesses coletivos relevantes e, no que neste contexto particularmente importa, a proteção da saúde[4].

Estes instrumentos foram, conforme é consabido, adotados anteriormente à utilização generalizada dos computadores, internet e dos assinaláveis progressos tecnológicas que, se por um lado apresentam enormes vantagens, por outro lado

[2] «Artigo 8.º da CEDH – Direito ao respeito pela vida privada e familiar 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros». Convenção Europeia dos Direitos do Homem (https://www.echr.coe.int/Documents/Convention_POR.pdf) acesso em 2020-07-26.

[3] «Artigo 12.º da DUDH – Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques». Cfr. Declaração Universal dos Direitos Humanos (https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf) acesso em 2020-07-26.

[4] A proteção da saúde encontra-se apenas prevista na parte final do artigo 8.º da CHDH.

aumentam consideravelmente os riscos para o âmbito de proteção do direito à reserva sobre a intimidade da vida privada.

Estes riscos foram potenciados pela globalização digital e intrínseca inexistência de fronteiras, e justificaram a autonomização do direito à proteção de dados pessoais, cujo bem jurídico tutelado é a privacidade na sua dimensão de direito à autodeterminação informacional, atenta a utilização da informação pessoal que, em última instância, sempre deverá servir a pessoa humana e não, apenas, os interesses das organizações (públicas ou privadas).

Com efeito, o direito à reserva sobre a intimidade da privada e o direito à proteção de dados pessoais distinguem-se na sua formulação e alcance porquanto o primeiro consiste numa proibição genérica de ingerência que apenas poderá ser legitimada por critérios de interesse geral superior (sempre sujeitos a ponderação)[5], e o segundo num mecanismo de segurança e proteção para o titular dos dados sempre que estes sejam objeto de tratamento, considerando-se um direito moderno e dinâmico[6].

Por conseguinte, trata-se de um direito sempre convocado no âmbito de qualquer operação de tratamento de dados pessoais, com um alcance naturalmente mais amplo que o direito à reserva sobre a intimidade da vida privada, projetando-se a tutela relativamente a todas as operações e categorias de dados pessoais tratados independentemente da relação que se estabelece com a privacidade e impactos que

[5]«El derecho a la privacidad se refiere a situaciones en las que se ha visto lesionado un interés particular o «la vida privada» de una persona. (...) el concepto de «vida privada» ha tenido una interpretación amplia en la jurisprudencia en el sentido de que se aplica a situaciones íntimas, información sensible o confidencial, información que podría perjudicar la percepción de la ciudadanía respecto de una persona e incluso aspectos de la propia vida profesional y conducta pública. Sin embargo, la determinación de si existe o ha existido (o no) una injerencia en la «vida privada» depende del contexto y de los hechos de cada caso». Cfr. Agencia de los Derechos Fundamentales de la Unión Europea, Manual de legislación europea en materia de protección de datos, Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2019. P. 23.

[6] Conclusões da Advogada Geral Eleanor Sharpston no âmbito dos processos C-92/09 e C-93/09, articulado n.º 71. (http://curia.europa.eu/juris/document/document.jsf?text=&docid=80291&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=11269075), acesso em 2020-07-10.

nesta se observem (que variam na sua maior ou menor dimensão de gravidade em função da natureza ou categoria de dado tratado)[7].

Em bom rigor, quando se convoca a privacidade neste contexto, chama-se à colação um regime jurídico de tutela específico para a informação pessoal – excluindo por isso a liberdade pessoal de conduzir a própria vida, a proteção da honra, bom nome e reputação ou a identidade pessoal – que se traduz numa faculdade de controlo sobre a mesma e que exige uma tutela alargada e por isso mais ampla que a mera exclusão de terceiros a uma esfera de segredo.

Assim, acompanhando de perto Paulo Mota Pinto, «(...) poderíamos dizer que esse interesse é o de evitar ou de controlar a tomada de conhecimento ou a revelação de *informação pessoal.* (...) O interesse do indivíduo na sua privacidade, isto é, em subtrair-se à atenção dos outros em impedir o acesso a si próprio ou em obstar à tomada de conhecimento ou à divulgação de informação pessoal (interesses estes que resumindo, poderíamos dizer serem os interesses em *evitar a intromissão* dos outros na esfera privada e em impedir *a revelação* de informação pertencente a esta esfera (...)»[8].

Esta proteção foi progressivamente consolidada por via de um percurso temporal substantivo e assume contemporaneamente a necessidade de uma disciplina uniforme de forma a garantir um elevado nível de proteção às pessoas singulares, não apenas à escala regional, mas de igual forma à escala internacional.

---

[7] «El tratamiento de datos personales también puede violar el derecho a la vida privada (...) Sin embargo, no es necesario demonstrar una violación de la vida privada para que se apliquen las normas de protección de datos. (...) Por el contrario, cualquier operación que implique el tratamiento de datos personales podría entrar en el ámbito de aplicación de la normativa de protección de datos y dar lugar a que se aplique el derecho a la protección de los datos personales. Por ejemplo, cuando una empresa registre información relativa a los nombres de sus empleados y a la remuneración que reciban, el mero registro de esta información no podrá considerarse injerencia en su vida privada. Sin embargo, sí podría alegarse que existe tal injerencia, por ejemplo, en el caso de que el empresario comunicase información personal de los empleados a terceros. En cualquier caso, los empresarios deben cumplir la normativa de protección de datos, puesto que el registro de información de los empleados constituye tratamiento de datos». Cfr. Agencia de los Derechos Fundamentales de la Unión Europea, (nota 5), p. 22-23.

[8] Pinto, Paulo Mota, Direitos de Personalidade e Direitos Fundamentais – Estudos, Coimbra: GestLegal, 2018, p. 506-507.

Os avanços tecnológicos impulsionaram assim a adoção da Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108 do Conselho da Europa) em 1981 – recentemente modernizada com a adoção do Protocolo de Modificação CETS n.º 223 a 18 de abril de 2018[9] – que permanece até à atualidade como único instrumento internacional juridicamente vinculante no âmbito da proteção de dados pessoais (para todos os Estados signatários e que a tenham ratificado regularmente), encontrando-se disponível para adesão por países terceiros – aderiram à Convenção 108 todos os Estados Membros do Conselho da Europa (47) e mais 9 Estados que não integram o Conselho da Europa[10].

O direito à proteção de dados pessoais encontra-se expressamente reconhecido no artigo 8.º da Carta Europeia dos Direitos Fundamentais (CEDF)[11] como direito fundamental, elevando o seu conteúdo de proteção ao âmbito do direito primário[12] da União Europeia, adquirindo expressão de desenvolvimento no artigo 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE)[13] integrado no capítulo relativo aos princípios gerais da União Europeia.

---

[9] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data as it will be amended by its Protocol CETS N.º 223 (https://rm.coe.int/16808ade9d), acesso em 2020-07-12.

[10] COUNCIL of Europe Portal, Chart of signatures and ratifications of Treaty 108 - Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data Status as of 14/07/2020 (https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=LjCeqKNC), acesso em 2020-07-14.

[11] «Artigo 8.º Proteção de dados pessoais 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente». Cfr. Carta dos Direitos Fundamentais da União Europeia (https://www.europarl.europa.eu/charter/pdf/text_pt.pdf) acesso em 2020-07-08.

[12] O Direito da União compreende o direito primário e direito secundário ou derivado. É direito primário da União os Tratados (Tratado da União Europeia e Tratado sobre o Funcionamento da União Europeia) e direito secundário ou derivado os atos jurídicos especificados no artigo 288.º do TFUE, designadamente, os regulamentos, diretivas e decisões da União Europeia que tenham sido adotas pelas instituições da União de acordo com o princípio das competências atribuídas nos Tratados.

[13] «Artigo 16.º (ex-artigo 286.º TCE) 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. O Parlamento Europeu e o Conselho, deliberando de acordo com o

O artigo 16.º do TFUE é, nos termos do mesmo constante, a base jurídica de adoção do pacote de reformas da disciplina legal em matéria de proteção de dados que se operou em 2016[14], designadamente, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revogou a Diretiva 95/46/CE (RGPD.

Tratando-se de um regulamento entrou em vigor, simultaneamente, em todos os Estados Membros da União Europeia no dia 25 de maio de 2016, sem necessidade de transposição para o direito interno, impondo uma disciplina uniformizada entre os vários Estados Membros que se pretendia verificada em maio de 2018, data em que terminou o período transitório de dois anos para que as organizações se colocassem em conformidade com as novas[15] obrigações.

Grande parte do conteúdo constante do Regulamento era já objeto de previsão na Diretiva 95/46/CE, que havia sido transposta com diferenças significativas para o direito nacional dos Estados Membros, ao que acrescia as diferenças assinaláveis de atuação das autoridades de controlo nos termos previstos na legislação interna, o que justificava o nível de proteção diferenciado que era observável até à adoção deste ato jurídico.

processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes. As normas adotadas com base no presente artigo não prejudicam as normas específicas previstas no artigo 39.º do Tratado da União Europeia». Cfr. Tratado sobre o Funcionamento da União Europeia, (https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A12012E%2FTXT), acesso em 2020-07-31.

[14] A modernização da legislação europeia em proteção de dados pessoais incluiu a adoção da Diretiva 2016/680 e do Regulamento (UE) 2018/1725.

[15] Novas em sentido restrito porquanto a maior parte do conteúdo substantivo do Regulamento (UE) 2016/679 já se encontrava amplamente previsto da Diretiva 95/46/CE.

2. Do estado de epidemia a pandemia – emergência de uma situação de saúde pública global

O incidente de um surto de infeção provado por um novo vírus da família dos *coronaviridae*, inicialmente identificado na província de Hubei na China, rapidamente evoluiu de uma situação epidémica para a declaração do estado de pandemia pela Organização Mundial de Saúde[16].

Conforme se pode observar, com uma incidência geográfica delimitada de início, rapidamente evoluiu para a propagação de uma infeção global, determinando a emergência de uma situação de saúde pública universal[17] [18], que impõe uma resposta de amplitude igualmente globalizada.

A sociedade hodierna, caraterizada pela rápida circulação de pessoas e bens, mas sobretudo pela acentuada dinâmica de mobilidade das pessoas, contribuiu para a célere propagação da doença sem que houvesse tempo, circunstâncias e modo para

[16] No dia 31 de dezembro de 2019 a Comissão Municipal de Saúde de Wuhan reportou a verificação de 27 casos de pneumonia de etiologia desconhecida, identificando como principal foco de contágio o mercado municipal de Wuhan, tendo reportado a identificação de um novo coronavírus (SARS-COV-2), responsável pela doença respiratória aguda designada COVID-19, vírus introduzido em humanos por transferência de espécie. Os primeiros casos identificados na União Europeia foram comunicados no dia 24 (França) e 28 (Alemanha) de janeiro de 2020, sendo que a 30 de janeiro a Organização Mundial de Saúde declarou a epidemia do novo coronavírus uma emergência de saúde pública internacional (Public Health Emergency of International Concern – PHEIC), a que se seguiu a declaração do estado pandémico global no dia 11 de março de 2020. O enquadramento cronológico do surto de COVID-19 pode ser consultado em European Center for Disease Prevention and Control Cfr. European Center for Disease Prevention and Control, «Event Background COVID-19» (https://www.ecdc.europa.eu/en/novel-coronavirus/event-background-2019) acesso em 2020-07-26.

[17] A noção de saúde pública é interpretada de acordo com o disposto na alínea c) do artigo 3.º do Regulamento (CE) N.º 1338/2008, entendendo-se por saúde pública todos os elementos relacionados com a saúde, designadamente, o estado de saúde, incluindo a morbilidade e a incapacidade, as motivações 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 quaisquer despesas e o financiamento dos cuidados de saúde, bem como as causas de mortalidade. Cfr. Regulamento (CE) N.º 1338/2008 do Parlamento Europeu e do Conselho de 16 de dezembro de 2008, «Relativo às estatísticas comunitárias sobre saúde pública e saúde e segurança no trabalho» (https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX:32008R1338) acesso em 2020-07-26.

[18] O artigo 12.º do Regulamento Sanitário Internacional de 23 de maio de 2005 estabelece os critérios para a determinação de uma emergência de saúde pública de âmbito internacional. Cfr. Regulamento Sanitário Internacional, (https://www.dgs.pt/autoridade-de-saude-nacional/ficheiros-externos/regulamento-sanitario-internacional-pdf.aspx), acesso em 2020-03-11.

uma concertação adequada de resposta à pandemia, desde logo pela necessidade de se adotarem medidas urgentes que visassem mitigar a extrema virulência e capacidade de contágio do novo coronavírus sob pena de, a breve trecho, se observarem efeitos sociais negativos e irreparáveis em função do desconhecimento da biologia do agente infecioso, a sua virulência e comportamento a curto e longo prazo (leia-se baseada em informação científica suficiente e consolidada).

A incerteza subjacente às medidas de contingência de saúde pública a adotar resulta assim da sua modelação ao próprio desenvolvimento do conhecimento do agente infecioso e da situação pandémica, não se admitindo todavia que deixem de ser cientificamente fundamentadas e socialmente relevantes para que a comunidade com elas se conforme, adotando comportamentos individuais socialmente responsáveis, não expondo os demais a riscos incertos e indesejáveis.

O padrão complexo e dinâmico da pandemia tem assim expressão nas decisões políticas e medidas de contingência adotadas pelos Estados e respetivas autoridades de saúde por um lado, e por outro na sociedade, exigindo-se um reforço da solidariedade e cooperação[19].

O princípio da cooperação, que necessariamente se concretiza por via da solidariedade, com a emergência da pandemia não pode apenas ser apreciado a nível regional, porquanto o caráter transversal da pandemia convoca a solidariedade global, que se desenvolve a partir dos comportamentos sociais individuais nos ordenamentos jurídicos internos[20].

---

[19] Cumpre assinalar que a saúde pública não é um mero somatório da saúde individual, tratando-se de um interesse coletivo, e por isso digno de proteção jurídica, que necessariamente tutela de igual forma interesses individuais, tais como a vida e a integridade física, mas não se esgota na sua dimensão sanitária, projetando-se bem assim em nas condições de subsistência da própria sociedade, tratando-se com efeito de uma tutela sistémica. Refere, a este propósito, Susana Aires de Sousa que nos «(...) crimes previstos no Decreto n.º 2-A/2020, de 20 de março, que procede à execução da declaração do estado de emergência, fundamentam-se não na tutela da saúde pública, mas antes na obediência a ordens de autoridade (...)». Cfr. Sousa Susana Aires de, «Saúde Pública, Direito Penal e "Abate Clandestino"», (https://www.uc.pt/covid19/article?key=a-6eb8a5985f) acesso em 2020-07-26.

[20] Projetando-se uma eminente rutura dos serviços com a emergência da pandemia, à semelhança do que se verificou em Espanha e Itália, a prestação de cuidados de saúde num contexto de contingência, em que os recursos disponíveis são escassos, impôs a hierarquização de prioridades de forma a alocar

«Tem uma relação estreita com o princípio da justiça, uma vez que enfatiza, no reconhecimento do valor individual de cada pessoa, a necessidade de ajudar aqueles cuja vida e dignidade estão mais ameaçadas, em especial os que pertencem a grupos vulneráveis»[21-22].

Ganha, desta forma, extrema importância a transparência das autoridades de saúde na informação relativa à evolução da pandemia para que a sociedade compreenda as medidas adotadas e coopere ativamente num momento de crise sanitária em que é imprescindível a compreensão de incapacidade estrutural socio-económica que afeta diretamente a saúde, direitos e dignidade pessoais, impondo-se a responsabilidade partilhada entre a comunidade e o Estado na prossecução da prevenção primária e secundária do contágio[23] [24].

Aos Estados compete assim, numa situação de emergência como aquela que hoje se vivência, definir e aplicar medidas proporcionais, adequadas, necessárias e transparentes porquanto quaisquer decisões neste domínio terão sempre expressão

os recursos de resposta nos cuidados de saúde segundo o princípio da distribuição equitativa dos recursos disponíveis (materiais e humanos), que foi alcançada pela colaboração dos cidadãos através do imprescindível isolamento social e dever geral de recolhimento.

[21] Conselho Nacional de Ética para as Ciências da Vida, «Situação de Emergência de Saúde Pública pela Pandemia COVI-19: Aspetos Éticos Relevantes», Lisboa: CNECV, 2020. (https://dev.bydas.com/cnecv2/files/1587396084_1586006035_posi%C3%A7%C3%A30%20cnecv%20covid19_03_abril_2020.pdf) acesso em 2020-07-10. P. 7.

[22] «Em situação de escassez de um bem ou serviço, a racionalidade do seu uso ou consumo exige prioridades. A proteção da saúde é, em Portugal, «um direito dos indivíduos e da comunidade que se efectiva pela responsabilidade conjunta dos cidadãos, da sociedade e do Estado, em liberdade de procura e de prestação de cuidados. (…). A nossa lei não se preocupou apenas com a igualdade, ou seja, que todos tivessem igual acesso à saúde, mas também com a equidade, acrescentando às diversas igualdades o princípio da diferenciação positiva: mais cuidados a quem mais deles necessita (*equal care for equal need*)». Campos, António Correia de, «Ética e prioridades em saúde», Ética Aplicada – Saúde, Lisboa: Edições 70, 2018. P. 101-103.

[23] Comissão Nacional de Proteção de Dados, «Orientações sobre a divulgação de informação relativa a infetados por COVID-19», (https://www.cnpd.pt/home/covid19/covid19.htm) acesso em 2020-06-15. P. 1.

[24] Em Portugal foi criada a plataforma Estamos On COVID-19 onde é disponibilizada diariamente pela Autoridade Nacional de Saúde informação relativa aos totais nacionais de casos suspeitos, confirmados, recuperados e de óbitos, sendo que no site da Direção Geral de Saúde (DGS) é ainda possível consultar informação mais pormenorizada do número de infetados e óbitos por concelho. Estamos On COVID-19 (https://covid19estamoson.gov.pt/); DGS (https://covid19.min-saude.pt/) acessos em 2020-06-28.

na esfera dos direitos e liberdades, mas também deveres, dos cidadãos, pessoas singulares, mas de igual forma na comunidade em geral e nas próprias organizações (públicas e privadas)[25].

Neste desiderato, quaisquer medidas adotadas no contexto de emergência, à legitimidade jurídica que lhes é imanente acresce a legitimidade ética, cuja reflexão antecede a própria regulamentação jurídica, porquanto o conjunto de princípios bioéticos que permitiram a evolução para um verdadeiro biodireito e uma biopolítica encontram-se pré ordenados «(…) pela consciencialização de que alguns problemas bioéticos prementes não se situam ao nível da tomada de decisão individual, mas antes exigem um amplo consenso ético e uma vontade colectiva de acção, tal como se verifica no plano da saúde pública ou do ambiente»[26].

Com efeito, se o princípio da precaução se reveste de efeito compulsório dirigido aos Estados, coadjuvados pelas autoridades competentes, a adotar as medidas de contingência adequadas a prevenir ou mitigar (potenciais e efetivos) riscos para a saúde pública[27], tal como se observa no âmbito do surto de COVID-19, não podem

[25] Neste sentido, refere o Conselho Nacional de Ética para as Ciências da Vida (CNECV) que «Algumas medidas prescritas poderão mesmo colidir com princípios bioéticos tidos como adquiridos, como é o caso do respeito pela autonomia e, através dela, a tutela da liberdade individual». Conselho Nacional de Ética para as Ciências da Vida, (nota 21), P. 3.

[26] Neves, Maria do Céu, Osswald, Walter, Bioética Simples, 2.ª ed. rev. e atual., Lisboa: Verbo, 2014. P. 139.

[27] O princípio da precaução encontra-se consagrado no direito primário da União Europeia, designadamente, no artigo 168.º do Tratado sobre o Funcionamento da União Europeia, sob o título XIV – A Saúde Pública, dispõe que «1. (…) A acção da União, que será complementar das políticas nacionais, incidirá na melhoria da saúde pública e na prevenção de doenças e afecções humanas e na redução das causas de perigo para a saúde física e mental. Esta acção abrangerá a luta contra grandes flagelos, fomentando a investigação sobre as respectivas causas, formas de transmissão e prevenção, bem como a informação e a educação sanitária e a vigilância das ameaças graves para a saúde com dimensão transfronteiriça, o alerta em caso de tais ameaças e o combate contra as mesmas. (…) 5. O Parlamento Europeu e o Conselho (…) também podem adotar medidas de incentivo destinadas a proteger e a melhorar a saúde humana, e nomeadamente a lutar contra grandes flagelos transfronteiriços, medidas relativas à vigilância das ameaças graves para a saúde com dimensão transfronteiriça, ao alerta em caso de tais ameaças e ao combate contra as mesmas (…)». Cfr. Tratado sobre o Funcionamento da União Europeia (https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF), acesso em 2020-07-25.

aqueles afastar-se do conteúdo normativo, mas também ético, dos princípios da proporcionalidade, adequação e necessidade.

Ora, não obstante o contexto de incerteza da emergência que suscita, naturalmente, dificuldades na definição de políticas de prevenção, acompanhamento e réplica, estas necessariamente têm de ser modeladas em função da informação e evolução epidemiológica e ponderadas sob a perspetiva dos benefícios esperados e riscos relativos à sua concretização (ou não concretização), devendo a sua execução ser monitorizada e modelada de acordo com a evolução da pandemia.

Com a finalidade de prevenir e mitigar determinados riscos (potenciais ou efetivos) para a saúde pública, sob a égide do dever de proteção da saúde que compete aos Estados, cedem os interesses económicos (não se poderá deixar de ter presente a este prepósito que uma economia não recupera pessoas, mas pessoas recuperam uma economia). Tais interesses não podem, contudo, permanecer refratários sob pena de também no setor da economia de observarem prejuízos irreparáveis e dificilmente recuperáveis.

No contexto de retoma de economia, mas de igual forma das atividades pessoais diárias, surgiram nos diversos segmentos da sociedade propostas dos diversos setores de atividade (científico, tecnológico, empresarial) com o objetivo de auxiliar o controlo sanitário da transmissão do contágio.

As soluções tecnológicas, em bom rigor, têm uma aptidão intrínseca para uma resposta global no controlo sanitário da propagação do contágio, por via de ecossistemas de partilha de dados, apresentando-se como instrumentos potenciadores da salvaguarda da saúde pública e individual.

O emprego de soluções tecnológicas, com o objetivo de mitigar o risco de propagação do contágio, porquanto proporcionam segurança na transição para a retoma da economia e mobilidade geográfica, nacional e internacional, implicando operações de tratamento de dados, não podem é deixar de observar os direitos e

liberdades fundamentais das pessoas singulares em matéria de proteção de dados pessoais.

A legislação aplicável neste domínio, por conseguinte, veicula uma resposta eficiente à pandemia cumprindo simultaneamente o objetivo de proteger a saúde pública[28] e individual, bem como os direitos fundamentais à privacidade e proteção de dados, permitindo a delineação de uma estratégia sanitária eficiente de desconfinamento e controlo do surto pandémico, se se encontrar um equilíbrio entre os direitos fundamentais que aqui se colocam em causa (saúde pública e a privacidade e proteção de dados pessoais).

O princípio da concordância prática exige, assim, que partindo do pressuposto da legitimidade do fim, a idoneidade do meio se evidencie pela adequação à prossecução da finalidade. Trata-se de uma avaliação de teleológica de proporcionalidade face à finalidade concreta.

A adoção de medidas urgentes destinadas à mitigação e contenção do surto de COVID-19 colocaram os Estados, mas também organizações públicas e privadas, no epicentro de operações de tratamento de várias categorias de dados pessoais, que se devem apresentar em primeira instância proporcionais e necessárias, importando sempre que o meio se revele necessário para a satisfação daquela finalidade concreta.

A este propósito note-se que o próprio conceito de tratamento de dados pessoais é um conceito com uma amplitude significativa compreendendo uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou conjuntos de dados pessoais, por meios automatizados ou não automatizados, como sejam a recolha, o registo, a organização, a estruturação, a conservação, a adaptação, a alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão,

[28] Note-se, em todo o caso, que a noção de saúde pública convoca uma proteção sistémica, porquanto não se limita ao somatório de todas as saúdes individuais.

difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição[29].

Objeto destas operações são, nos termos do n.º 1 do artigo 4.º do RGPD os dados pessoais consistentes em quaisquer informações relativas a uma pessoa singular (titular dos dados) identificada ou identificável, considerando-se identificável a pessoa singular que possa ser identificada, direta ou indiretamente, por referência particularmente a um identificador, como seja o nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um, ou mais, aspetos específicos da sua identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular[30].

Adquirem particular relevância no contexto pandémico atual os dados pessoais de saúde que, atenta a particular sensibilidade que os carateriza, conhecem precisas bases jurídicas que legitimam o tratamento, mas de igual forma exigem garantias adequadas face à especificidade desta categoria.

Nos termos do n.º 15 do artigo 4.º do RGPD são dados pessoais de saúde os «(...) dados 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»[31] [32]. Ora, a especial sensibilidade desta categoria de dados pessoais convoca

[29] N.º 2 do artigo 4.º REGULAMENTO (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, «Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)», (https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679) acesso em 2020-07-26. Doravante designado RGPD ou Regulamento (UE) 2016/679.

[30] REGULAMENTO (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679), acesso em 2020-07-26.

[31] A noção de dados pessoais de saúde não pode sequer ser objeto de interpretação restritiva conforme resulta do acórdão do Tribunal de Justiça da União Europeia (TJUE) no processo C- 101/01, designadamente, artigos 50 e 51 do acórdão. Cfr. Acórdão do Tribunal de Justiça, Processo C-101/01, de 6 de novembro de 2003 (http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=11270858) acesso 2020-06-22.

[32] «Os dados relativos à saúde podem ser obtidos a partir de diferentes fontes como, por exemplo: 1. Informações recolhidas por um prestador de cuidados de saúde na ficha clínica (como a «história clínica» e os resultados de exames e tratamentos; 2. Informações que se convertem em dados de saúde através do cruzamento com outros dados, revelando assim o estado de saúde ou os riscos de saúde (como pressuposto de que uma pessoa apresenta um risco mais elevado de sofrer ataques cardíacos

uma tutela qualificada atendendo aos impactos negativos que se podem produzir na esfera jurídica pessoal do titular.

A informação de saúde[33] encontra-se, por isso, 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

O RGPD é um ato jurídico intrinsecamente genérico e flexível que permite a gestão modelar das operações de tratamento de dados pessoais no âmbito das medidas de prevenção e vigilância do surto de COVID-19, salvaguardando, todavia, o respeito pelos direitos fundamentais à privacidade e à proteção de dados pessoais.

Na verdade, o próprio n.º 6 do artigo 19.º da Constituição da República Portuguesa (CRP) ao estabelecer como limites absolutos à suspensão do exercício dos direitos, a vida, a integridade pessoal ou a capacidade civil e a cidadania, na sua lógica e alcance compreende os direitos conexos, designadamente, os previstos no n.º 1 do artigo 26.º da CRP onde se inclui o direito à reserva sobre a intimidade da vida privada

em razão de uma pressão arterial elevada medida durante um determinado período de tempo; 3. Informações provenientes de um inquérito de «autoverificação», em que os titulares dos dados respondem a perguntas relacionadas com a sua saúde (por exemplo, indicação de sintomas); 4. Informações que se convertem em dados de saúde devido à sua utilização num contexto específico (tais como, as informações relativas a uma viagem recente ou à presença numa região afetada pelo COVID-19 processadas por um profissional de saúde para fazer um diagnóstico)». Comité Europeu de Proteção de Dados, «Diretrizes 03/2020 sobre o tratamento de dados relativos à saúde para efeitos de investigação científica no contexto do surto de COVID-19», (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_pt.pdf), acesso em 2020-04-29, P. 5.

[33] Nos termos do disposto no artigo 2.º da Lei N.º 12/2005, de 26 de janeiro, relativa à informação genética pessoal e informação de saúde, a informação de saúde compreende todo o tipo de informação, direta ou indireta, legada à saúde, presente ou futura, de uma pessoa, quer se encontre com vida ou tenha falecido, bem como a sua história clínica e familiar. Note-se que a informação médica, para efeitos do disposto no n.º 1 do artigo 5.º da mesma lei deverá ser compreendida em conjugação com o disposto no na alínea a) do artigo 3.º da Diretiva 2011/24/CE. Lei n.º 12/2005, de 26 de janeiro, (http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1660&tabela=leis), acesso em 2020-07-10; Diretiva 2011/24/CE, relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços, (https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32011L0024&from=PT), acesso em 2020-07-19.

e a proteção legal contra quaisquer formas de discriminação e, por conseguinte, o direito à privacidade e à proteção de dados pessoais (sendo certo que o artigo 35.º da CRP autonomiza este direito do direito matriz à reserva sobre a intimidade da vida privada, conferindo ao direito à proteção de dados pessoais dignidade fundamental constitucionalmente autónoma)[34] [35] [36].

Por conseguinte, o estado de exceção que pode legitimar a imposição de restrições ao exercício de direitos e liberdades[37] [38], desde que proporcionadas e limitadas ao período de emergência, não poderá é ultrapassar o imperativo de proteção dos dados dos respetivos titulares, devendo assegurar-se que o tratamento

[34] Com efeito, nem o Decreto do Presidente da República N.º 14 A/2020 de 18 de março, que declara o estado de emergência com fundamento na verificação de uma situação de calamidade pública, nem o Decreto do Presidente da República N.º 17 A/2020, de 2 de abril ou o Decreto do Presidente da República N.º 20 A/2020, de 17 de abril que procederam à primeira e segunda renovação da declaração do estado de emergência com fundamento na verificação de uma situação de calamidade pública, previam a suspensão do exercício do direito à privacidade ou à proteção de dados pessoais.

[35] Toda a legislação aprovada no ordenamento jurídico nacional no contexto do surto de COVID-19 pode ser consultada por ordem cronológica em (https://dre.pt/legislacao-covid-19-upo).

[36] Em sentido absolutamente oposto, o governo da Hungria ao declarar o estado de emergência, determinou a suspensão do exercício de alguns direitos em matéria de proteção de dados, não obstante a suspensão se verificar exclusivamente durante o período do estado de exceção. A este propósito o Comité Europeu de Proteção de Dados Dados publicou a declaração sobre a restrição de direitos no contexto do estado de emergência a 2 de junho de 2020, referindo a situação observada na Hungria. Cfr. European Data Protection Board, «Statement on restrictions on data subjects rights in connection to the state of emergency in Member States», (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_art_23gdpr_20200602_en.pdf), acesso em 2020-06-05.

[37] A declaração do estado de emergência em Portugal, nos termos do n.º 3, 4 e 5 do artigo 19.º da Constituição da República Portuguesa, apenas pode determinar a suspensão do exercício de alguns direitos, liberdades e garantias (a especificação dos direitos, liberdades e garantias cujo exercício fica suspenso é adequadamente fundamentada), com respeito pelo princípio da proporcionalidade, limitando se a sua extensão, duração e meios utilizados ao estritamente necessário, não podendo ter duração superior a 15 dias, sem prejuízo de eventuais renovações.

[38] Neste sentido pronunciou-se o Comité Europeu de Proteção de Dados, «Declaração sobre o tratamento de dados pessoais no contexto do surto de COVID-19», (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementreopeningbordersanddataprotection_pt.pdf) acesso em 2020-03-20, P. 1, «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. (…) o Comité Europeu para a Proteção de Dados gostaria de sublinhar que, mesmo nestes tempos de exceção, os responsáveis pelo tratamento de dados e os subcontratantes devem assegurar a proteção de dados pessoais dos respetivos titulares. (…) Esta emergência pode legitimar a imposição de restrições às liberdades, desde que sejam proporcionadas e limitadas ao período de emergência».

cumpre a vocação de transparência e serve efetivamente os melhores interesses da pessoa humana.

Evidencia-se, nestes termos, a necessidade de uma interpretação ético-jurídica global no emprego das novas tecnologias no contexto da emergência de saúde pública atenta a pluralidade dos destinatários de quaisquer medidas de biovigilância preventiva e de mitigação do risco provocado para a saúde pública pelo surto de COVID-19.

3. Operações de tratamento de dados pessoais no contexto do controlo sanitário de propagação do contágio

Como é bom de se ver, é a humanidade enquanto denominador comum da situação epidemiológica que tem um superior interesse na prevenção e redução da causa de perigo transfronteiriça para a saúde pública (aqui considerada globalmente) sendo que quaisquer ações de prevenção e vigilância com o objetivo direto de proteger a saúde pública podem alcançar um profícuo resultado com a adoção de instrumentos de execução com recurso a novas tecnologias e, consequentemente, dados pessoais.

O quadro legal de direito europeu e de direito interno (como é o Regulamento Geral de Proteção de Dados (RGPD) e a Lei N.º 58/2019, de 8 de agosto que assegura a execução na ordem jurídica interna o RGPD) em matéria de proteção de dados não obsta, em bom rigor, a que sejam adotadas medidas de contingência sanitária com recurso a tecnologias.

Neste desiderato, em primeira instância, os dados pessoais tratados devem apenas ser os necessários para atingir os objetivos visados[39], devendo apenas ser tratados para finalidades específicas e explícitas, conforme resulta deste logo do artigo 5.º do RGPD, exigindo-se que quaisquer medidas adotadas no âmbito da gestão da

[39] Observa-se, neste sentido, que a maioria das medidas adotadas que implicam operações de tratamento de dados pessoais determinam a recolha das, pelo menos, seguintes categorias de dados: dados de contato, dados relativos à saúde e dados de localização. Neste sentido, Comissão Nacional de Proteção de Dados, «Deliberação 2020/262», (https://www.cnpd.pt/home/covid19/covid19.htm), acesso em 2020-06-20, P. 2v.

situação de emergência, bem como o processo de decisório que às mesmas presidiu, se encontre devidamente documentado e fundamentado.

Acresce aos princípios gerais vertidos no artigo 5.º [40] 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.

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[41]. 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[42].

O cumprimento dos princípios gerais relativos ao tratamento de dados pessoais consagrados no n.º 1 do artigo 5.º, bem como a obrigação de executar todas as medidas necessárias e adequadas a cumprir as obrigações dele resultantes e a necessária comprovação da eficácia das medidas adotadas – conforme se alcança do princípio de *accountability* previsto no n.º 2 do mesmo artigo – impõe ainda a realização de uma avaliação de impacto (artigo 35.º do RGPD).

A avaliação de impacto sobre a proteção de dados consiste num processo que permite identificar e minimizar os riscos, avaliando a proporcionalidade das operações e gerindo os riscos destas resultantes, donde o próprio n.º 1 do artigo 35.º do RGPD prevê esta obrigação para o responsável pelo tratamento [43] sempre que, e

[40] No n.º 1 do artigo 5.º o princípio da licitude, lealdade e transparência ((a); limitação das finalidades ((b); minimização dos dados ((c); exatidão ((d); limitação da conservação ((e); integridade e confidencialidade ((f).

[41] Comité Europeu de Proteção de Dados (nota 38), P. 2

[42] Comité Europeu de Proteção de Dados (nota 38), P. 2

[43] Admite-se, ainda, no n.º 8 do artigo 35.º que a avaliação de impacto possa ser realizada pelo subcontratante.

antes de iniciar o tratamento, a operação for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares tendo em conta a natureza, âmbito, contexto e finalidades do tratamento.

Enquanto instrumento de responsabilização, demonstração de conformidade e de gestão do risco, o n.º 3 do artigo 35.º prevê a obrigatoriedade de realização da avaliação de impacto, designadamente na sua alínea b), nos casos de tratamentos em grande escala de categorias especiais de dados, tais como os elencados no n.º 1 do artigo 9.º e entre os quais se observam os dados pessoais de saúde.

A importância deste instrumento para o cumprimento dos princípios e demais obrigações em matéria de proteção de dados evidencia-se desde logo pela leitura das disposições conjugadas do artigo 35.º e 23.º, que não admite o afastamento desta obrigação do responsável pelo tratamento pelo legislador nacional, compreendendo-se no âmbito destas limitações as situações de exceção constitucional em que se possam encontrar os Estados Membros[44] conforme o é a atual situação global de emergência de saúde pública.

4. Tratamento de dados por motivos de interesse público no domínio da saúde pública: a ameaça transfronteiriça grave para a saúde

O RGPD prevê regras aplicáveis ao tratamento de dados pessoais num contexto de surto pandémico, como o que se observa com o novo coronavírus, permitindo que as autoridades competentes em matéria de saúde pública (em Portugal a autoridade de saúde é a Direção Geral de Saúde[45]) procedam a operações de tratamento de dados pessoais em conformidade com o direito nacional e nas condições nele estabelecidas,

[44] Comissão Nacional de Proteção de Dados (nota 39), p. 8-9.

[45] Conforme resulta das disposições conjugadas da Base 34 da Lei N.º 95/2019, de 4 de setembro – Lei de Bases da Saúde (https://dre.pt/web/guest/pesquisa/-/search/124417108/details/maximized) e artigo 5.º e 6.º do Decreto Lei N.º 135/2013, de 4 de outubro, que estabelece as regras de designação, competência e funcionamento das entidades que exercem o poder de autoridade de saúde (https://dre.pt/pesquisa/-/search/500190/details/maximized). (https://dre.pt/web/guest/pesquisa/-/search/124417108/details/maximized), acesso em 2020-06-27.

conforme é o tratamento de dados pessoais necessário por motivos de interesse público importante no domínio da saúde pública[46].

4.1. Vigilância epidemiológica e alerta rápido de ameaças graves para a saúde

A cláusula de proteção reforçada vertida no artigo 9.º do RGPD consubstancia «(...) uma salvaguarda de direitos fundamentais em face do tratamento de dados pessoais. E essa salvaguarda traduz-se na necessidade de preencher um dos fundamentos jurídicos (ou uma das finalidades admissíveis) previstos no n.º 2, que nada mais constituem do que ponderações do legislador comunitário em relação a restrições a direitos fundamentais»[47].

Por conseguinte, preside por isso às operações de tratamentos de dados pessoais de saúde uma regra geral de proibição (n.º 1 do artigo 9.º do RGPD), não obstante as derrogações previstas para esta categoria especial de dados (n.º 2 do artigo 9.º do RGPD), tais como as operações de tratamento necessárias por motivos de interesse público importante no domínio da saúde pública com base no direito da União Europeia ou no direito interno, nos termos previstos na alínea i) do n.º 2 do artigo 9.º do RGPD[48], ao que acresce o próprio considerando 46 que prevê a necessidade do tratamento desta categoria de dados sensíveis se for necessário para fins humanitários, incluindo a monitorização de epidemias e a sua propagação[49].

[46] Alínea i) do n.º 2 do artigo 9.º do RGPD.
[47] Duarte, Tatiana, Comentário ao Regulamento Geral de Proteção de Dados, Coimbra: Almedina, 2018, p. 237.
[48] De igual forma quando seja necessário proteger os interesses vitais do titular dos dados, nos termos da alínea c) do n.º 2 do artigo 9.º do RGPD.
[49] 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. (...). Alguns tipos de tratamento podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo de o tratamento for necessário para fins humanitários, incluindo a monitorização de epidemias e a sua propagação ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana». REGULAMENTO (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679) acesso em 2020-07-26.

Atente-se que nestas circunstâncias não é sequer requisito de licitude o consentimento, nos termos das disposições conjugadas da alínea a) do n.º 1 do artigo 6.º e alínea a) do n.º 2[50] do artigo 9.º do RGPD.

Ora, o tratamento necessário por motivos de interesse público no domínio da saúde pública, nos termos da alínea i) do n.º 2 do artigo 9.º do RGPD, particularmente no que concerne à proteção contra ameaças transfronteiriças graves para a saúde[51], consiste essencialmente num sistema de vigilância epidemiológica, assente na recolha, registo, análise, interpretação e divulgação sistemática de dados e análises de doenças transmissíveis, bem como outros problemas de saúde especiais conexos (alínea d) do artigo 3.º da Decisão N.º 1082/2013/UE, de 22 de outubro)[52] [53].

A vigilância epidemiológica é, com efeito, um procedimento de monitorização vocacionado para o alerta rápido que permite o combate e o planeamento da preparação e resposta a ameaças transfronteiriças graves para a saúde que, no escopo do princípio da cooperação, pretende complementar a ação coordenada das políticas

[50] As exceções previstas no n.º 2 concretizam a previsão de cláusulas de exclusão da ilicitude das operações de tratamento em referência que, de acordo com um juízo de proporcionalidade em relação ao interesse predominante, justificam e legitimam o tratamento de dados pessoais de saúde. No mesmo sentido, Duarte, Tatiana (nota 59), p. 238.

[51] Consideram-se ameaças transfronteiriças graves para a saúde, nos termos da alínea g) do artigo 3.º da Decisão N.º 1082/2013/UE «uma ameaça para a vida ou um perigo grave para a saúde pública de origem biológica, química, ambiental ou desconhecida que se propague ou implique um risco considerável de se propagar através das fronteiras nacionais dos Estados-Membros, e que possam tornar necessária a coordenação a nível da União a fim de assegurar um nível elevado de proteção da saúde humana»; de acordo com a alínea a) do artigo 2.º são ameaças de ordem biológica as doenças transmissíveis, a resistência antimicrobiana e infeções associadas aos cuidados de saúde relacionados com doenças transmissíveis e as biotoxinas ou outros agentes biológicos nocivos não relacionados com doenças transmissíveis.

[52] Decisão N.º 1082/2013/UE do Parlamento Europeu e do Conselho, de 22 de outubro, relativa às ameaças sanitárias transfronteiriças graves e que revoga a Decisão N.º 2119/98/CE, (https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013D1082&from=pt), acesso em 2020-06-15.

[53] Nos termos do n.º 1 do artigo 9.º da Decisão N.º 1082/2013/UE as autoridades nacionais competentes ou a Comissão devem notificar um alerta através Sistema de Alerta Rápido e de Resposta o aparecimento ou evolução de uma ameaça transfronteiriça grave para a saúde quando a ameaça é invulgar ou inesperada no local e momento específicos, causa ou pode causar uma morbilidade ou mortalidade humanas significativas, propaga-se ou pode propagar-se rapidamente, ou excede ou pode exceder a capacidade de resposta nacional; a ameaça afeta ou pode afetar mais do que um Estado-membro; a ameaça exige ou pode exigir uma resposta coordenada ao nível da União.

nacionais dos Estados Membros (o que aliás resulta das disposições conjugadas do n.º 1 e 2 do artigo 1.º e artigo 4.º da Decisão N.º 1082/2013/UE).

A este procedimento de monitorização subjaz um sistema de notificação de deteção de doenças que representem ameaças transfronteiriças que é operado através do Sistema de Alerta Rápido e de Resposta devendo as autoridades nacionais com competências para o efeito notificar o aparecimento ou evolução de uma ameaça transfronteiriça grave para a saúde [54] [55].

Conforme resulta da alínea i) do n.º 3 do artigo 9.º da Decisão N.º 1082/2013/UE, na sequência da notificação de um alerta através do EWRS[56], a Comissão e as autoridades competentes em saúde pública dos Estados-Membros partilham as informações adequadas e úteis que se considerem pertinentes para coordenar a resposta à ameaça, o que inclui a partilha de dados pessoais[57] [58].

De acordo com o artigo 16.º da Decisão N.º 1082/2013/UE a autoridade nacional competente para proceder à notificação no EWRS é considerada responsável pelo tratamento (n.º 7), estabelecendo como medidas específicas de proteção de dados pessoais a implementação de medidas técnicas e organizativas adequadas a proteger

[54] O Early Warning and Response System encontra-se previsto no n.º 1 do artigo 8.º da Decisão N.º 1082/2013/UE .

[55] Artigo 8.º e 9.º da Decisão N.º 1082/2013/UE do Parlamento Europeu e do Conselho, de 22 de outubro, relativa às ameaças sanitárias transfronteiriças graves e que revoga a Decisão N.º 2119/98/CE, (https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013D1082&from=pt), acesso em 2020-06-15.

[55] EWRS – Early Warning and Response System.

[56] A Decisão de Execução (UE) 2017/253 da Comissão, de 12 de fevereiro, estabelece procedimentos para a notificação de alertas no âmbito do sistema de alerta rápido e de resposta adotado em relação às ameaças sanitárias transfronteiriças graves e para o intercâmbio de informações, consulta e coordenação de respostas a essas ameaças em conformidade com a Decisão N.º 1082/2013/UE do Parlamento Europeu e do Conselho, (https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32017D0253), acesso em 2020-03-15.

[57] A alínea i) do n.º 3 do artigo 9.º da Decisão N.º 1082/2013/UE prevê especificamente a partilha de dados pessoais necessários para efeitos de localização de contatos, previsão que se encontra melhor desenvolvida em relação a medidas de proteção específicas no artigo 16.º conforme se analisará.

[58] O n.º 3 do artigo 9.º da Decisão N.º 1082/2013/EU elenca, designadamente, o tipo e origem do agente; data e local do incidente ou do surto; meios de transmissão ou de propagação; dados toxicológicos; métodos de deteção e de confirmação; riscos para a saúde pública; medidas de saúde pública aplicadas ou que tencione aplicar; medidas que não sejam de saúde pública; dados de localização de contatos; quaisquer outras informações relevantes para a ameaça.

os dados pessoais contra a destruição acidental ou ilegal, a perda acidental ou o acesso não autorizado, bem como qualquer forma de tratamento ilegal (n.º1).

Para este efeito o EWRS inclui uma função de transmissão seletiva de mensagens que assegura que os dados pessoais apenas são comunicados às autoridades nacionais competentes dos Estados-Membros que sejam partes interessadas nas medidas de localização e rastreio de contatos (n.º 2 e 3), devendo a transmissão seletiva de mensagens ser concebida e utilizada de forma a garantir um padrão de segurança e legalidade em relação ao intercâmbio de dados pessoais necessário (n.º 2), visando cumprir o critério superior de *privacy by design* e *privacy by default* nos termos do artigo 25.º do RGPD.

Para efeitos de cumprimento do princípio da limitação da conservação é, de igual forma, definido um período de doze meses para o apagamento após a data de envio da mensagem seletiva que contenha dados pessoais (n.º 5), sendo certo que, observando o princípio da necessidade, caso uma autoridade competente verifique que uma notificação de dados pessoais por si efetuada ao abrigo do n.º 3 do artigo 9.º se revelou *ex post* contrária à luz do RGPD, designadamente, por ser desnecessária para a aplicação das medidas de localização e rastreio de contatos em causa, deve disto informar os Estados-Membros aos quais a notificação foi transmitida (n.º 6).

4.2. Operações de tratamento de dados pessoais de saúde pela autoridade de saúde pública nacional

A Lei N.º 81/2009, de 21 de agosto, criou um sistema nacional de informação e vigilância epidemiológica, designado SINAVE (Sistema Nacional de Vigilância Epidemiológica), que instituiu um sistema de vigilância integrada em saúde pública[59] [60], que identifica situações de risco, recolhe, atualiza, analisa e divulga dados relativos

[59] A rede nacional do sistema integrado de vigilância envolve os serviços operativos da saúde (públicos e privados), os laboratórios, bem como as autoridades de saúde.

[60] O regulamento de notificação obrigatória de doenças transmissíveis ao SINAVE foi publicado pela Portaria n.º 248/2013, de 5 de agosto, (http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=1982A0011&nid=1982&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=); a lista de doenças transmissíveis de notificação obrigatória

a doenças transmissíveis e outros riscos em saúde pública, contribuindo de igual forma para a preparação de planos de contingência em circunstâncias de emergência ou de calamidade pública[61].

A finalidade do tratamento de dados do SINAVE encontra-se no n.º 2 do artigo 20.º da Lei N.º 81/2009, de 21 de agosto, e consiste em determinar se o estado de saúde da pessoa representa um risco potencial para a saúde pública, prevendo-se no n.º 4 do mesmo artigo que quaisquer operações de tratamento de dados necessárias à gestão e avaliação de risco em saúde pública garantem o princípio da minimização dos dados, da exatidão, da minimização do período de conservação e que o tratamento será sempre efetuado por profissionais de saúde habilitados para o efeito, quando necessário para as finalidades de exercício de medicina preventiva, atos de diagnóstico médico, prestação de cuidados de saúde ou gestão dos serviços de saúde[62].

As entidades que integram o sistema de vigilância nacional recolhem e transmitem os dados relativos à identificação da doença ou evento, bem como a descrição detalhada das caraterísticas clínicas e microbiológicas detetadas ou outra informação relevante para a caraterização do evento de forma anonimizada e agregada, conforme resulta das disposições conjugadas no n.º 1 do artigo 3.º e n.º 2 do artigo 6.º do Despacho N.º 4355, de 25 de março[63].

Nos termos do n.º 1 do artigo 6.º do regulamento de notificação obrigatória de doenças transmissíveis os casos de patologias de notificação obrigatória e outros

consta do Despacho N.º 15395-A/2016, de 21 de dezembro, (https://www.dgs.pt/ficheiros-de-upload-2013/sinave-lista-de-ddo-pdf.aspx).

[61] Artigos 1.º e 2.º da lei N.º 81/2009, de 21 de agosto, que institui um sistema de vigilância em saúde pública, (http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1981&tabela=leis&nversao=&so_miolo=), acesso em 2020-06-25.

[62] O n.º 3 e 4 do artigo 3.º da Portaria N.º 248/2013, de 5 de agosto define os perfis de acesso para a entidades participantes no procedimento de notificação obrigatória, segregando o acesso de acordo com os perfis atribuídos.

[63] Despacho N.º 4355/2014, de 25 de março, que determina os métodos de vigilância epidemiológica e microbiológica, (https://dre.pt/web/guest/pesquisa/-/search/3353794/details/normal?q=Despacho+n.%C2%BA%204355%2F2014), acesso em 2020-07-20.

riscos para a saúde pública são identificados pelos médicos no exercício da sua profissão e completados com a notificação laboratorial (sempre que aplicável)[64]. Ora, esta obrigação de reporte exclui o consentimento do titular dos dados, porquanto se trata de uma obrigação legal cuja base jurídica de licitude se alcança na alínea i) do n.º 2 do artigo 9.º do RGPD.

O artigo 17.º deste diploma, com a epígrafe "poder regulamentar excecional" prevê que o membro do governo responsável pela área da saúde, sob proposta do Diretor Geral da Saúde (n.º 2 do art.º 17.º), emita e adote as medidas indispensáveis em situações de emergência em saúde pública com a finalidade de tornar exequíveis as normas de contingência que se revelem adequadas a evitar a propagação de qualquer infeção ou contaminação, designadamente, em casos epidemiológicos.

Neste sentido foi concebida a plataforma TRACE COVID-19[65] [66]que tem por objeto a gestão de doentes em autocuidados e ambulatório, tratando-se de uma ferramenta de suporte ao seguimento clínico efetivo e medidas de saúde públicas adequadas a doentes com suspeita ou confirmação da doença COVID-19, através de um conjunto de tarefas geradas pelo sistema que permitem esta monitorização[67].

---

[64] Portaria n.º 248/2013, de 5 de agosto, (http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=1982A0011&nid=1982&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=), acesso em 2020-07-31.

[65] Pese embora a conceção desta plataforma de *contact tracing* não tenha sido objeto de uma avaliação de impacto ex ante, conforme já foi assinalado pela Comissão Nacional de Proteção de Dados, dever-se-á proceder à mesma ainda que a operação de tratamento já se encontre em curso por força da natureza essencial para a gestão do risco ou que a sua função tenha sido alcançado por outra via. «(...) a plataforma TRACE COVID-19 foi desenhada, implementada e utilizada sem que essa avaliação tivesse tido lugar. Ora, a importância da sua realização apresenta-se como evidente no caso concreto. Com efeito, se a mesma tivesse sido realizada antes do desenho da solução tecnológica, certamente que a análise do impacto do tratamento de dados permitiria ter detetado alguns dos riscos por ela gerados e a prevenção da afetação (desnecessária) dos direitos e liberdades dos titulares dos dados, mediante a adoção de medidas adequadas para a mitigação desse impacto, nos termos determinados pelo artigo 25.º do RGPD». Cfr. Comissão Nacional de Proteção de Dados (51), p. 7-8.

[66] «(...) foi esclarecido que a SPMS atua neste tratamento de dados pessoais como subcontratante da Direção-Geral de Saúde (DGS) (...)». Comissão Nacional de Proteção de Dados (nota 39), p. 1v.

[67] Direção Geral de Saúde, «Norma N.º 004/2020 – COVID-19: Fase de Mitigação», (https://www.dgs.pt/directrizes-da-dgs/normas-e-circulares-normativas/norma-n-0042020-de-23032020-pdf.aspx), acesso em 2020-07-20, P. 4; A Comissão Nacional de Proteção de Dados publicou a Deliberação 2020/262 a respeito desta plataforma de *contact tracing* de doentes em vigilância e autocuidado. Comissão Nacional de Proteção de Dados (nota 39).

Nesta ferramenta são tratadas as seguintes categorias de dados pessoais: dados relativos de contato (morada, contato telefónico, email), dados relativos à identificação (nome, número de utente e/ou NIF e/ou documento de identificação civil, data de nascimento), dados relativos à saúde (estado de vigilância, estado do exame, data de início e fim de vigilância, origem do utente, link epidemiológico/contato, registo de óbito), dados relativos à localização (domicílio, hospital, outra). Quanto ao registo das vigilâncias encontram-se os dados referentes: à informação de uma vigilância, resumo dos sintomas e perguntas efetuadas, observações e cálculo de um *score* de risco com base na sintomatologia[68].

Esta plataforma será integrada com o SINAVE, designadamente com o SINAVE Lab. e SINAVE Med., para recolha dos dados relativos aos exames laboratoriais de forma a proceder-se a uma vigilância eficaz do doente monitorizado[69].

A autenticação na ferramenta de vigilância de doentes em autocuidado é concretizada através das contas já utilizadas pelos profissionais de saúde do Serviço Nacional de Saúde (SNS) e do Ministério da Saúde já identificados nos seus sistemas, tendo sido criadas contas "guest" para as entidades de saúde privadas[70].

A TRACE COVID-19 conhece três perfis de acesso – local[71], regional[72], e nacional[73] – que são estabelecidos de acordo com o número de instituições às quais o utilizador tem acesso, sendo permitidas a todos os perfis de utilizador as seguintes operações de tratamento: inserção, atualização de doentes, tarefas e vigilâncias, e a transferência de utentes entre unidade responsável por vigilância. Todos os perfis são administrados de acordo com os princípios da identidade, pelo estabelecimento de *users* nominais e princípios de acessos mínimos, restringindo-se o acesso ao mínimo

[68] Comissão Nacional de Proteção de Dados (nota 39), p. 2v-3.
[69] Idem – Ibidem.
[70] Comissão Nacional de Proteção de Dados (nota 39), p. 1v-2.
[71] O perfil local acede aos dados do respetivo Agrupamento de Centros de Saúde e Unidade Funcional ou instituição hospitalar.
[72] O perfil regional acede aos dados do Agrupamento de Centros de Saúde e Unidades Funcional regionais.
[73] O perfil nacional acede aos dados de todas as instituições.

necessário para as funções de gestão, administração e operação às contas de privilégios mais elevados[74].

Como se pode observar, a plataforma de *contact tracing* TRACE COVID-19 agrega e concentra a informação relativa à saúde dos doentes COVID-19, permitindo uma monitorização abrangente e em larga escala dos doentes infetados e registados nas diversas unidades de saúde nacionais, encontrando-se por isso sujeita a regras de proteção reforçadas de confidencialidade, conforme resulta das disposições conjugadas da alínea h) do n.º 2 e 3 do artigo 9.º, 25.º e 32.º do RGPD, impondo-se a necessidade de assegurar um nível de segurança adequado ao risco atendendo à informação de grande sensibilidade nesta constante.

Ademais e considerando a especial circunstância em que a base de dados que suporta a plataforma de *contact tracing* foi criada não poderá deixar de se ter presente que o princípio da limitação das finalidades, previsto na alínea b) do n.º 1 do artigo 5.º do RGPD, conhecendo algumas refrações, determina uma prudente reutilização dos dados pessoais porquanto a finalidade da sua criação é, em bom rigor, transitória e particularmente especificada em relação à situação de emergência que a justifica.

Nestes termos, quaisquer refrações àquele princípio devem pautar-se pela adstrição ao princípio vertido na alínea e) do n.º 1 do artigo 5.º, como será o caso da reutilização para efeitos de investigação de investigação científica epidemiológica – artigo 89.º do RGPD – desde que sujeitos a regras reforçadas de proteção, tais como a pseudonimização ou anonimização irreversível[75].

---

[74] Comissão Nacional de Proteção de Dados (nota 39), p. 2.

[75] Neste sentido também se pronunciou o Comité Europeu de Proteção de Dados na Diretriz 03/2020 relativa ao tratamento de dados relativos à saúde para efeitos de investigação científica. «Há que salientar que o princípio da integridade e da confidencialidade deve ser lido em articulação com os requisitos do artigo 32.º, n.º 1, e do artigo 89.º, n.º 1, do RGPD. As referidas disposições devem ser plenamente respeitadas. Por conseguinte, tendo em conta os riscos elevados acima referidos, devem ser aplicadas medidas técnicas e organizativas adequadas e atualizadas para garantir um nível de segurança suficiente. Tais medidas devem consistir, pelo menos, na pseudonimização, na encriptação, em acordos de não divulgação, numa atribuição estrita das funções de acesso, no estabelecimento de restrições na função de acesso, bem como de registos de acesso». Cfr. Comité Europeu de Proteção de Dados (nota 32), p. 11.

4.3. Utilização de aplicações digitais para controlo sanitário da transmissão do SARS-COV-2

Com o objetivo de auxiliar o controlo sanitário da propagação do contágio do SARS-COV-2 as organizações, públicas e privadas, têm apresentado diversas soluções tecnológicas com o propósito de oferecer uma resposta adicional na monitorização das cadeias de contágio (melhor seria que fosse transfronteiriça), assentes na recolha de informação através dos telemóveis pessoais com aplicações digitais, comummente designadas de *apps* de *contact tracing*, que consubstanciam "marcadores de contato" da infeção COVID-19.

Estas aplicações são concebidas por via da criação de um ecossistema de dados relativos à marcação de contato visando proporcionar um benefício para a saúde pública e individual, através do cruzamento de *big data* de identificação pseudonomizada individual, rastreando em termos de modo e circunstâncias a propagação do novo coronavírus num certo espaço temporal, reforçando a qualidade e segurança da estratégia sanitária modelar de desconfinamento que se vai edificando progressivamente. Note-se a este propósito que o rastreamento de contatos não deverá depender da utilização de dados de localização individuais, mas sim de informações de proximidade dos utilizadores de forma a atenuar-se uma ingerência excessiva, e por isso desproporcionada, no domínio da privacidade que é a liberdade de movimentação.

O pressuposto é de que, nos termos do princípio da concordância prática, a ingerência no domínio da movimentação física e da informação de saúde – valores eminentemente pessoais – encontra-se justificada perante os benefícios coletivos alcançados pela recolha e agregação dos dados pessoais.

Ora, um mecanismo digital, como o é um marcador de contato para sinalização de um indivíduo que foi testado positivamente, para identificar supervenientemente pessoas que com ele estiveram em contato exige necessariamente uma ponderação ética no domínio do direito à proteção de dados pessoais sob pena de a jusante

encontrarmo-nos num sistema de biovigilância cujos prejuízos se devem ter por imprevisíveis.

A necessária ponderação ética é presidida assim pela necessidade de capacitação individual de proteção da saúde individual e de terceiros, concomitantemente com as medidas de prevenção e proteção individual já convencionadas para controlo da pandemia, procurando-se evitar modelos de vigilância permanentes ou a estigmatização dos indivíduos – que se poderão observar por via da evidência das desigualdades sociais e segregação de grupos sociais mais vulneráveis (inerentes à iliteracia digital, bem como à possibilidade de aquisição de equipamentos móveis que suportem esta tecnologia) – e que neste sentido considerem os princípios vertidos no artigo 25.º do RGPD na sua dimensão de ética *by design* e ética *by default*.

Com este propósito, já se pronunciou o Conselho Nacional de Ética para as Ciências da Vida, cuja posição se acompanha de perto, no sentido de que «Para se aceitar que as aplicações para dispositivos móveis devam fazer parte da estratégia sanitária de controlo do surto pandémico, designadamente das cadeias de transmissão do vírus na comunidade, possibilitando respostas rápidas, haverá que ponderar, com critério, se os meios utilizados (parametrização das aplicações, telemóveis com certas caraterísticas técnicas e o uso de dados de identificação pessoal) são efetivos e proporcionados aos objetivos de saúde pública a que se destinam e, não menos relevante, que medidas permitem prevenir o risco de violação de direitos fundamentais, como o direito à privacidade»[76].

Com efeito, as *apps* de *contact tracing* podem representar um relevante mecanismo de segurança na transição para a retoma da "nova normalidade", bem como para o regresso à mobilidade geográfica – seja nacional ou internacional –

[76] Conselho Nacional de Ética para as Ciências da Vida, «Aplicações Digitais Móveis para Controlo da Transmissão da COVID-19. Aspetos Éticos Relevantes», Lisboa: CNECV, 2020, (https://www.cnecv.pt/files/1593523643_62f80ed69c317b6cee76810d493bb77a_posic-a-0-cnecv-apps-mo-veis-controlo-covid19-29-06-2020.pdf), p. 3, acesso em 2020-07-10.

porquanto assumem a vocação de auxílio às autoridades de saúde para controlo da propagação infeciosa. Contudo, a utilidade de controlo sanitário e o valor social e jurídico refratário com o recurso a esta tipologia de *apps*, apenas se alcança pela reunião de pressupostos que dificilmente são reunidos cumulativamente.

O desiderato de controlo das cadeias de transmissão do SARS-COV-2 com recurso à tecnologia de *contact tracing* terá assim de ter como pressuposto um modelo de governança de privacidade e de dados pessoais presidido pelo princípio da transparência, garantindo-se a subsistência da relação de confiança entre a sociedade, o Estado e as autoridades de saúde pela precisa identificação de critérios de segurança, auditoria, rastreabilidade e responsabilidade que subjazem a uma medida que, em maior ou menor grau, representa uma ingerência na reserva da vida privada e privacidade dos indivíduos[77], cumulativamente e sempre com caráter instrumental relativamente a uma estratégia sanitária que, necessariamente, convoca uma realização generalizada de testes de diagnóstico e uma efetiva capacidade de resposta do serviço nacional de saúde[78].

A eficácia que se pode reconhecer à tecnologia de rastreamento de contatos enquanto instrumento com aptidão para alcançar um benefício social relevante para efeitos de gestão do contágio depende da reunião de um conjunto de pressupostos que, em todo o caso, serão sempre dificilmente reuníveis, como sejam: voluntariedade na instalação da *app* – que sempre se encontrará condicionada pela capacidade

[77] Neste sentido, se pronunciou o Comité Europeu de Proteção de Dados ao afirmar que «(...) acredita firmemente que, quando tratamento de dados pessoais é necessário para a gestão da pandemia COVID-19, a proteção de dados é indispensável para construir confiança, criar condições de aceitação social de qualquer solução e, assim, garantir a eficácia dessas medidas. Uma vez que o vírus não conhece fronteiras, parece preferível desenvolver uma abordagem europeia comum em resposta à atual crise ou, pelo menos, criar um quadro interoperável». Cfr. Comité Europeu para a Proteção de Dados, «Diretrizes n.º 4/2020 sobre a utilização de dados de localização e ferramentas de *contact tracing* no contexto do surto de COVID-19», (https://www.cnpd.pt/home/orientacoes/Diretrizes_4-2020_contact_tracing_covid_with_annex_en_PT.pdf), p. 3, acesso em 2020-04-25.

[78] World Health Organization, «Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing», (https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1), p. 1, acesso em 2020-05-30; World Health Organization «Contact tracing in the context of COVID-19», (https://apps.who.int/iris/handle/10665/332049), acesso em 2020-05-20.

económica individual para a aquisição de equipamentos e literacia digital necessárias à utilização de tecnologia com caraterísticas técnicas avançadas para a finalidade sanitária em causa; descarregamento e ativação da aplicação por uma percentagem significativa da população; cumprimento das orientações sanitárias recomendadas após sinalização de contato com uma pessoa diagnosticada com SARS-COV-2.

A este respeito é inteligível que uma estratégia sanitária de saúde pública para controlo da transmissão do novo coronavírus com recurso a esta tecnologia compreenda a realização dos testes de diagnóstico subsequentes aos casos sinalizados como contatos, supondo-se desta forma uma capacidade de resposta do serviço nacional de saúde a uma percentagem significativa da população que instale a aplicação de rastreio, porquanto sem uma utilização generalizada deste instrumento não se alcançará o seu objetivo.

Não sobranceiras são, de igual forma, as barreiras inerentes à voluntariedade da ação da pessoa singular tais como a necessidade de transportar consigo o telemóvel, manter a conexão de dados ou a ativação permanente do reencaminhamento de sinalização de contato, às quais acrescem as fragilidades relativamente à definição de um período de duração de contato ou proximidade física que, efetivamente, consubstanciem um risco acentuado[79].

4.3.1. Considerações éticas sobre sistemas digitais de rastreio de proximidade

Conforme já se pôde observar, o *contact tracing* não é uma novidade no rigor dos seus termos porquanto é já empregue do âmbito da vigilância em saúde pública,

[79] Conselho Nacional de Ética para as Ciências da Vida (nota 76), p. 3-4. Ressalva a este propósito, dando conta da existência da barreiras físicas determinantes para a possibilidade de contágio, que «A verificação de uma determinada distância entre um telemóvel cujo detentor está infetado e o telemóvel de outro cidadão não significa, necessariamente, a existência de um contágio, mas apenas a coexistência dos dois telemóveis num dado espaço, como indício da eventualidade de nele terem coexistido os respetivos detentores, ou seja os indivíduos podem ter estado fisicamente separados de um modo tal que não tenha havido a possibilidade de um contágio entre si».

apresentando-se as ferramentas de rastreio de proximidade no contexto do surto pandémico como um *input* ao *contact tracing*.

O rastreio retrospetivo de proximidade é particularmente pertinente num contexto em que a capacidade de virulência é exponencial e já se encontra diagnosticada, encontrando-se sobremaneira vocacionado para a fase pré sintomática da infeção respiratória que, de toda a forma, não representa uma diminuição do acentuado potencial infecioso do SARS-COV-2[80], devendo por isso reconhecer-se a legitimidade do seu propósito.

Sempre se poderá afirmar que o recurso a tecnologias de rastreio de proximidade, ainda que redutoras da privacidade, sempre serão menos restritivas que imposições gerais de recolhimento obrigatório. Todavia, não se poderá, de igual forma, deixar de ter presente que a avaliação da eficácia desta tecnologia sempre terá de ser ponderada à luz das restantes alternativas e do desenho da própria tecnologia, particularmente no que concerne à minimização do impacto efetivo na privacidade, padrões de segurança e proteção da informação e transparência quanto às finalidades da operação de tratamento.

Ora, um contexto de emergência em saúde pública não legitima, *per se*, ingerências excessivas na esfera jurídica de liberdade das pessoas singulares, independentemente das dimensões de liberdade pessoal (e de igual forma na privacidade) em que sejam observáveis, pelo que quaisquer restrições ou ingerências, conforme o são as medidas de rastreio de proximidade, solicitam uma preocupação ética eminente no que respeita à privacidade e à proteção de dados pessoais, cuja tutela é permanentemente convocada atenta a sua amplitude e alcance.

[80] «COVID-19 presents a problema for contact tracing as usually practiced because around 50% of transmissions happen early in infection, before symptoms start, and before test results can be acted on. This means that COVID-19 moves too quickly through the population to be amenable to standart contact tracing methods». Cfr. PARKER, Michael J.; FRASER, Christophe; ABELER-DÖRNER, Lucie; BONSALL, David, «Ethics of instantaneous contact tracing using mobile phones apps in the control of the COVID-19 pandemic», Journal of Medical Ethics, 46, 2020, (https://jme.bmj.com/content/medethics/46/7/427.full.pdf), p. 427, acesso em 2020-06-06.

Em bom rigor, note-se que, o processamento de informação de proximidade numa operação de tratamento de dados com esta finalidade tem aptidão para produzir efeitos sobremaneira gravosos na esfera jurídica das pessoas singulares, que não se cingem ao potencial discriminatório e estigmatizante, produzidos quase de forma imediata na própria liberdade de circulação e reunião familiar[81].

A finalidade de informar os utilizadores que estiveram expostos ao vírus num período de tempo epidemiologicamente relevante, tem consequências imediatas no exercício de liberdades fundamentais, tal como a de circulação[82], mas de igual forma no exercício da atividade profissional atento o dever de permanecer em isolamento profilático até que o teste laboratorial apresente resultado negativo. Sendo certo que os próprios testes poderão apresentar resultados inconclusivos ou falsos positivos, deve por isso assegurar-se que o mecanismo de retificação ou atualização dos resultados subsequentes seja tecnicamente célere de forma a atenuar quaisquer eventos adversos que se venham a observar na sequência de notificação de exposição.

Pretendendo atenuar o impacto negativo na privacidade dos utilizadores, no quadro atual de proteção de dados pessoais, deve ser dada preferência a meios menos invasivos que não impliquem a utilização de dados relativos à localização da pessoa singular[83], devendo a informação tratada restringir-se a dados relativos à proximidade entre utilizadores através de, e a título de exemplo, tecnologia *bluetooth low energy*.

Para este efeito, o Comité Europeu de Proteção de Dados reforçou a importância do princípio da minimização, *by design e by default* no âmbito do recurso

[81] PARKER, Michael J.; FRASER, Christophe; ABELER-DÖRNER, Lucie; BONSALL, David, (nota 80), p. 429.
[82] O que implica, bem assim, repercussões na esfera jurídico-laboral, porquanto será necessário, no caso de um trabalhador, apresentar justificação de faltas e desencadear o processo de baixa por doença.
[83] Nos termos da Diretiva e-Privacy por dados de localização entendem-se «quaisquer dados tratados numa rede de comunicações eletrónicas ou por um serviço de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas acessível ao público». Alínea c) do artigo 2.º da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, (https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32002L0058), acesso em 2020-09-13.

a esta tecnologia para gestão da emergência sanitária[84], afirmando que «(...) as aplicações de rastreamento de contato não exigem o rastreamento da localização de utilizadores individuais. Em vez disso, devem ser utilizados dados de proximidade[85]; uma vez que estas aplicações podem funcionar sem identificação direta dos indivíduos, devem ser tomadas medidas adequadas para evitar a reidentificação; as informações recolhidas devem residir no equipamento terminal do utilizador e apenas as informações relevantes devem ser recolhidas quando tal for absolutamente necessário»[86].

Neste sentido, é particularmente importante que seja assegurada a impossibilidade de identificação ou inferência de identificação do utilizador diagnosticado por via da utilização de técnicas criptográficas, sendo certo que a recolha do histórico de contatos de proximidade deverá ser sempre precedida pelo diagnóstico de um profissional de saúde e a ação de autorização subsequente do utilizador voluntária.

O *bluetooth* não poderá, ainda assim, ser considerado uma panaceia neutra quanto ao resultado porquanto não exclui riscos efetivos para a privacidade da localização da pessoa singular, desde logo por exigir a sua ativação permanente (contrariamente à utilização tradicional desta tecnologia que é meramente transitória), abrindo-se por esta via a monitorização constante do dispositivo e, por isso, do utilizador.

---

[84] Dever-se-á entender a especificação deste objetivo para conformação com o princípio da limitação das finalidades previsto na alínea b) do n.º 1 do artigo 5.º do RGPD, excluindo-se outros tratamentos posteriores à gestão da crise sanitária provocada pelo surto de COVID-19. De igual forma o cumprimento do princípio da limitação da conservação ganha aqui expressão, limitando-se esta ao período da emergência epidemiológica de saúde pública, o que não significa que posteriormente não possam ser utilizados para finalidades de pesquisa científica ou estatísticos (alínea j) do n.º 2 do artigo 9.º do RGPD) desde que asseguradas as medidas técnicas e organizativas necessárias à proteção da informação em conformidade com o artigo 89.º do RGPD.

[85] Por conseguinte, quaisquer fontes de modelação e contenção da propagação do contágio com recurso a tecnologia de *contact tracing* devem depender de informações relativas à proximidade entre utilizadores e não do rastreamento da localização de forma a mitigar a lesão que sempre se deverá ter por observável na privacidade das pessoas singulares.

[86] Comité Europeu de Proteção de Dados (nota 77), p. 7.

A informação de proximidade recolhida no terminal do equipamento móvel do utilizador encontra-se no âmbito da norma vertida no n.º 3 do artigo 5.º da Diretiva e-Privacy que expressamente consagra que «Os Estados Membros asseguram que o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só sejam permitidos se este tiver dado o seu consentimento prévio com base em informações claras e completas(...)»[87], donde resulta que o consentimento livre, informado, explícito, específico e inequívoco se traduz ou numa declaração de vontade, ou num ato material revelador do consentimento, adstrito aos objetivos daquele tratamento específico subsequente.

Ora, o consentimento é, neste contexto, necessariamente enformado pelo dever qualificado de informação atendendo ao grau de ingerência na privacidade da pessoa singular, privacidade que reclama tutela precedente a quaisquer prejuízos que venham a ser observados em consequência de uma operação de tratamento de dados.

O processamento de dados de saúde, conceito que não pode ser objeto de interpretação restritiva, sendo admitido para fins de interesse público relevante em saúde pública, encontra-se em todo o caso sujeito a uma tutela reforçada que impõe uma normalização transparente do processamento da informação para o utilizador que deverá consentir ponderando o elevado nível de risco que representa para os seus direitos e liberdades fundamentais, bem como o potencial discriminador e estigmatizante da informação tratada.

Significa isto que, prescindindo-se do consentimento enquanto base jurídica de licitude para a operacionalização do tratamento de dados pessoais desta tipologia, o consentimento ganha especial relevância no âmbito da interação do utilizador antes e após ser diagnosticado com a infeção respiratória aguda.

[87] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, (https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32002L0058), acesso em 2020-09-13.

O rastreamento de proximidade, instrumental à marcação de contatos, enquanto operação de tratamento de dados pessoais encontra, nestes termos, a base jurídica de licitude nas disposições conjugadas da alínea e) do n.º 1 do artigo 6.º com as alíneas h) e i) do n.º 2 do artigo 9.º do RGPD, atendendo à necessidade do processamento das categorias de dados tratados por razões de interesse público na área da saúde pública[88], designadamente no que concerne ao objetivo de informar as pessoas singulares em relação à potencial exposição das mesmas ao SARS-COV-2, excluindo-se o consentimento do titular dos dados como requisito de licitude para a criação deste tipo de tratamento de dados.

A exclusão do consentimento enquanto base jurídica legitimadora no desenho desta metodologia de rastreio não afasta o caráter voluntário da utilização das *apps* de *contact tracing*[89].

Com efeito, e atenta a vocação instrumental em relação a uma política alargada de medidas de prevenção primárias, a utilização desta tecnologia encontrará a sua matriz fundante na voluntariedade do utilizador, a quem se terá de assegurar uma efetiva liberdade de escolha na utilização daquela.

Em bom rigor, uma limitação ao direito fundamental à autodeterminação pessoal num Estado Direito Democrático, ainda que no contexto excecional de emergência em saúde pública, terá sempre de observar o princípio da proporcionalidade, adequação e necessidade, donde sempre se pugnará pelo caráter voluntário de utilização da *app* atendendo ao seu potencial para intensificar desigualdades, discriminações e a segregação de pessoas mais vulneráveis[90].

[88] «Quando as autoridades públicas prestam um serviço com base num mandato atribuído por e em conformidade com os requisitos legais, afigura-se que a base jurídica relevante para o tratamento é a necessidade de desempenhar uma tarefa de interesse público, ou seja, o artigo 6.º, n.º 1, alínea e), do RGPD». Comité Europeu de Proteção de Dados (nota 77), p. 7.

[89] PARKER, Michael J.; FRASER, Christophe; ABELER-DÖRNER, Lucie; BONSALL, David, (nota 80), p. 429.

[90] No mesmo sentido a World Health Organization, (nota 78), p. 1.

4.3.2. STAYWAY COVID: uma *app* instrumental a uma estratégia global de interrupção das cadeias de contágio

Nos termos do n.º 2 do art.º 1.º do Decreto Lei N.º 52/2020, de 11 de agosto, «O STAYWAY COVID é um sistema digital para dispositivos móveis pessoais com sistema operativo «IOS» ou «ANDROID», que utiliza como sensor de proximidade a tecnologia «Bluetooth Low Energy» e notifica os utilizadores da exposição individual a fatores de contágio por SARS-CoV-2, decorrente de contacto com o utilizador da aplicação que posteriormente venha a ser confirmado com COVID-19, nos termos definidos pela Direção-Geral da Saúde (DGS), funcionando como um instrumento complementar e voluntário de resposta à situação epidemiológica pelo reforço da identificação de contactos»[91].

Trata-se de uma aplicação desenvolvida pelo Instituto de Engenharia de Sistemas de Computadores, Ciência e Tecnologia, em parceira com o Instituto de Saúde Pública da Universidade do Porto e as empresas Keyruptive e Ubirider, tendo sido atribuída à DGS a competência de responsável pelo tratamento de dados pessoais (n.º 1 do art.º 3.º) e aos Serviços Partilhados do Ministério da Saúde EPE (SPMS) (n.º 2 do art.º 3.º), na qualidade de subcontratante, a responsabilidade de assegurar os serviços e meios técnicos necessários ao seu funcionamento.

A operação de tratamento de dados que permite o funcionamento da aplicação é excecional e transitória[92], mantendo-se apenas enquanto a finalidade de controlo

[91] Decreto-Lei N.º 52/2020, de 11 de agosto, que estabelece o responsável pelo tratamento de dados e regula a intervenção do médico no sistema STAYWAY COVID, (https://dre.pt/web/guest/home/-/dre/140013521/details/maximized?serie=I&day=2020-08-11&date=2020-08-01), acesso em 2020-08-12.

[92] Um dos fatores que podem motivar a instalação desta tipologia de tecnologia é precisamente a garantia de que os dados tratados serão definitivamente eliminados após o período de exceção. Esta garantia não só consubstancia um princípio ético fundamental nas relações verticais como nas horizontais. Todavia, note-se que a dimensão relacional de confiança é construída e suportada por diversos fatores que não residem em meras afirmações declaratórias, donde os antecedentes e as informações (muitas vezes inconsistentes e aparentemente incongruentes) reveladas pelas autoridades competentes no contexto das medidas de modelação preventiva e de resposta à evolução da pandemia não têm contribuído para a consolidação da relação de confiança necessária à prossecução do reforço deste modelo de vigilância em saúde pública. No mesmo sentido, PARKER, Michael J.; FRASER, Christophe; ABELER-DÖRNER, Lucie; BONSALL, David, (nota 80), p. 430.

sanitário da situação epidemiológica o justificar conforme previsto no artigo 5.º do Decreto-Lei N.º 52/2020, de 11 de agosto.

Por conseguinte, o rastreio de proximidade deverá apenas ocorrer num lapso de tempo determinado, particularmente enquanto o rastreio contatos não puder apenas ser assegurado por intervenção humana, destinando exclusivamente a alertar ao potencial risco de exposição e não para efeitos de monitorização das medidas de quarentena obrigatória ou aferição do cumprimento das regras distanciamento social.

A aplicação de rastreio de contatos utiliza o sistema Google-Apple Exposure Notification (GAEN)[93] que foi concebido especificamente para habilitar o funcionamento de aplicações de rastreio de proximidade com recurso a *bluetooth*, uma vez que a aplicação não executa autonomamente funcionalidades do sistema operativo, encontrando-se autorizado o acesso apenas a uma aplicação por país[94] [95].

O utilizador voluntário que descarregue e configure a aplicação no seu dispositivo móvel pessoal, aderindo assim a este sistema de notificação de exposição ao risco de contágio[96], é integrado no sistema que permite calcular o risco de contágio com uma pessoa infetada, através do cruzamento de marcadores de contatos pseudoaleatórios de proximidade que são gerados diariamente pela aplicação num intervalo de 10 a 20 minutos[97].

Os identificadores pseudoaleatórios de proximidade são difundidos por *bluetooth* e recebidos nos dispositivos móveis pessoais de outros utilizadores da

---

[93] Google-Apple Exposure Notification, Exposure Notification: Using technology to help public health authorities fight COVID-19, (https://www.google.com/covid19/exposurenotifications/), acesso em 2020-08-18.

[94] Comissão Nacional de Proteção de Dados, «Deliberação 2020/277», (https://www.cnpd.pt/home/decisoes/Delib/DEL_2020_277.pdf), p. 2, acesso em 2020-07-05.

[95] Google-Apple Exposure Notification, Exposure Notification: Using technology to help public health authorities fight COVID-19, (https://www.google.com/covid19/exposurenotifications/), acesso em 2020-08-18.

[96] «O sistema STAYAWAY adota um modelo descentralizado, isto é, os dados não são coligidos, armazenados e processados num servidor central, mas sim no dispositivo móvel do utilizador. O cálculo do risco e notificação do utilizador são efetuados localmente nesse dispositivo». Cfr. Comissão Nacional de Proteção de Dados (nota 89), p. 1v.

[97] Comissão Nacional de Proteção de Dados (nota 93), p. 2v-3.

aplicação que se encontrem no perímetro geográfico alcançável do sinal e ficam armazenados por um prazo de 14 dias no dispositivo móvel pessoal[98].

Assim, nos termos do art.º 4.º do Decreto-Lei N.º 52/2020, caso um utilizador da aplicação seja diagnosticado com COVID-19 o médico obtém e comunica àquele um código de legitimação pseudoaleatório constituído por 12 números que, deverá ser introduzido pelo utilizador na *app* caso assim o pretenda fazer.

Para obtenção do código de legitimação de diagnóstico é necessário que o médico registe a data dos primeiros sintomas ou, no caso de doentes assintomáticos, a data da realização do teste laboratorial[99], sendo que a obtenção do código de legitimação pseudoaleatório gera simultaneamente um código de acesso pseudoaleatório.

O doente deverá, nesta sequência, introduzir o código comunicado pelo médico na aplicação dando início ao envio automático das chaves diárias armazenadas no dispositivo móvel pessoal nos últimos 14 dias para o serviço de publicação de diagnóstico na aplicação[100].

O serviço de publicação de diagnóstico cruza os identificadores de contato pseudoaleatórios que se encontram armazenados no seu servidor com os recebidos de outros dispositivos móveis pessoais com os quais o utilizador esteve num determinado espaço geográfico e de tempo que se encontram registados no seu dispositivo móvel pessoal, calculando localmente o risco com base na distância física e duração do contato de proximidade em função da exposição individual,

[98] Comissão Nacional de Proteção de Dados (nota 93), p. 2v.
[99] De acordo com n.º 3 do art.º 4.º do Decreto-lei N.º 52/2020 os dados são registados sem qualquer identificação do doente diagnosticado.
[100] Comissão Nacional de Proteção de Dados (nota 93), p. 3.

apresentando nesta sequência um alerta ao utilizador com a informação em relação modo subsequente de procedimento[101] [102].

O desiderato de cumprir a finalidade de alertar os utilizadores para um eventual risco de contágio, concomitantemente com a garantia de privacidade endereçada às pessoas singulares, é assim prosseguida tendo como princípio orientador a voluntariedade da sua utilização.

Na verdade, as fases de desencadeamento das notificações de proximidade de exposição ao risco[103], considerando que lhes é subjacente o processamento de informação de saúde – particularmente protegida pela tutela reforçada que lhe é conferida com a proibição geral vertida no n.º 1 do artigo 9.º do RGPD – permitem ao utilizador o controlo da informação pessoal pseudonimizada que é tratada e que, nesta etapa, se encontra subordinada ao consentimento do titular dos dados.

A voluntariedade é assim notada *ex ante*, porquanto o utilizador poderá desativar o *bluetooth* no dispositivo móvel, interrompendo o envio e a receção dos identificadores pseudoaleatórios de proximidade, bem como *ex post* diagnóstico através de atos materiais positivos ou negativos inequívocos quanto ao processo volitivo final em relação à operação de tratamento de dados.

---

[101] «No dispositivo móvel, a aplicação pode apresentar ao utilizador três estados diferentes: sem risco, alerta de potencial contacto de risco, diagnosticado com COVID-19. Em cada um destes estados, é apresentada informação adicional. No caso de diagnóstico positivo, após terem sido comunicadas as chaves TEK, por ação do utilizador, este é informado de que a aplicação STAYAWAY «deixa de monitorizar os contactos», devendo ser reinstalada a aplicação após recuperação e o regresso à vida normal para reiniciar o processo». Comissão Nacional de Proteção de Dados (nota 93), p. 3-4.

[102] Parte-se sempre do pressuposto que existe uma efetiva capacidade de testagem, que permita diagnósticos céleres, pelo que os resultados laboratoriais constituem um vetor determinante, não só para efeitos de diminuição dos dias de isolamento profilático em caso de resultado negativo, mas de igual forma na definição de um protocolo de procedimentos para o doente confirmado com o COVID-19 que, regra geral, terá de ser isolado num contexto de agregado familiar. Em sentido próximo, cfr. PARKER, Michael J.; FRASER, Christophe; ABELER-DÖRNER, Lucie; BONSALL, David, (nota 80), p. 427-428.

[103] «A primeira manifestação de vontade exerce-se quando é instalada a aplicação no seu dispositivo móvel pessoal. Posteriormente, caso tenha um diagnóstico positivo para a COVID-19, tem ainda a possibilidade de não comunicar essa informação à aplicação, bastando para tal não informar o médico de que é utilizador da STAYAWAY ou, ainda que o faça, não introduzir posteriormente o código de legitimação no sistema. Este conjunto de ações está na sua inteira disponibilidade e sob o seu total controlo». Cfr. Comissão Nacional de Proteção de Dados (nota 93), p. 4-5.

Acresce que sempre será possível a desinstalação da aplicação, sendo certo que, se por um lado seria expectável o apagamento dos dados do utilizador, por outro o controlo do alcance desta ação está na disponibilidade do sistema operativo GAEN, cujo benefício na disponibilização desta plataforma é dificilmente discernível e em relação ao qual se suscitam reservas (particularmente no que concerne à utilização futura da informação que seja recolhida)[104].

O consentimento, enquanto derrogação ao regime jurídico especial de proteção de dados sensíveis, é nestes termos apenas considerado válido por força da conformação ao princípio da transparência (alínea a) do n.º 1 do artigo 5.º e artigo 12.º do RGPD) que deverá encontrar-se na informação prévia que é disponibilizada ao utilizador, de forma a assegurar que a manifestação de vontade é esclarecida, livre, explicita e consciente relativamente ao tratamento de dados pessoais.

Não se refere o consentimento a uma mera declaração de vontade reduzida a escrito, mas antes a um ato positivo inequívoco que apenas poderá resultar do exercício de uma liberdade informada de acordo com o padrão do utilizador médio, que permita a observância do cumprimento do dever de transparência através da qualificação do dever de informação, considerando a limitação da proteção conferida a dados que assumem caraterísticas particularmente sensíveis, revestindo por isso a qualidade de causa de exclusão da ilicitude do tratamento.

Por conseguinte, pode-se afirmar que a tutela é convocada de forma centralizada no titular dos dados a quem compete ponderar, de acordo com um juízo de proporcionalidade, a respeito dos direitos e interesses refratários face a um interesse que considere individualmente mais relevante, como o poderá ser a saúde pública, justificando o tratamento.

[104] Ressalva-se a este propósito que se é possível a instalação da aplicação sem qualquer registo para ativação da mesma, em bom rigor o utilizador sempre será identificável porquanto não é possível o download da *app* sem acesso às lojas virtuais onde os utilizadores têm de ser autenticados.

5. Considerações finais

Não sendo propósito do presente artigo trazer respostas ou apresentar soluções para as problemáticas suscitadas pela utilização de tecnologias de monitorização no contexto do surto provocado por COVID-19, são agora expendidas algumas considerações a título reflexivo a respeito do interesse que cede a propósito do interesse público na proteção da saúde.

A vigilância epidemiológica com recurso às novas tecnologias tem um propósito ético e jurídico de promoção e proteção da saúde, constituindo a matriz de uma resposta modelar adequada a uma emergência epidemiológica/pandémica, mas cujo alcance se encontra muito além deste objetivo primário.

Com aptidão para evidenciar as iniquidades, é contudo um mecanismo que permite a definição de políticas de saúde públicas adequadas a mitigar desigualdades sociais e a acautelar a posição de vulnerabilidade em que se encontra parte da população, designadamente, por se achar endereçada a grupos de risco que, por isso, merecem especial proteção.

Não deixando, contudo, de suscitar controvérsia por força das limitações intrínsecas à privacidade e ao exercício de outras liberdades, o emprego de novas tecnologias no âmbito da vigilância epidemiológica é ponderada em correspondência à adequação dos meios empregues em relação à finalidade prosseguida.

O surto pandémico provocado pelo surto de COVID-19 convocou, assim, para a discussão pública o emprego de diversas soluções tecnológicas de vigilância para a prevenção e mitigação das cadeias de contágio do SARS- COV-2, colocando em especial destaque a disciplina legal de proteção de dados pessoais.

Sendo certo que a maioria dos sistemas de vigilância em saúde pública, como o Early Warning and Response System a nível europeu, ou o SINAVE no âmbito interno, eram já utilizados sem suscitar grande preocupação para a sociedade, a adoção de tecnologias de rastreio de proximidade no contexto do *contact tracing* promoveram a reflexão ético-jurídica relativamente aos benefícios e riscos para a

privacidade, particularmente por força do potencial perpetuador de iniquidades resultantes da estigmatização e discriminação dos indivíduos.

Se os avanços tecnológicos assinaláveis se caraterizam pela ausência de fronteiras digitais, a saúde pública sistémica é também caraterizada pela necessidade de adoção de políticas de saúde pública globais que importam considerações ético-jurídicas além fronteiras, especialmente por àquelas se encontrarem subjacentes pessoas singulares, cuja informação pessoal é tratada, impondo que se acautele simultaneamente o direito fundamental à proteção de dados pessoais.

A concordância prática entre a salvaguarda do bem comum, a saúde pública, a equidade e a solidariedade social (valores eminentemente coletivos) e a autodeterminação pessoal, a privacidade e as liberdades pessoais não é meramente declaratória, porquanto o alcance daqueles primeiros não se autocompraz sem a reciprocidade dos valores eminentemente pessoais. Todavia, o interesse público na proteção da saúde impõe uma ponderada adequação de partilha dos riscos não se admitindo a adoção de soluções tecnológicas compulsórias, subtraídas à voluntariedade dos utilizadores.

A emergência de saúde pública global provocada pelo novo coronavírus determinou a aplicação de metodologias modelares de resposta às cadeias de contágio suportadas em diversas operações de tratamento de categorias de dados pessoais. Ora, se algumas destas operações, tais como os sistemas de vigilância epidemiológica por autoridades de saúde pública podem encontrar-se enquadradas num valor superlativo de proteção da saúde pública, admitindo-se por isso dispensar o consentimento da pessoa singular, porquanto ainda se encontram na esfera de proteção dos interesses do titular dos dados, o rastreio de proximidade não poderá resultar de uma imposição heterónoma.

O direito fundamental à proteção de dados pessoais será sempre um direito pessoal reconhecido e não uma mera criação técnico-jurídica sem consequências práticas na voluntariedade da sua limitação.

O objetivo de qualquer procedimento de vigilância será o de limitar a propagação do contágio, permitindo às autoridades públicas de saúde operar uma gestão do risco adequada através da sinalização de casos diagnosticados com COVID-19, seguimento dos contatos primários do doente e monitorização dos casos em vigilância ativa. Neste sentido, consistindo o *contact tracing* na identificação de todos os indivíduos que podem ter sido expostos ao contágio, num período epidemiológico relevante, é um instrumento de importância reforçada porquanto permite o isolamento do diagnosticado e possíveis contagiados com COVID-19, interrompendo as cadeias de transmissão do vírus.

Não se recolhendo dados relativos à localização geográfica, o rastreamento de proximidade não deixa, contudo, de possibilitar a rastreabilidade de movimentos, sendo sobremaneira importante que se assegure que o sistema de notificação não permitirá revelar qualquer informação do utilizador que faz desencadear o envio dos códigos pseudoaleatórios.

Ora, o rastreamento de contatos é um protocolo de identificação de contatos cuja exposição ao risco de infeção é significativa, permitindo a adoção de medidas sanitárias previamente definidas no quadro de um programa de saúde pública mais amplo.

Quer isto significar que o rastreio de proximidade, ainda que não recolha dados pessoais relativos à localização, não deve ser prioritário em relação às medidas tradicionais convencionadas de rastreamento de contatos, devendo por isso a sua utilização ser estritamente voluntária, assegurando-se uma verdadeira liberdade de escolha entre a sua utilização ou não.

A privacidade, em período anterior à pandemia, era o epicentro do desenho das soluções tecnológicas contemporâneas, que devem ser dotadas de uma delineação ética centrada na pessoa humana. A utilização de *apps* de rastreio de proximidade, conjugadas com medidas mais restritivas de outras liberdades, apenas se poderá ter por estritamente voluntária, deixando-se ao utilizador a centralização da tutela da

privacidade , competindo lhe ponderar se a limitação voluntária à privacidade e à proteção de dados pessoais é justificada face ao objetivo prosseguido.

O seu caráter instrumental relativamente a um plano alargado de proteção da saúde pública tem assim de ser assegurado, não devendo a pessoa singular ser penalizada no exercício dos seus direitos e liberdades no domínio da proteção da saúde, sob pena de não se anuir que o consentimento nesta operação de tratamento de dados pessoais seja verdadeiramente livre e a utilização desta tecnologia voluntária.