e-pública
Revista Eletrónica de Direito Público

Protecção de dados em tempos de COVID-19 – Breves reflexões

Data protection in times of COVID-19 – Brief remarks

MARIANA MELO EGÍDIO

VOL. 7 Nº 1 ABRIL 2020

WWW.E-PUBLICA.PT

ICJP INSTITUTO DE CIÊNCIAS JURÍDICO-POLÍTICAS
CIDP CENTRO DE INVESTIGAÇÃO DE DIREITO PÚBLICO

COM O APOIO DE:

FCT Fundação para a Ciência e a Tecnologia

ISSN 2183-184x

PROTECÇÃO DE DADOS EM TEMPOS DE COVID-19 – BREVES REFLEXÕES

DATA PROTECTION IN TIMES OF COVID-19 – BRIEF REMARKS

MARIANA MELO EGÍDIO
Faculdade de Direito da Universidade de Lisboa
Alameda da Universidade
1649-014 Lisboa, Portugal
marianameloegidio@fd.ulisboa.pt

Resumo: A pandemia de COVID-19, enquanto situação de calamidade pública, motivou que fosse decretado pela primeira vez o estado de emergência ao abrigo da Constituição de 1976, mas lançou também desafios ao regime de protecção de dados pessoais. Porém, ao contrário de outros direitos suspensos no período de estado de emergência e restringidos em estado de calamidade, o regime do direito em causa resulta, em primeira linha, do Direito Europeu.

Assim, o tratamento de dados pessoais realizado pela Administração Pública tem de ser baseado, mesmo em estado de excepção (constitucional ou administrativo) nos mesmos fundamentos de licitude previstos no RGPD. Analisar-se-á o problema dos limites ao tratamento de dados pessoais pela Administração Pública a partir das orientações publicadas pela CNPD sobre divulgação de informação relativa a infetados por COVID-19 por parte de autarquias locais, precisamente para confirmar que o estado de excepção não apaga as exigências provenientes do RGPD nesta matéria.

Palavras-chave: estado de excepção, rastreamento de contactos, licitude do tratamento, interesse público, Administração Pública

Abstract: The COVID-19 pandemic, as a public calamity situation, motivated not only the first state of emergency declaration under the 1976 Constitution, but it also posed some challenges to personal data protection. However, unlike other rights suspended during the state of emergency or restricted during the state of calamity, the regime in question is primarily a result of European – not national – law.

Thus, the processing of personal data carried out by the Public Administration

must be based, even in a state of exception (should it be constitutional or administrative), on the lawfulness of processing reasons provided for in the GDPR. The problem of the limits on data processing by the Public Administration will be analyzed based on the guidelines published by the CNPD on the disclosure of information by local authorities regarding people infected with Covid-19, so as to confirm that the state of exception does not erase the requirements imposed by the GDPR.

Keywords: emergency state, contact tracing, lawfulness of processing, public interest, public authorities

1. Introdução: o estado de emergência e a protecção de dados pessoais

A declaração do estado de emergência, a que se sucedeu a declaração do estado de calamidade, tem vindo a colocar interessantes questões em sede de protecção de dados[1] – mas talvez, como veremos, com menor intensidade face a outros domínios afectados pela suspensão de direitos fundamentais inerente à declaração do estado de emergência ou pela imposição de restrições, enquanto consequência do estado de calamidade[2].

Por um lado, o contexto de combate à pandemia e à disseminação do coronavírus SARS-CoV-2 levou à discussão, também no âmbito da União Europeia, da admissibilidade do recurso a apps de *contact tracing*[3]; por outro, foi amplamente discutida em Portugal a admissibilidade de medição da temperatura corporal dos trabalhadores, ainda que sem registo da mesma, o que motivou até a aprovação de uma norma visando especificamente ultrapassar quaisquer dúvidas sobre a legalidade da referida medição – cfr. o artigo 13.º-C do Decreto-Lei n.º 20/2020, de 1 de Maio[4] – mas que pode, ela própria, suscitar dúvidas de

1. Sobre algumas destas mudanças estruturais e desafios colocados ao direito à protecção de dados, cfr. F. Paes Marques, *Impacto na gestão de dados pessoais*, vídeo disponível em https://www.youtube.com/watch?v=AlspEYJuN9g&list=PLdC_vodN92GBSXWSVvJL2d8ou-U-SqMPnP&index=17 (consultado em 15 de Maio de 2020).

2. Cfr., a este propósito, as medidas excecionais e temporárias de resposta à epidemia SARS-CoV-2 e à doença COVID-19 no âmbito da declaração de situação de calamidade em todo o território nacional, constantes do anexo à Resolução do Conselho de Ministros n.º 33-A/2020, de 30 de março. A referida resolução invoca, como suas normas habilitantes, o artigo 12.º e 13.º do Decreto-Lei n.º 10-A/2020, de 13 de março, por força do disposto no artigo 2.º da Lei n.º 1-A/2020, de 19 de março, e, no que mais interessa, o artigo 17.º da Lei n.º 81/2009, de 21 de agosto, bem como o artigo 19.º da Lei n.º 27/2006, de 3 de julho, e ainda a alínea *g*) do artigo 199.º da Constituição. A Lei n.º 27/2006, de 3 de julho, refere-se à Lei de Bases da Protecção Civil, enquanto a Lei n.º 81/2009, de 21 de agosto, corresponde ao acto legislativo que institui um sistema de vigilância em saúde pública, que identifica situações de risco, recolhe, actualiza, analisa e divulga os dados relativos a doenças transmissíveis e outros riscos em saúde pública, bem como prepara planos de contingência face a situações de emergência ou tão graves como de calamidade pública. Por sua vez, os restantes dois diplomas correspondem a actos legislativos já adoptados no contexto da resposta à pandemia e já alvo de várias alterações: a Lei n.º 1-A/2020, de 19 de março, que cria medidas excecionais e temporárias de resposta à situação epidemiológica provocada pelo coronavírus SARS-CoV-2 e da doença COVID-19, e o Decreto-Lei n.º 10-A/2020, de 13 de março, que estabelece medidas excecionais e temporárias relativas à situação epidemiológica do novo Coronavírus - COVID 19.

3. Já aplicadas em vários países da Ásia, nomeadamente China, Singapura, Japão e Coreia do Sul. Sobre o uso destas aplicações, cfr. https://www.economist.com/china/2020/05/02/a-view-from-the-covid-19th-floor?utm_campaign=later-linkinbio%20theecono-mist&utm_content=later6956747&utm_medium=social&utm_source=instagram (acedido em 15 de Maio de 2020).

4. Artigo 13.º-C Controlo de temperatura corporal

1 - No atual contexto da doença COVID-19, e exclusivamente por motivos de proteção da saúde do próprio e de terceiros, podem ser realizadas medições de temperatura corporal a trabalhadores para efeitos de acesso e permanência no local de trabalho.

2 - O disposto no número anterior não prejudica o direito à proteção individual de dados, sendo expressamente proibido o registo da temperatura corporal associado à identidade da pessoa, salvo com expressa autorização da mesma.

3 - Caso haja medições de temperatura superiores à normal temperatura corporal, pode ser impedido o acesso dessa pessoa ao local de trabalho.

constitucionalidade[5].

Também a Comissão Nacional de Protecção de Dados emanou neste período um conjunto de orientações[6] sobre proteção de dados no contexto da COVID-19, interessando-nos particularmente analisar as "Orientações sobre divulgação de informação relativa a infetados por Covid-19", nomeadamente no tocante ao tratamento de dados pessoais por parte da Administração Pública (em especial, autarquias locais), na parte em que analisa a aplicação da alínea *e*) do n.º 1 do artigo 6.º e da alínea *i*) do n.º 2 do artigo 9.º, do RGPD no âmbito do tratamento de dados por entidades públicas.

5. Cfr., levantando algumas dúvidas, A. SOUSA PINHEIRO, "A COVID – 19 e a proteção de dados pessoais", Observatório Almedina, 28 de abril de 2020, acessível em https://observatorio.almedina.net/index.php/2020/04/28/a-covid-19-e-a-protecao-de-dados-pessoais/ (acedido em 15 de Maio de 2020), "Acrescentamos que se a legislação nacional optar por introduzir uma norma que habilite empregadores a registar ou avaliar sem registo a temperatura corporal dos trabalhadores estamos perante a violação do artigo 59.º, n.º 1, alínea c) e do artigo 9.º do RGPD. No primeiro caso, consideramos relevante entender que a saúde foi aditada na IV revisão constitucional, justificando-se por representar (…) uma obrigação que impende sobre a entidade empregadora de proporcionar ao trabalhador as condições de trabalho mais conformes com a prevenção da doença, seja de índole profissional ou outra. Existindo autoridade competente para proceder à avaliação de dados de saúde de trabalhadores, entendemos ser invasiva a intervenção de entidades empregadoras na recolha de dados sensíveis, com ou sem registo formal, com ou sem fundamento no consentimento. (…) Diferente será a situação em que um trabalhador esteja infetado dentro da organização. Nesse caso pensamos que a solução adequada passa por conservar o registo, não lhe dando publicidade junto dos demais trabalhadores, mas informando-os de que existiu um caso positivo. Parece ser esse o sentido, no caso português, da Orientação n.º 6/2020, de 26 de fevereiro da Direção-Geral de Saúde. Para cumprir a citada Orientação, deve ser criado, também, um espaço de isolamento do trabalhador que apresente sintomas da patologia." Com críticas bastante incisivas, partido da afirmação que "a norma legal não contém o grau de precisão e previsibilidade que, num Estado de Direito, se exige a qualquer norma restritiva de direitos, liberdades e garantias", cfr. a resposta da CNPD ao Requerimento 19/XIV (1.ª), subscrito pelo Deputado Telmo Correia, do Grupo Parlamentar do CDS-PP, sobre orientações da CNPD em relação à medição da temperatura corporal dos trabalhadores, datada de 12 de Maio de 2020, pp. 10-11, acessível em https://www.cnpd.pt/home/covid19/rp19-xiv-1ei-a.pdf (acedido em 15 de Maio de 2020).

6. Cfr. https://www.cnpd.pt/home/covid19/covid19.htm (acedido em 15 de Maio de 2020). As orientações emanadas pela CNPD referem-se a diferentes temáticas: (i) orientações sobre recolha de dados de saúde dos trabalhadores, datadas de 23 de Abril de 2020; (ii) orientações sobre divulgação de informação relativa a infetados por Covid-19, datadas de 22 de Abril de 2020; (iii) orientações sobre o controlo à distância em regime de teletrabalho, datadas de 17 de Abril de 2020 e (iv) orientações para utilização de tecnologias de suporte ao ensino à distância, datadas de 8 de Abril de 2020. Figura ainda (v) a resposta da CNPD ao Requerimento 19/XIV (1.ª), subscrito pelo Deputado Telmo Correia, do Grupo Parlamentar do CDS-PP, sobre orientações da CNPD em relação à medição da temperatura corporal dos trabalhadores, datada de 12 de Maio de 2020, bem como a publicação de (vi) Directrizes n.º 4/2020 sobre a utilização de dados de localização e ferramentas de *contact tracing* no contexto do surto de COVID-19, aprovadas pelo Comité Europeu para a Proteção de Dados e ainda (vii) um comunicado sobre a utilização de sistemas de videovigilância e de alarmística por entidades de segurança privada, datado de 2 de Abril de 2020, onde a CNPD conclui que "o estado de emergência decretado não alterou as atribuições e as competências públicas, pelo que se mantêm centralizadas no Estado as funções de controlo de entrada e deslocação em território nacional, estando vedada à Administração Pública Local e às entidades privadas a utilização de meios de captação de imagens e som no espaço público para esta finalidade."

Mas, antes desta análise, há um ponto prévio que deve ser esclarecido.

Ao contrário do que se poderá concluir quanto a outras normas de direitos fundamentais, não houve propriamente um regime aplicável à protecção de dados em período de normalidade constitucional e um regime diverso em período de emergência. É verdade que o Decreto do Presidente da República n.º 17-A/2020, de 2 de abril, que renovou o estado de emergência (anteriormente decretado pelo Decreto do Presidente da República n.º 14-A/2020, de 18 de março) veio prever, no elenco de direitos parcialmente suspensos – cfr. alínea *h*) do artigo 4.º – a suspensão do direito à proteção de dados pessoais, nos seguintes termos: "as autoridades públicas competentes podem determinar que os operadores de telecomunicações enviem aos respetivos clientes mensagens escritas (SMS) com alertas da Direção-Geral da Saúde ou outras relacionadas com o combate à epidemia", enunciado normativo que veio a ser replicado no Decreto do Presidente da República n.º 20- A/2020, de 17 de abril, o qual renovou, pela última vez, o estado de emergência. Esta suspensão não figurava, porém, no Decreto do Presidente da República n.º 14-A/2020, de 18 de março, que declarou o estado de emergência com efeitos a 19 de março de 2020.

Não obstante, nem o Decreto n.º 2-B/2020, de 2 de abril, nem o Decreto n.º 2-C/2020, de 17 de abril – os quais regulamentaram a primeira e a segunda renovações do estado de emergência – adoptaram disposições específicas de concretização da mencionada suspensão – pese embora deles conste uma norma sobre o acesso a dados anonimizados do Sistema Nacional de Vigilância Epidemiológica para investigação científica (cfr. o artigo 39.º e 42.º, respectivamente[7]).

Este primeiro ponto justifica-se precisamente porque a única norma da Constituição que versa directamente sobre protecção de dados é a que resulta do artigo 35.º, em particular do seu n.º 4, remetendo em qualquer caso para a lei.

Por outro lado, o regime nacional de protecção de dados encontra-se, desde 2018, plenamente alinhado com o dos outros Estados-membros da União Europeia, visto que qualquer operação de tratamento de dados tem de respeitar o Regulamento UE 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD), bem como, no quadro interno, a Lei n.º 58/2019, de 8 de agosto, que procura executá-lo.

Assim, qualquer análise sobre a validade de operações de tratamento de dados realizadas em período de estado de emergência não poderá ter uma resposta diferente à que será dada à mesma questão em estado de normalidade constitucional

7. "A Direção-Geral da Saúde disponibiliza à comunidade científica e tecnológica portuguesa o acesso a microdados de saúde pública relativos a doentes infetados pelo novo coronavírus SARS--CoV -2 e a pessoas com suspeita de COVID-19, devidamente anonimizados e sem possibilidade de identificação do respetivo titular, que se encontrem na posse da Direção-Geral da Saúde ou sob a sua responsabilidade", assim correspondendo a um pedido reiterado da comunidade científica. Sobre estas normas, as *guidelines* aplicáveis (Guidelines 3/2020, do Comité Europeu de Proteção de Dados) e a eventual desconformidade do procedimento seguido com o RGPD, cfr. A. Sousa Pinheiro, "A COVID-19 e a proteção de dados pessoais", Observatório Almedina, 28 de abril de 2020.

– seja ela a licitude da medição da temperatura corporal dos trabalhadores, da utilização de *drones* ou câmaras de videovigilância para vigiar deslocações de cidadãos, da admissibilidade de recurso a aplicações que recorram a dados de localização para apoiar a resposta à pandemia, modelando a propagação do vírus – de modo a avaliar a eficácia global das medidas de confinamento – ou que promovam o rastreamento de contactos, notificando os indivíduos de que estiveram próximos de um portador confirmado do vírus, visando em ambos os casos rapidamente cortar as cadeias de contágio[8]. Esta a conclusão a que se terá de necessariamente chegar, visto o regime aplicável ao tratamento de dados pessoais não ser constitucionalmente densificado, mas decorrer do regime europeu de protecção de dados, que contém inclusive normas, como a do artigo 23.º do RGPD, aplicáveis às limitações que os Estados-membros poderão impor ao regime de protecção de dados que decorre do RGPD[9].

O regime aplicável às restrições ao direito à protecção de dados pessoais é, por conseguinte, o mesmo, quer em estado de normalidade, quer em estado de excepção constitucional.

2. Aplicações de rastreabilidade de contactos (*contact tracing*): corona *apps*

Foi já objecto de ampla divulgação quer o documento *Joint European Roadmap towards lifting COVID-19 containment measures* (documento 2020/C 126/01, da Comissão[10]), quer a Declaração sobre o tratamento de dados pessoais no

8. Cfr., com mais detalhe, https://www.who.int/publications-detail/contact-tracing-in-the-contextof-covid-19 (acedido em 15 de Maio de 2020).

9. E mesmo neste âmbito, com limites. Como refere o artigo 23.º, apenas se aplicará às obrigações e aos direitos previstos nos artigos 12.º a 22.º e no artigo 34.º, bem como no artigo 5.º, na medida em que tais disposições correspondam aos direitos e obrigações previstos nos artigos 12.º a 22.º, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar os objectivos previstos no próprio artigo 23.º. Sobre a protecção de dados pessoais relacionada com a COVID-19, cfr. o artigo de A. Sousa Pinheiro de 19 de Abril de 2020, disponível em https://www.jornaldenegocios.pt/opiniao/colunistas/detalhe/20200419-1730-a-covid-19-e-a-protecao-de-dados-pessoais, (acedido em 15 de Maio de 2020), afirmando "Conclui-se, desta forma, que qualquer direito integrado na proteção de dados pessoais – direitos de informação, apagamento, oposição, acesso, retificação, portabilidade e a decisões baseadas na definição de perfis – pode ser afetado de forma proporcional no contexto de uma pandemia." Porém, a referida afectação terá, ainda assim, de levar em conta o regime europeu de protecção de dados, não podendo o legislador nacional, em sede de estado de excepção, afastar unilateralmente o respectivo regime, sem que as restrições que imponha – independentemente da figura jurídico-constitucional a que recorra (*suspensão* ao abrigo de um estado de excepção ou *restrição*) – respeitem o regime decorrente do RGPD. Cfr., com mais desenvolvimento, A. Sousa Pinheiro, "A COVID – 19 e a proteção de dados pessoais", Observatório Almedina, 28 de abril de 2020, "Ao contrário do que ocorre nas constituições dos Estados-membros, a legislação europeia, particularmente o RGPD, não prevê regimes de exceção que conduzam a regimes de emergência que, no limite, pudessem conduzir à suspensão do Regulamento ou de algumas das suas disposições. O que se encontra previsto, como veremos, respeita a regras habilitantes de restrições aos direitos previstos no RGPD e em legislação europeia de proteção de dados."

10. Acessível em https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf, o qual prevê, no ponto 5.2, p. 6, expressamente que "The use of such mobile applications should be voluntary for individuals,

contexto do surto de COVID-19, adotada pelo Comité Europeu de Proteção de Dados a 19 de Março de 2020, quer ainda as directrizes sobre a utilização de dados de localização e ferramentas de *contact tracing* no contexto do surto de COVID-19, adoptadas pelo Comité Europeu para a Protecção de Dados a 21 de Abril de 2020[11], confluindo no sentido de as referidas aplicações serem de adesão voluntária e de o tratamento de dados ter necessariamente de ser feito de forma anonimizada[12] – pois "o vírus não discrimina, mas o seu impacto sim"[13].

Depois de alguma discussão na comunicação social, ficou esclarecido que a aplicação a ser implementada em Portugal, integrada na iniciativa Monitorcovid19.pt e desenvolvida pelo INESC TEC[14], será uma plataforma de uso voluntário (ou seja, o utilizador terá de dar o seu consentimento, ao fazer voluntariamente o *download* da *app*), a qual permite aos utilizadores interessados descobrir casos de contacto próximo com infectados por COVID-19 e que utilizará apenas a tecnologia Bluetooth[15] – embora, para que seja eficaz

---

based on users' consent and fully respecting European privacy and personal data protection rules."

11. Diretrizes n.º 4/2020, difundidas em Portugal pela CNPD e acessíveis em https://www.cnpd.pt/home/orientacoes/Diretrizes_4-2020_contact_tracing_covid_with_annex_en_PT.pdf (acedido em 15 de Maio de 2020).

12. Sobre estes limites, cfr. também https://www.aclu.org/report/aclu-white-paper-limits-location-tracking-epidemic?redirect=aclu-white-paper-limits-location-tracking-epidemic, (acedido em 15 de Maio de 2020), analisando diferentes modelos tecnológicos e optando pelo uso agregado de dados. A mencionada Comunicação *Joint European Roadmap towards lifting COVID-19 containment measures*, no já referido ponto 5.2, p. 6, defende, sem margem para dúvidas, que "The use of such mobile applications should be voluntary for individuals, based on users' consent and fully respecting European privacy and personal data protection rules." e que "Tracing close proximity between mobile devices should be allowed only on an anonymous and aggregated basis, without any tracking of citizens, and names of possibly infected persons should not be disclosed to other users. Mobile tracing and warning applications should be subject to demanding transparency requirements, be deactivated as soon as the COVID-19 crisis is over and any remaining data erased", concluindo mesmo que "Such data, if pooled and used in anonymised, aggregated format in compliance with EU data protection and privacy rules, could contribute to improve the quality of modelling and forecasting for the pandemic at EU level".

13. Cfr. A. Donald e P. Leach, "Human Rights – The Essential Frame of Reference in the Global Response to COVID-19", *VerfBlog*, 2020/5/12, https://verfassungsblog.de/human-rights-the-essential-frame-of-reference-in-the-global-response-to-covid-19/ (acedido em 15 de Maio de 2020).

14. Ainda sem data de lançamento à data de conclusão deste texto. Recorre ao protocolo *open-source* DP-3T (*Decentralized Privacy-Preserving Proximity Tracing*), fazendo o INESC TEC/FDUP parte de um consórcio internacional onde se integram também outros peritos de tecnologia, juristas, engenheiros e epidemiologistas, com o objectivo de impedir que o recurso a esta tecnologia leve a uma maior vigilância por parte dos governos e consequentemente a um ataque ao Estado de Direito (outras entidades parte do consórcio são, por exemplo, a University College London, as Universidades de Oxford, Turim e Salerno e a Universidade de Stanford).

Sobre o consórcio por detrás da referida aplicação, cfr. https://github.com/DP-3T/documents. O protocolo DP-3T integrava originalmente o projecto PEPP-PT (*Pan-European Privacy-Preserving Proximity Tracing*), tendo-se entretanto desvinculado do mesmo, por este se tratar de um sistema de servidor centralizado.

15. A tecnologia Bluetooth permite a comunicação sem fios entre equipamentos, pelo que o telemóvel do utilizador que descarregue voluntariamente a aplicação emitirá um identificador anónimo, composto por algarismos aleatórios, que serão rotativos. Será através do cruzamento destes identificadores anónimos que será possível perceber se o utilizador esteve próximo de

no rastreio dos contágios, a *app* tenha de ser instalada por 60% dos utilizadores (percentagem que está alinhada com o nível expectável de eficácia em outros países). Na apresentação pública da aplicação foi salientado que a mesma não partilhará dados sobre o utilizador e não recorrerá à localização do dispositivo, cumprindo "escrupulosamente as leis europeias e nacionais de proteção de dados"[16].

Estando a sua eficácia dependente de uma adesão expressiva da sociedade, gerando uma sensação de "falsa segurança" e não sendo impossível – como já reconhecido pelo consórcio que está a desenvolver a aplicação – o surgimento de casos de falsos positivos, a obrigatoriedade pelo Estado da imposição de utilização da aplicação sempre poderia suscitar dificuldades face ao princípio da *aptidão* ou da *idoneidade*, enquanto subprincípio do princípio da proibição do excesso[17], argumento que também aponta, assim, a favor do seu carácter voluntário.

3. Orientações sobre divulgação de informação relativa a infetados por COVID-19: o tratamento de dados pessoais na luta contra pandemia dados pessoais na luta contra pandemia

3.1. A Administração Pública e o tratamento de dados pessoais: fundamentos de licitude

alguém infectado. De acordo com a equipa que está a desenvolver a aplicação, os dados aleatórios da *app*, quando descontextualizados, "são como lixo", ou seja, não será possível, através dos identificadores anónimos que a aplicação emite, identificar a pessoa em concreto, para além de a aplicação poder ser desligada a qualquer momento. Sobre as vantagens das *apps* com recurso a Bluetooth, cfr. https://www.reuters.com/article/us-health-coronavirus-apps/bluetooth-phone-apps-for-tracking-covid-19-show-modest-early-results-idUSKCN2232A0 e sobre o funcionamento da tecnologia, cfr. o documento conjunto da Apple e Google, em https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.0.pdf (Maio de 2020), em modo "FAQ's", respondendo a algumas das principais questões sobre o uso de aplicações de rastreamento de contactos com recurso a tecnologia Bluetooth – cfr. em especial o esquema da p. 4. (acedido em 15 de Maio de 2020).

16. Para mais detalhes, cfr. https://www.publico.pt/2020/04/27/ciencia/noticia/apresentada-hoje-aplicacao-telemovel-rastreio-contagio-covid19-1914036 (acedido em 15 de Maio de 2020).

17. Por todos, J. Reis Novais, *Princípios Estruturantes de Estado de Direito*, Coimbra, Almedina, 2019, pp. 98-110. A exigência de respeito pelo princípio da proibição do excesso por parte das medidas implementadas em sede de estado de excepção não pode deixar de ser também uma exigência material das restrições em matéria de protecção de dados pessoais – como seria, aliás, em período de normalidade. Sintetizando, cfr. A. Sousa Pinheiro, "A COVID – 19 e a proteção de dados pessoais", Observatório Almedina, 28 de abril de 2020, "Os tratamentos de dados pessoais em estado de emergência, que implicam necessariamente restrições a direitos fundamentais (máxime ao direito à proteção de dados pessoais, previsto no artigo 8.º da Carta Europeia de Direitos Fundamentais) devem obedecer, nomeadamente, ao princípio da proporcionalidade e ao respeito do conteúdo essencial dos direitos afetados – artigo 52.º, n.º 1 da Carta Europeia de Direitos Fundamentais – acompanhado pelo artigo 9.º, n.º 2, alínea g) do RGPD" e especificamente quanto a este problema, "Em estado de pandemia a restrição de direitos fundamentais apresenta-se inevitável, porém como em qualquer situação deve encontrar-se justificada quanto à sua proporcionalidade e ausência de excesso. Nas leituras feitas apresentam-se as vantagens do controlo e monitorização de indivíduos no contexto da COVID-19, mas não abundam as explicações sobre a necessidade insuprível da utilização das apps."

A luta contra a pandemia de COVID-19, sendo naturalmente um objectivo do Estado Português e convocando o recurso a meios aptos à prossecução desse objectivo, não apaga porém – como julgamos ter ficado assente *supra* – o respeito pelo regime de tratamento de dados pessoais decorrente do RGPD, independentemente de o direito à protecção de dados estar *plenamente em vigor* ou *suspenso* parcialmente em virtude da declaração do estado de emergência.

Assim é porque, quer as aplicações de rastreamento de contactos já analisadas, quer a divulgação de informação relativa a infectados por COVID-19, implicam uma ou várias operações de tratamento de dados, nos termos do n.º 2 do artigo 4.º do RGPD e convocam ainda o regime especial da licitude de tratamento[18] previsto no RGPD para o tratamento de dados relativos à saúde[19], nomeadamente o artigo 9.º do RGPD.

Ora, sendo incontestável que também as autoridades públicas estão submetidas ao RGPD e à Lei n.º 58/2019, de 8 de Agosto – aliás, o direito da protecção de dados surgiu inicialmente para regular o tratamento da informação pessoal por parte de autoridades públicas, quando os meios tecnológicos começaram a adquirir maior relevância, visando sobretudo o Estado e as grandes empresas, tendo como efeito apenas reflexo a protecção dos titulares de dados[20] – o regime decorrente do RGPD aplicar-se-á naturalmente também ao tratamento de dados pela Administração Pública[21].

Por conseguinte, o tratamento de dados pessoais pela Administração Pública – central, regional ou autárquica – terá de ser fundamentado no artigo 6.º do RGPD e, especificamente quanto a dados relativos à saúde, no artigo 9.º do RGPD – ou seja, para ser lícito, terá de ser justificado no âmbito de um dos fundamentos de licitude aí previstos.

Relativamente ao artigo 6.º, importa fazer algumas precisões: embora este preveja, para além do tratamento baseado no *consentimento* do titular dos dados (cfr. a alínea *a*) do n.º 1), o tratamento necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito (alínea *c*) e também o tratamento quando for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular (alínea *d*) e ainda se for necessário

18. Referir este ponto – o da licitude do tratamento – não significa, evidentemente, esquecer a conexão com os princípios relativos ao tratamento de dados pessoais, decorrentes do artigo 5.º do RGPD, a saber: i) licitude, lealdade e transparência; ii) limitação das finalidades; iii) minimização dos dados; iv) exatidão; v) limitação da conservação; vi) integridade e confidencialidade e vii) responsabilidade.

19. Nos termos do n.º 15 do artigo 4.º do RGPD os "dados relativos à saúde" são os dados pessoais 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.

20. Cfr. A. Barreto Menezes Cordeiro, *Direito da Protecção de Dados – À luz do RGPD e da Lei n.º 58/2019*, Coimbra, Almedina, 2020, p. 39.

21. O artigo 2.º da lei de execução esclarece que a mesma é aplicável ao tratamento de dados pessoais realizados em território nacional, *independentemente da natureza pública* ou privada do responsável pelo tratamento ou subcontratante e representantes, *mesmo que o tratamento de dados pessoais seja efetuado em cumprimento de obrigações legais ou no âmbito da prossecução de missões de interesse público*.

ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento (alínea *e*), estes diferentes fundamentos de licitude não serão todos convocáveis em concreto[22].

Em primeiro lugar, o consentimento do titular de dados perante a Administração Pública não é, normalmente, considerado válido como fundamento para o tratamento de dados pessoais pela Administração Pública, como explicita o considerando (43) do RGPD[23]. Podendo eventualmente haver margem para o fundamento de licitude assentar numa obrigação contratualmente prevista (cfr. a alínea *b*) do artigo 6.º) será muito mais frequente o fundamento para a licitude do tratamento pela Administração Pública decorrer da alínea *c*).

Neste caso, será a lei que determinará a finalidade do tratamento, bem como as especificações, tipos de dados, limitações, entidades a que a informação poderá ser fornecida, prazo de conservação e outras medidas destinadas a garantir um tratamento lícito e leal – em decorrência, aliás, do princípio da legalidade[24]. Isto significa que a Administração Pública apenas deve proceder ao tratamento de dados no exercício das suas funções se estiver devida e legalmente autorizada a fazê-lo, mediante uma autorização legal suficientemente pormenorizada e específica.

Embora a alínea *d)*, na referência que faz a interesses vitais, parecesse a mais adequada a fundamentar qualquer tratamento de dados relativo a infetados por COVID-19, justamente por visar a luta contra a pandemia – aspecto que aparece, aliás, mencionado no considerando (46), que expressamente refere a monitorização de epidemias[25] – é um fundamento de licitude que só pode ter lugar

22. "Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento do titular dos dados em causa ou noutro fundamento legítimo, previsto por lei, quer no presente regulamento quer noutro ato de direito da União ou de um Estado-Membro referido no presente regulamento, incluindo a necessidade de serem cumpridas as obrigações legais a que o responsável pelo tratamento se encontre sujeito ou a necessidade de serem executados contratos em que o titular dos dados seja parte ou a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar"- cfr. o Considerando (40) do RGPD, também reiterado pelo artigo 8.º da Carta dos Direitos Fundamentais da União Europeia. Cfr. A. Sousa Pinheiro *et al*., *Comentário ao Regulamento Geral de Protecção de Dados*, Coimbra, Almedina, 2018, pp. 212-227.

23. "A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um *desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa*. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução."

24. Cfr., a este propósito, o considerando (45) do RGPD.

25. "O tratamento de dados pessoais também deverá ser considerado lícito quando for necessário à proteção de um interesse essencial à vida do titular dos dados ou de qualquer outra pessoa singular. Em princípio, o tratamento de dados pessoais com base no interesse vital de outra pessoa singular só pode ter lugar quando o tratamento não se puder basear manifestamente

quando o tratamento não se puder basear manifestamente noutro fundamento jurídico, como o próprio considerando esclarece; por outro lado, o mesmo considerando enquadra a monitorização de epidemias como servindo também importantes interesses públicos, o que aponta para a aplicabilidade, apenas, da alínea *e*) do n.º 1 do artigo 6.º[26].

Especificamente quanto ao tratamento de dados relativos à saúde, o RGPD prevê derrogações à proibição de tratamento desta categoria especial de dados pessoais nas seguintes situações: (i) consentimento (alínea *a*); (ii) protecção dos interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento (alínea *c*) e (iii) se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados (alínea *g*)[27].

Qualquer das causas de licitude impõe, não obstante, a demonstração da *necessidade* do tratamento, enquanto decorrência do princípio da proporcionalidade, aplicável ao tratamento de dados pessoais.

Sendo a publicação dos dados naturalmente importante para a prossecução do interesse da transparência da informação, particularmente intenso quando está

---

noutro fundamento jurídico. Alguns tipos de tratamento podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo, se o tratamento for necessário para fins humanitários, incluindo a *monitorização de epidemias* e da sua propagação ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana."

26. A alínea *f*) não é aplicável ao tratamento de dados por entidades públicas, como o artigo 6.º, n.º 1 esclarece (a tradução portuguesa refere "por via electrónica", mas trata-se de um lapso, que não se encontra nem na versão inglesa, nem na francesa – assim, a alínea *f*) não será aplicável ao tratamento de dados efectuado por autoridades públicas na prossecução das suas atribuições, o que é aliás confirmado pelo considerando (47): "Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas atribuições".

27. Também apontando para estes fundamentos, cfr. A. Sousa Pinheiro, "A COVID – 19 e a proteção de dados pessoais", Observatório Almedina, 28 de abril de 2020, «Assim, em situação de pandemia, para além de os tratamentos de dados estarem basicamente fundados na lei, no interesse público e na proteção de interesses vitais, existe a necessidade de cumprir o princípio da proporcionalidade na definição de restrições a direitos integrados na proteção de dados pessoais. Por outro lado, o RGPD prevê – no artigo 23.º – uma regra específica sobre restrições que devem, na UE ou em cada Estado, revestir forma legal (de acordo com os respetivos ordenamentos jurídicos) e respeitar os princípios já citados. O fundamento das restrições à face deste artigo encontra-se no n.º 1, alínea e), quando se referem "objetivos importantes de saúde pública". Reforçando a aplicação do artigo 23.º compete verificar que o Considerando (73) alude às restrições a qualquer direito integrado na órbita da proteção de dados na medida em que aquelas "sejam necessárias e proporcionais numa sociedade democrática. Conclui-se, desta forma, que qualquer direito integrado na proteção de dados pessoais – direitos de informação, apagamento, oposição, acesso, retificação, portabilidade e a decisões baseadas na definição de perfis – pode ser afetado de forma proporcional no contexto de uma pandemia.»

em causa a disseminação de uma pandemia[28], já do ponto de vista do princípio da proteção de dados pessoais e do direito à privacidade, não esquecendo a própria garantia da segurança jurídica, a divulgação deve estar baseada em lei que a permita e – se necessário – que especifique quais os dados a publicar, a finalidade da publicação e as garantias inerentes.

Ora, embora elaboradas a propósito da Proposta de Lei n.º 120/XIII – que veio a dar origem à Lei n.º 58/2019, de 8 de Agosto – é importante analisar algumas das objecções então formuladas pela CNPD, por permitirem justamente melhor compreender a aplicabilidade dos fundamentos de licitude ao tratamento de dados pessoais por parte da Administração Pública. Refiro-me às objecções formuladas quanto ao artigo 23.º, relativo à reutilização de dados pela Administração Pública e que, não tendo sido suprimido pelo legislador, veio a ser uma das disposições que a CNPD, na deliberação 2019/494, de 3 de Setembro de 2019 – e em coerência com as objecções que já anteriormente formulara – deliberou desaplicar.

A primeira crítica assenta na referência que o artigo 23.º da lei de execução faz a que as finalidades diferentes têm de corresponder a um interesse público, "como se tal constituísse uma garantia suficiente da tutela dos direitos dos cidadãos ou um fundamento suficiente para excecionar o princípio consagrado na alínea *b*) do n.º 1 do artigo 5.º do RGPD".

Na realidade, "todas as finalidades de tratamentos de dados realizados por entidades públicas só podem ser de interesse público, porque a função da administração pública é exclusivamente a da prossecução de interesses públicos", ainda que – no que constitui uma precisão importante – "as entidades públicas só poderem prosseguir os interesses públicos que coincidam com as respetivas atribuições legalmente definidas, e não todo e qualquer interesse público"[29], o que ajuda a conformar a aplicabilidade da própria alínea *e*) do artigo 6.º, n.º 1, do RGPD – o interesse público terá de ser enquadrado no âmbito das atribuições legalmente definidas da pessoa colectiva em causa.

A segunda crítica que a CNPD faz no referido parecer à Proposta de Lei n.º 120/XIII, reporta-se ao princípio da finalidade e permite compreender que "uma norma do direito nacional que admita a utilização de dados pessoais dos cidadãos para qualquer fim de interesse público viola ostensivamente o princípio da finalidade e o disposto na alínea b) do n.º 1 do artigo 5.º do RGDP" e que, por

28. Os dados disponibilizados publicamente pela DGS são fonte da informação para os órgãos de comunicação social e para entidades públicas e privadas que entendem dar-lhe visibilidade, de entre as quais se destacam os sítios institucionais dos municípios, como explica a CNPD nas "Orientações sobre divulgação de informação relativa a infetados por Covid-19" a 22 de Abril de 2020

29. Parecer disponível em http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679626d56304c334e706447567a4c31684a53556c4d5a57637651303394e4c7a4644451554e4554456376524739 6a5a57593359544d794f4330325a44526c4c54526c4e546b74596a41304e4331694e54426d4f5449314d6a64684d7a45756347526d&fich=cef7a328-6d4e-4e59-b044-b50f92527a31.pdf&Inline=true (consultado em 15 de Maio de 2020).

outro lado, o interesse público como fundamento da licitude do tratamento de dados pessoais tem de corresponder a um interesse "qualificado, «importante», quando em causa estejam certas categorias especiais de dados, ou seja legitimando a recolha e subsequentes operações sobre dados pessoais quando justificadas por um específico interesse público." Não é, portanto, qualquer missão ou objectivo que a Administração vise prosseguir que pode ser enquadrado num tratamento necessário "ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento".

3.2. O tratamento de dados efectuado pelas autarquias locais em estado de excepção: a divulgação de dados de saúde relativos a infectados por COVID-19

Como tive oportunidade de avançar *supra*, as "Orientações sobre divulgação de informação relativa a infetados por Covid-19" emanadas pela CNPD a 22 de Abril de 2020 – em pleno estado de emergência – constituem um documento importante para confirmar que (i) não existe um regime excepcional de protecção de dados, mesmo em período de estado de emergência, sendo necessário que as eventuais restrições respeitem também o regime consagrado no RGPD e que (ii) não havendo nenhuma alteração legal relativa ao regime aplicável ao tratamento de dados, as conclusões que daí se retiram quanto ao tratamento de dados pessoais por parte da Administração Pública e, em particular sobre a aplicação da alínea *e*) do n.º 1 do artigo 6.º do RGPD, serão também relevantes em cenário de normalidade constitucional.

As referidas orientações foram emanadas por terem sido dirigidas à CNPD queixas de cidadãos que, após diagnóstico de COVID-19, viram "os seus dados pessoais, de identificação e contacto, incluindo de crianças, expostos nas páginas e nas redes sociais da responsabilidade da autarquia local, após a confirmação do diagnóstico de Covid-19. Algumas autarquias locais não expõem os dados pessoais dos infetados, mas disponibilizam informação discriminada por freguesia, sem acautelarem o diminuto número de casos, os quais facilmente reconduzem, especialmente em pequenas localidades, à identificação dos doentes."[30]

Após relembrar (embora não se tratasse de averiguar o modo como a informação chegara às autarquias) que "tanto os serviços de saúde da área, como as autoridades locais ou regionais de saúde, continuam obrigados a sigilo, seja por força das regras deontológicas a que estão sujeitos, seja pelas obrigações legais a que estão adstritos, de entre as quais se encontram as regras de proteção de dados" a CNPD vem esclarecer que "as autarquias locais não podem publicar dados de saúde com identificação das pessoas a quem os mesmos dizem respeito."

Existem duas razões para tal: (i) em primeiro lugar, por se tratar de informação sujeita a um regime jurídico especialmente protegido, por corresponder a

30. Como resulta da nota de rodapé 1 das referidas orientações, a própria DGS não disponibiliza informação desagregada quando o número de infetados no concelho é inferior a três.

uma categoria de dados pessoais que é suscetível de gerar ou promover a estigmatização e a discriminação dos respetivos titulares (como visto *supra*, aplicando-se o n.º 1 do artigo 9.º do RGPD).

Pergunta-se, não obstante, se poderiam as autarquias locais invocar a necessidade de conhecer e divulgar dados de saúde identificados ou individualizados para a prossecução da sua missão genérica de garantir a saúde e a proteção civil das populações locais. Ora, como visto no ponto anterior, também o tratamento de dados pessoais pela Administração Pública terá de ser enquadrado num dos fundamentos de licitude do tratamento previstos no RGPD e, tratando-se de dados de saúde, num dos fundamentos especialmente previstos no artigo 9.º. Face à verificação de que o fundamento em causa – a alínea *i*) do n.º 2 do artigo 9.º – convocaria a existência de um interesse público "importante" e tendo em conta o que já foi exposto, seria ainda essencial – dado tratar-se de uma entidade pública – que esse tratamento dos dados estivesse previsto em norma legal, que igualmente especificasse os direitos e interesses dos titulares dos dados, norma inexistente em concreto – conclusão que também se colocaria caso o fundamento aplicável fosse o da alínea *g)* do n.º 1 do artigo 9.º.

A outra hipótese de licitude do tratamento – o consentimento – se já apresentava várias fragilidades quando estava em causa uma relação entre um particular e a Administração Pública fora do contexto da pandemia, mais fragilizada sai atendendo "à evidente situação de vulnerabilidade das pessoas que se encontram contaminadas pelo vírus, bem como a sua situação de dependência da intervenção das autoridades públicas", o que prejudica a emissão de um consentimento livre[31].

O principal problema da verificação do requisito da licitude fundada no interesse público surge, assim, da conjugação da necessidade de o mesmo estar legalmente previsto e enquadrar-se nas atribuições da pessoa colectiva – pois, como demonstra a CNPD, "é duvidoso que a prossecução do interesse público de saúde pública seja diretamente atribuição das autarquias locais, pelo menos na vertente de prevenção e combate de uma concreta epidemia, em face do estatuído nos artigos 2.º e 16.º do Decreto-Lei n.º 23/2019, de 30 de janeiro[32] (com eventual ressalva de decisão da autoridade nacional de saúde pública no sentido de as encarregar de algumas das suas tarefas)".

Finalmente, (ii) a publicação de dados pelas autarquias locais é ainda desconforme com o regime decorrente do RGPD já não por causa da licitude do tratamento – relativamente ao *fundamento* da mesma – mas pela violação do subprincípio da necessidade[33].

31. Nos termos do n.º 11 do artigo 4.º e da alínea *a)* do n.º 2 do artigo 9.º, do RGPD.

32. Concretiza o quadro de transferência de competências para os órgãos municipais e para as entidades intermunicipais no domínio da saúde

33. "Uma tal divulgação pública sempre se terá por desproporcionada, pelo impacto negativo que tem na vida das pessoas contaminadas – reitera-se, algumas das quais crianças –, com restrição excessiva dos seus direitos fundamentais, sem que se possa afirmar que a vantagem diretamente decorrente dessa divulgação, a existir, não é alcançável por outras vias menos lesivas e intrusivas da vida privada das pessoas", juízo que também é aplicável à divulgação de dados em número inferior a 3 no âmbito de uma freguesia.

Assim, a conclusão das próprias orientações da CNPD sintetiza de forma bastante perceptível que o tratamento de dados pessoais pela Administração Pública – aqui corporizada em autarquias locais, mas aplicável a qualquer outra entidade enquadrada na Administração Pública – só pode ocorrer com um fundamento de licitude que, mesmo que baseado na prossecução do interesse público, terá de (i) ser enquadrado nas atribuições da pessoa colectiva em causa e (ii) estar legalmente previsto, pelo que "A CNPD recorda que as autarquias locais, no âmbito da sua autonomia e do legítimo desempenho da sua missão de garantia da saúde e da proteção civil, se devem abster de adotar iniciativas que impliquem a recolha e a divulgação de dados pessoais dos seus concidadãos quando as mesmas não tenham base legal, nem sejam execução de orientações da autoridade nacional de saúde."

***