

DELIBERAÇÃO/2020/262

I. RELATÓRIO

A Comissão Nacional de Proteção de Dados (CNPD) recebeu várias participações dando conta de vulnerabilidades da ferramenta denominada Trace COVID-19, de acompanhamento de *contact tracing* de doentes em vigilância e autocuidado. O conteúdo das participações apontava para funcionalidades existentes na ferramenta com impacto na segurança e na confidencialidade dos dados pessoais, ao tornar possível a consulta sem aparente limitação no universo disponível e a exportação, sem qualquer controlo, de listagens de dados pessoais para tabelas de Excel.

A CNPD averiguou as situações reportadas, no uso das suas atribuições e competências enquanto autoridade administrativa independente com poderes de autoridade para o controlo dos tratamentos de dados pessoais, conferidos pelas alíneas *f)* e *h)* do n.º 1 do artigo 57.º, conjugado com os n.º 1 e n.º 2 do artigo 58.º, todos do Regulamento (UE) 2016/679, de 27 de abril de 2016 – Regulamento Geral sobre a Proteção de Dados (doravante, RGPD), em conjugação com o disposto no artigo 3.º e na alínea *b)* do n.º 1 e do n.º 2 do artigo 6.º, todos da Lei n.º 58/2019, de 8 de agosto, que executa na ordem jurídica interna o RGPD.

Plataforma Trace COVID-19

A Autoridade Nacional de Saúde emitiu a Norma n.º 4/2020, de 23 de março de 2020, que estabelece os procedimentos a adotar pelos profissionais de saúde dos Cuidados de Saúde Primários e das Equipas de Saúde Pública e Autoridades de Saúde na plataforma Trace COVID-19, a qual tem por objeto “a gestão de doentes em autocuidados e ambulatório” e corresponde a “uma ferramenta de suporte, para que, através de um conjunto de tarefas geradas pelo sistema, implementem o seguimento clínico efetivo e as medidas de Saúde Pública adequadas a doentes com suspeita ou confirmação de COVID-19”.

Existindo informação na página da Internet relativa a esta plataforma¹ que indicava que foi desenvolvida pela SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. (doravante SPMS), foram solicitados a 8 e a 20 de abril vários esclarecimentos a esta entidade, bem como documentação relativa à arquitetura e funcionamento da ferramenta Trace COVID-19

¹ Disponível em <https://tracecovid19.min-saude.pt/>

e ainda a Avaliação de Impacto sobre a Proteção de Dados, prevista no n.º 1 do artigo 35.º do RGPD.

Subsequentemente, foi esclarecido que a SPMS atua neste tratamento de dados pessoais como subcontratante² da Direção-Geral de Saúde (DGS), foi apresentada resposta às questões colocadas e remetidos os seguintes documentos: diagrama de tabelas da base de dados; *DDL script*³ da base de dados; caderno de especificações de requisitos; e manual do utilizador.

Foi efetuada uma diligência a 19 de maio, nas instalações da SPMS para verificar o funcionamento da plataforma e solicitados elementos para a instrução do processo e, finalmente, no dia 22 de maio, para verificar se existia uma vulnerabilidade na consulta dos dados dos doentes.

Da análise dos elementos fornecidos pela SPMS salienta-se que a autenticação na ferramenta Trace COVID-19 está a ser delegada para servidores na *cloud* “da plataforma Azure da Microsoft”. As contas utilizadas são aquelas que os profissionais do Serviço Nacional de Saúde (SNS) e do Ministério da Saúde já detêm, que os identifica nos seus sistemas, permitindo também o acesso ao “email e serviços de produtividade” (Office 365)⁴. As contas estão definidas nos servidores locais de *Active Directory* (AD)⁵ das várias entidades de saúde, são geridas por estas, e são sincronizadas com a AD da *Azure* (AAD)⁶ para permitir o acesso a várias ferramentas disponibilizadas *online*, designadamente à Trace Covid-19.

Para as entidades de saúde privadas são criadas contas “guest”, de acesso exclusivo à ferramenta, na AAD do SNS, sendo a gestão dessas credenciais da responsabilidade das respetivas entidades privadas. A SPMS justifica estas contas “guest” no facto de “alguns utentes quere[re]m ser seguidos pelo seu médico assistente em clínicas/hospitais privados”. Afirmou a SPMS que estas instituições externas ao SNS podem usar a aplicação Trace COVID-19 para realizarem vigilâncias dos seus doentes.

² Cf. alínea 8) do artigo 4.º do RGPD

³ *I.e.*, Sequências de declarações que quando executadas criam a estrutura de uma base de dados.

⁴ *Office 365* refere o conjunto de ferramentas de produtividade *MS Office* disponibilizado online na *cloud Azure*

⁵ *Active Directory* é o sistema criado pela Microsoft que armazena, organiza, e fornece acesso às informações de um diretório central com vista ao acesso a recursos em rede.

⁶ *Azure Active Directory* - serviço de gestão de identidade e acesso baseado na *cloud*

A SPMS remete o critério na atribuição do acesso e os procedimentos de login de cada utilizador da Trace COVID-19 para a “Circular Normativa que vai ser publicada no dia 17 de abril”⁷. Posteriormente, no dia 20 de abril, a SPMS veio afirmar que a Circular Normativa não estaria ainda concluída e que tinha a “expetativa de conseguir emitir na semana passada, no entanto, a Circular ainda está a ser articulada e fechada com a DGS.”. Declara a SPMS que “genericamente, todos os profissionais devem solicitar acesso via ServiceDesk e com autorização expressa do Conselho Clínico ou Conselho de Administração da respetiva instituição”.

No que respeita aos perfis de acesso à ferramenta Trace COVID-19, esclarece a entidade que “existem 3 perfis distintos: Local, Regional, e Nacional, consoante o número de instituições às quais o utilizador tem acesso”. Para a definição do perfil de utilizador “no momento do pedido de atribuição de acesso, a entidade com responsabilidade direta sobre o profissional (...) indica o perfil aplicável.”.

As operações permitidas a todos os perfis são a inserção e atualização de doentes/tarefas/vigilâncias, e a “transferência de utentes entre unidade responsável por vigilância”.

O perfil Local pode aceder aos dados do “respetivo ACeS⁸ e Unidade funcional ou instituição hospitalar”; o perfil Regional acede aos dados dos “ACeS e Unidades Funcionais regionais”; o perfil Nacional acede aos dados de todas as instituições.

A gestão dos acessos, no que respeita à atribuição e alteração dos perfis, cabe à SPMS, estando a informação dos perfis armazenada nos seus servidores localizados no *datacenter* do Porto, local onde também residem os sistemas que suportam a ferramenta e a base de dados.

Quanto a esta matéria, afirma ainda que os perfis são administrados seguindo “princípios de identidade, através de utilizadores únicos e individuais (users nominais) e princípios de acessos mínimos, sendo as contas de privilégios elevados restringida ao mínimo necessário para funções de gestão, administração e operação”.

⁷ Resposta dada no dia 16 de abril, junta ao processo.

⁸ Os Agrupamentos de Centros de Saúde são serviços de saúde com autonomia administrativa, constituídos por várias unidades funcionais, que integram um ou mais centros de saúde.

Para administração da ferramenta Trace COVID-19 existem dois perfis, o de “Admin Local - Utilizadores com acesso à informação nacional e aos Dashboards” e de “Administrador solução - Utilizadores com acesso à gestão e configuração das ferramentas e mecanismos de segurança. Os utilizadores com este perfil terão automaticamente acesso à informação de todos os modelos.”.

É também declarado que na consulta de dados pessoais “existe uma seleção automática e nativa (filtro embutido na aplicação, sem que possa ser afastada pelo utilizador) para que apenas possa consultar os utentes atribuídos/em vigilância pelo respetivo ACES/unidade.”.

Segundo a SPMS “continuam a ser implementados, progressivamente, mecanismos para evitar a alteração de dados identificativos dos utentes, ou que sejam provenientes de integração de informação de outros sistemas, nomeadamente não permitindo alterar os campos de nome, número de SNS, documento de identificação, contacto.”.

No que toca ao relacionamento com outras aplicações, é explicado que atualmente a ferramenta Trace COVID-19 “recebe dados de outros sistemas do SNS, mas (...) não envia dados para outros sistemas de informação (...)”, acrescentando que “são integrados dados oriundos do Registo Nacional de Utentes (RNU), da linha SNS24 e do Registo de Saúde Eletrónico (SER)”. Do caderno de especificação de requisitos conclui-se ser possível a importação de dados de “Ficheiros (flat, xml, excel, csv)”.

Relativamente à importação de dados contidos em ficheiros Excel, vem a SPMS esclarecer que este processo “ainda não está automatizado”, e que o mesmo terá feito sentido no início do projeto, visto que algumas unidades (ACeS e UF) faziam a vigilância recorrendo a ficheiros Excel, acrescentando que “não vemos utilidade nem prioridade no desenvolvimento deste automatismo, neste momento”.

Foi declarado que à data do envio dos documentos à CNPD, a ferramenta Trace COVID-19 tinha 72.375 utilizadores com perfil Local, 27 utilizadores com perfil Regional, e 18 utilizadores com perfil Nacional, nele constando 125.461 utentes em vigilância. Posteriormente, na inspeção de 19 de maio, verificou-se que o n.º de utilizadores era de 73.486 e estavam registados 372.184 utentes em vigilância.

Relativamente aos dados pessoais tratados na ferramenta Trace COVID-19 foram indicados os seguintes: nome; data de nascimento; morada; contacto telefónico e *email*; número de utente e/ou NIF e/ou documento de identificação “(por forma a acomodar utentes sem número de utente)”; estado de vigilância; estado de exame; data de início e fim de vigilância;

origem do utente; localização (domicílio, hospital ou outra); *link* epidemiológico/contacto; registo de óbito. A estes dados acrescem os registados nas vigilâncias: “informação referente a uma vigilância”; “resumo dos sintomas e perguntas efetuadas (ex: Temperatura, Tosse, Dor Garganta, Dor corpo, etc)”; “Observações”; “Cálculo de um score de risco com base na sintomatologia”.

A ferramenta permite a criação de relatórios e *dashboards*⁹ que “não são específicos de uma única área funcional e que cruzam informação [de] Visão Agregada Nacional [e] Indicadores Diários”. Esses documentos produzem indicadores como “Nº de Pessoas em Vigilância”, “Nº de Vigilâncias executadas”, “Nº de Utentes por estado de vigilância”.

Foram dadas informações sobre a transmissão de dados entre o servidor aplicacional¹⁰ e a base de dados e sobre as especificações técnicas.

Quanto às respostas dadas no ponto referente aos registos de auditoria, detetaram-se incongruências, designadamente pelo facto de esta funcionalidade apontar apenas para a “segunda fase”. Foram, por isso, solicitados novos esclarecimentos no dia 20 de abril. No dia seguinte, a informação chegada confirmou a existência desses registos, mas não dos mecanismos capazes da sua consulta – “Podemos não ter sido claros. O mecanismo de auditoria já existe e está já a ser efetuada. O que não existe é a disponibilização da funcionalidade de consulta dos dados recolhidos.”.

Sobre os registos dos acessos (*log* de acessos) à ferramenta Trace COVID-19, foi esclarecido que os mesmos ficavam guardados na AAD. Diferentemente, os registos de atividade aplicacional (*log* aplicacionais) “são guardados na infraestrutura no Datacenter da SPMS no Porto”.

A base de dados da ferramenta Trace COVID-19 é alvo de cópias de segurança (*backups*) diárias, sendo que somente a “equipa de operações e da equipa do datacenter da SPMS” tem “permissão para aceder e gerir o repositório dos backups”.

“Os acessos à base de dados de suporte da ferramenta são restritos à aplicação Trace COVID-19.”.

⁹ Quadros que mostram métricas e indicadores de forma visual, facilitando a compreensão das informações processadas.

¹⁰ Servidor *web* onde se executa a ferramenta Trace COVID-19 e que responde a pedidos dos clientes (*browsers*).

No que toca à avaliação de impacto sobre a proteção de dados solicitada pela CNPD, a SPMS declarou que se encontra “em elaboração à data da recolha dos elementos em análise”, não tendo, até ao presente momento, sido remetida à CNPD.

Quanto aos desenvolvimentos futuros já previstos para esta ferramenta, foi referido o “desenvolvimento e implementação de uma integração com o Sistema Nacional de Vigilância Epidemiológica (SINAVE), para recolha dos dados relativos aos exames laboratoriais, essenciais para a vigilância eficaz do doente”.

A este respeito a SPMS esclareceu “que será contemplada a integração com o SINAVE-Lab e SINAVE-Med; Circuitos automáticos; Contacto e acompanhamento diário junto do cidadão, por forma a permitir a devida sinalização de casos que careçam de outro tipo de cuidados”.

Está ainda previsto o desenvolvimento de uma “funcionalidade de reporte de outcomes clínicos (temperatura; tosse; ...) que integrará com o Trace Covid, para que o profissional de saúde que acompanha o cidadão possa ter acesso aos mesmos”. Essa funcionalidade de “auto-inserção” será incluída na Área do Cidadão do Portal do SNS e os dados aí recolhidos serão integrados na ferramenta Trace COVID-19. Paralelamente, e para a mesma funcionalidade de “auto-inserção”, será desenvolvida uma *app*¹¹.

Aquando da inspeção de 19 de maio, verificou-se que a Trace Covid-19 já integrava com o SINAVE-Lab.

O aproveitamento dos dados da base de suporte à ferramenta Trace COVID-19, findo o período de emergência que justificou a criação dessa ferramenta, está ainda a ser pensado pela DGS.

II. APRECIÇÃO

a) Fundamento de licitude

A DGS assume-se como responsável pelo tratamento, tendo a aplicação sido desenvolvida por determinação direta desta.

A alínea *i*) do n.º 2 do artigo 9.º do RGPD admite o tratamento de dados pessoais de saúde por motivos de interesse público no domínio da saúde pública, com base no direito do

¹¹ Aplicação para dispositivos móveis.

Estado-Membro que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular, em especial o sigilo médico.

Ora, a Lei n.º 81/2009, de 21 de agosto, que institui um sistema de vigilância em saúde pública, vem admitir, no artigo 17.º, um poder regulamentar excecional ao membro do Governo responsável pela área da saúde, sob proposta do Diretor-Geral da Saúde, como autoridade de saúde nacional, para a adoção de medidas indispensáveis em caso de emergência em saúde pública de forma a evitar disseminação da infeção ou contaminação. Por sua vez, o Decreto-Lei n.º 124/2011, de 29 de dezembro, alterado por último pelo Decreto-Lei n.º 152/2017, de 7 de agosto, na alínea *a)* do n.º 2 do artigo 12.º¹², atribui poder à DGS de emissão de normas e orientações em matéria de saúde pública. É neste contexto que o tratamento de dados pessoais designado por Trace Covid-19 encontra a sua previsão na Norma da DGS n.º 4/2020, de 23 de março e atualizada em 25 de abril, com a finalidade de profissionais de saúde gerirem doentes em autocuidados e ambulatório no âmbito da pandemia por Covid-19.

Importa dar nota de que a alínea *i)* do n.º 2 do artigo 9.º do RGPD exige que sejam previstas medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular, em especial o sigilo médico e essas medidas não constam da Norma 4/2020, com exceção da exigência de sigilo.

b) Mecanismo de autenticação

A autenticação na ferramenta Trace COVID-19 está a ser delegada para servidores na *cloud* da plataforma *Azure* da Microsoft, havendo sincronização das contas criadas e geridas nos servidores de AD das várias entidades de saúde com a AD da *Azure*.

A justificação apresentada pela SPMS para esta opção foi a possibilidade de maior abrangência no acesso à ferramenta Trace COVID-19 e porque permite a utilização de contas já usadas no SNS e no Ministério da Saúde (MS) e admite a autenticação a entidades privadas externas à rede privada da saúde. Para além disso, possibilita a concentração da informação de monitorização ao COVID-19, ao agregar, numa única plataforma, a gestão que é feita dos utentes infetados pelas diversas unidades de saúde, espalhadas pelo

¹² Cf. também alíneas *a)* e *b)* do n.º 2 do artigo 2.º do Decreto Regulamentar n.º 14/2012, de 26 de janeiro.



território nacional. Acrescenta que tem intenção de alargar a utilização deste mecanismo de autenticação na plataforma AAD de modo a permitir *single sign on*.

Para a escolha do mecanismo de autenticação importa que se tenha presente que as várias aplicações utilizadas no SNS contêm informação de grande sensibilidade, a qual está sujeita a regras reforçadas de confidencialidade (cf. n.º 3 do artigo 9.º e a alínea *b*) do n.º 1 do artigo 32.º do RGPD); e a Trace COVID-19 não é exceção, na medida em que, pela sua finalidade de gestão de doentes com suspeita ou confirmação de Covid-19 em autocuidados e ambulatório, contém a identificação destes doentes, bem como o seu domicílio ou o local onde se encontram em confinamento.

Ora, se se reconhece que os mecanismos da AD da *Azure* são seguros para garantir a autenticidade da credencial de acesso, não pode deixar de se manifestar perplexidade por não ser utilizado um modelo federado de autenticação para todas as plataformas do SNS, tanto mais que tendo cada instituição a sua própria AD, a solução natural seria a sua federação numa solução distribuída.

E isto porque a opção escolhida implica uma centralização de todos os utilizadores das plataformas do SNS (todos os profissionais de saúde e trabalhadores do SNS) na *Azure*, o que, independente das medidas de segurança adotados pela Microsoft, duplica desnecessariamente a informação dos utilizadores.

A duplicação de informação é sempre um risco (*v.g.*, porque a sincronização pode falhar, porque existem mais pontos onde se pode, ainda que negligentemente, introduzir alterações) e não sendo necessária, viola o princípio da minimização dos dados consagrado na alínea *c*) do n.º1 do artigo 5.º do RGPD.

Acresce que a contratualização da AAD está incluída num pacote “mais geral de fornecimento de vários serviços [...] e segue o contrato-tipo” usado pela Microsoft, que assume neste tratamento de dados pessoais a qualidade de subcontratante (cf. alínea 8) do artigo 4.º do RGPD). Deste modo, o subcontratante, em obediência ao artigo 28.º do RGPD, deveria estar contratualmente vinculado, entre outros, ao tratamento de dados pessoais de acordo com as instruções documentadas do responsável, situação que nos contratos-tipo da Microsoft se tem constatado não ocorrer. Importa, por isso, que o responsável pelo tratamento corrija a situação dando cumprimento ao artigo 28.º do RGPD.

c) Procedimento para a criação de conta de utilizador

Para profissionais de instituições dentro da rede do Ministério da Saúde, os pedidos de acesso à ferramenta Trace COVID-19 são validados pelo serviço de origem e podem ser efetuados numa área reservada no portal *Service Desk* ou, pelo envio de um ofício, emitido pelo Conselho Clínico ou pelo Conselho de Administração da instituição. Os pedidos podem ser feitos para um ou mais utilizadores e são indicadas as suas respetivas contas institucionais.

Para as entidades privadas de saúde com prestação de cuidados no âmbito da Covid-19, o acesso à ferramenta é facultado mediante pedido efetuado pelas instituições a que os profissionais pertencem, incluindo-se no pedido o endereço institucional de *email* dos utilizadores a quem se pretende dar acesso, para envio das respetivas credenciais. A conta é criada diretamente na AAD, pela SPMS, e a plataforma remete um *email* para o endereço do utilizador com instruções para validação da conta.

O responsável pelo tratamento não faz qualquer validação do perfil profissional dos pedidos de acesso, ficando essa responsabilidade do lado da instituição que requer a criação dos acessos.

Ora, este procedimento não garante que utilizadores da Trace COVID-19 sejam efetivamente profissionais de saúde sujeitos a sigilo profissional, o que enfraquece o cumprimento do disposto na alínea *i)* do n.º 2 do artigo 9.º do RGPD. Na verdade, o responsável pelo tratamento não dispõe de qualquer elemento informativo que lhe permita verificar a fiabilidade da informação transmitida pela instituição que requer a criação dos acessos, não tendo forma de confirmar se se trata de um profissional de saúde sujeito a dever de sigilo. Quando é certo que, quanto às instituições públicas do SNS, é possível efetuar uma integração com os sistemas do MS para os utilizadores dessas instituições.

Nestes termos, e tendo em conta que não estão fixadas no ordenamento jurídico nacional, quanto a este tratamento, medidas adequadas e específicas para defesa dos direitos fundamentais e dos interesses do titular dos dados, como exige a alínea *i)* do n.º 2 do artigo 9.º do RGPD, importa criar, pelo menos, um mecanismo que garanta, do lado do responsável pelo tratamento, que o acesso só é conferido a quem seja profissional de saúde sujeito a dever de sigilo profissional, como decorre da mesma norma.



d) Perfis de acesso

As participações recebidas na CNPD referiam a possibilidade de acesso à plataforma sem aparente limitação no universo de informação nela disponível.

Da análise da informação recebida conclui-se, como já se referiu, que existem três perfis distintos: o local, o regional, e o nacional. Para a definição do perfil de utilizador “no momento do pedido de atribuição de acesso, a entidade com responsabilidade direta sobre o profissional (...) indica o perfil aplicável.”.

Ou seja, não é possível afirmar que a totalidade da informação esteja disponível a todos os utilizadores e, com exceção dos utilizadores com perfil nacional, existe uma limitação garantida por um filtro embutido na aplicação, que não pode ser afastada pelo utilizador.

Relativamente ao perfil local, nas instituições do SNS, dentro de cada ACES podem existir unidades funcionais e, dentro destas, subunidades. Quando se trata de um utilizador de uma unidade de saúde como Unidade de Saúde Familiar (USF) ou Unidade de Cuidados de Saúde Personalizados (UCSP), o menor universo de consulta possível engloba os dados referentes a todas as unidades pertencentes ao mesmo agrupamento do centro de saúde onde a sua unidade está inserida. Em suma, um utilizador que exerça a sua atividade numa unidade funcional, dentro de um determinado centro de saúde, terá acesso aos registos dos doentes acompanhados em todas as unidades dos centros de saúde pertencentes ao mesmo ACES.

No caso das entidades privadas, o universo de registos visível não possui a mesma regra das instituições de saúde públicas, sendo mais limitada. Para os grupos de saúde privados, que agregam vários estabelecimentos, cada um deles possui uma área própria na ferramenta Trace COVID-19, e só podem ser consultados pelos profissionais de saúde da instituição que acompanha o doente. Os utilizadores das restantes entidades do grupo não têm acesso a esses dados.

As autoridades de saúde, locais, regionais e nacional, têm também acesso aos registos correspondentes à sua área de competência.

As operações permitidas a todos os perfis são a inserção e atualização de doentes, registo de tarefas e vigilâncias, e a possibilidade de “transferência de utentes entre unidade responsável por vigilância”.

Os utilizadores apenas têm privilégios de acesso e registo de informação e, segundo os SPMS, “continuam a ser implementados, progressivamente, mecanismos para evitar a alteração de dados identificativos dos utentes, ou que sejam provenientes de integração de informação de outros sistemas, nomeadamente não permitindo alterar os campos de nome, número de SNS, documento de identificação, contacto.”.

Assim, conclui-se que, quanto às instituições de saúde públicas, apesar de existirem alguns mecanismos de limitação dos acessos, o modo como a ferramenta está construída permite a partilha dos dados pessoais de todos os doentes registados nas unidades funcionais dependentes de uma instituição hierarquicamente superior, como acontece, por exemplo, no caso dos ACES.

Tendo em conta que um ACES pode ter várias dezenas de unidades funcionais, a ferramenta possibilita o acesso a um utilizador de qualquer uma dessas unidades aos dados pessoais de todos os doentes registados no conjunto das unidades funcionais do mesmo agrupamento. Ora, esta solução não é aceitável por violar o princípio da minimização dos dados, consagrado na alínea *c)* do n.º 1 do artigo 9.º do RGPD. De facto, uma vez que os doentes apenas são acompanhados por uma unidade funcional, torna-se desnecessário que outros utilizadores, fora dessa unidade, tenham acesso a todo universo de doentes do ACES.

e) Dados pessoais tratados

Na consulta dos doentes o utilizador tem acesso aos seguintes dados pessoais: nome, n.º de utente do SNS, contacto telefónico, endereço de *email*, n.º de contribuinte, n.º de cartão do cidadão, n.º de identificação da segurança social, data de nascimento, género, nacionalidade, profissão, habilitações literárias, morada, código postal, localidade postal, distrito, concelho e freguesia, unidade de saúde, temperatura corporal, medicação, tosse, dores musculares, dor de garganta, cefaleias, cansaço, dispneia, *score* de risco com base na sintomatologia, sem sintomas, outros sintomas.

Os campos temperatura corporal, medicação, tosse, dores musculares, dispneia, cansaço, cefaleia e sem sintomas são binários (s/n) e obrigatórios. O campo temperatura corporal é numérico e também obrigatório.

São ainda tratados os dados relativos aos resultados dos testes por integração com o SINAVE-Lab, o estado da vigilância, as datas de início e fim da vigilância, as datas do início

e fim dos sintomas, e vários registos de vigilância bem como data de alta e de óbito. Informações avulsas sobre outros sintomas/queixas ou sobre a condição clínica, passada ou presente, podem ser inseridas em caixas de texto livre.

Durante a inspeção surgiram dúvidas quanto à necessidade do dado morada, tendo a mesmo sido, em comunicação posterior, justificada pelo facto de, pontualmente, haver equipas de profissionais de saúde que fazem acompanhamento com visitas ao domicílio dos doentes que têm sob a sua vigilância.

Os dados pessoais número fiscal, número de cartão do cidadão ou número da segurança social, se são justificados no momento em que a pessoa é inserida na plataforma, para prevenir duplicações na ausência do número de utente do SNS, não têm qualquer relevância no acompanhamento clínico do doente em vigilância e, por isso, em respeito pelo princípio da minimização e da confidencialidade, previstos nas alíneas *c)* e *f)* do n.º 1 do artigo 5.º do RGPD, não deveriam estar disponíveis aos utilizadores que não tenham privilégios de alteração de dados.

Também no que respeita aos doentes recuperados e falecidos, atendendo à finalidade do tratamento – acompanhamento e vigilância dos doentes em autocuidado – não se compreende por que se mantêm na base de dados. Deste modo, está novamente em causa o princípio da minimização dos dados, consagrado na alínea *c)* do n.º 1 do artigo 5.º do RGPD.

f) Sistema de auditoria

A plataforma Trace COVID-19 faz o registo de auditoria das operações realizadas, armazenando um conjunto alargado de informação de onde se destacam os seguintes dados: tipo de operação, data e hora, *username* e endereço IP da máquina cliente. Toda a informação apresentada ao utilizador, nas várias operações que realiza, fica também incluída do registo de auditoria.

No caso de uma consulta de dados de utente, a CNPD confirmou que o registo de auditoria inclui a data e hora em que foi realizada a operação, o utilizador que a realizou, o endereço da máquina onde a consulta foi efetuada, e o resultado da pesquisa realizada (toda a informação apresentada ao utilizador).

Na prática, o registo de auditoria da informação consultada resulta numa reprodução da informação clínica dos utentes pesquisados o que é claramente excessivo.



Ora, um registo de auditoria para cumprir a sua finalidade não necessita da reprodução de toda a informação.

Na verdade, o conhecimento dos dados a que cada utilizador acede pode ser obtido pela existência de um histórico de alterações, com o qual se consegue reconstituir a informação existente num dado momento e que está sujeito às mesmas regras de proteção de dados implementadas na plataforma, a par com os parâmetros utilizados na pesquisa, esses sim registados em auditoria.

Por outro lado, não resulta dos elementos recolhidos que os registos de auditoria contenham informação sobre o número de resultados devolvidos pela pesquisa (v.g. sem resultados, um resultado, múltiplos resultados), isto porque é também importante conhecer o número de tentativas frustradas.

Deve, por isso, alterar-se o conteúdo dos registos de auditoria em conformidade e aplicar um mecanismo criptográfico que garanta a integridade do registo de auditoria como, por exemplo, uma assinatura digital.

g) Potencial vulnerabilidade

h) Mecanismo de rastreabilidade e notificação

Por força do disposto no n.º 6 do artigo 29.º da Lei n.º 58/2019, de 8 de agosto, o responsável pelo tratamento está obrigado a criar mecanismos de rastreabilidade e notificação ao titular de qualquer acesso aos seus dados pessoais.

Este mecanismo não está implementado na plataforma Trace COVID-19, pelo que deve o responsável proceder às alterações necessárias para cumprir esta obrigação legal e, deste modo, permitir ao titular dos dados um maior controlo sobre o tratamento da informação que lhe diz respeito, nos termos do artigo 35.º da Constituição da República Portuguesa.

i) Avaliação de Impacto sobre a Proteção de Dados

Nos termos do n.º 1 do artigo 35.º do RGPD, sempre que um tratamento de dados pessoais, tendo em conta a sua natureza, âmbito, contexto e finalidade, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento está obrigado a proceder, antes de iniciar o tratamento, a uma avaliação de impacto sobre a proteção de dados pessoais. Sendo certo que a alínea *b)* do n.º 3 do mesmo artigo especifica essa obrigação nos casos de tratamento *em grande escala* que incida sobre *dados especialmente protegidos*, elencados no n.º 1 do artigo 9.º do RGPD, entre os quais constam os dados relativos a saúde, não restam dúvidas que o RGPD impõe esta obrigação no caso em apreço, admitindo-se que a avaliação possa ser feita pelo subcontratante, como decorre do n.º 8 do artigo 35.º.

No entanto, 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 dos 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.

O facto de essa avaliação não ter sido realizada e de, no seu seio, não terem sido equacionadas soluções de proteção de dados desde a conceção, ajustadas aos riscos que esta plataforma comporta, conduziu, precisamente, à necessidade de correções sucessivas neste sistema de informação, à medida que aqueles riscos iam sendo comunicados pelos utilizadores ou detetados pelo subcontratante.

Poder-se-á, com verdade, alegar que a plataforma foi criada numa situação de emergência de saúde pública, para assegurar um mais eficiente acompanhamento dos doentes e das pessoas suspeitas de infeção, emergência que mereceu inclusive o enquadramento no Decreto do Presidente da República n.º 14-A/2020, de 18 de março, e nos ulteriores decretos, a declarar o estado de emergência. E invocar que, ante a urgência na adoção de medidas que garantissem em tempo útil a melhor resposta a esta pandemia, nas prioridades da autoridade nacional de saúde tivesse ficado para segundo plano a realização da avaliação de impacto.

Note-se, porém, que a obrigação imposta pelo artigo 35.º do RGPD é considerada crucial para o cumprimento dos princípios e regras de proteção de dados pessoais. Aliás, reflete essa importância a circunstância de tal obrigação não se inserir no conjunto de obrigações do responsável que podem ser afastadas *em abstracto* pelo legislador dos Estados-Membros da União, nos termos do artigo 23.º do RGPD. Por outras palavras, o reconhecimento desse poder legislativo derogante dos direitos e obrigações previstos no RGPD não abrange, sequer em situações de exceção constitucional dos Estados-Membros, a obrigação de avaliação de impacto sobre a proteção de dados.

Tendo presente a razão de ser e a importância desta obrigação imposta pelo RGPD, não deixa, contudo, de se admitir que a situação de emergência de saúde pública com que a DGS se debateu pode constituir uma situação legitimadora de atuações administrativas concretas *praeter legem*, bem como *contra legem*. Com efeito, é pacífico que, tanto o estado de necessidade administrativo (consagrado no n.º 2 do artigo 3.º do Código do Procedimento Administrativo), como o estado de emergência administrativo (regulado por leis especiais), são causa de exclusão da ilicitude de atuações administrativas concretas para salvaguardar

o interesse público que está em grave perigo¹⁴. Poderá surgir a dúvida se uma declaração de estado de emergência por um Estado-Membro é suficiente para justificar a atuação concreta da autoridade administrativa nacional contra uma imposição do Direito da União, mas dir-se-ia que os motivos urgentes de interesse público importante que legitimam juridicamente uma ação administrativa em violação da lei nacional, também poderão servir de justificação para legitimar a mesma ação em violação do Direito da União. Desde que, insiste-se, esteja em causa uma atuação *concreta* de uma autoridade pública e não uma norma abstrata definida pelo poder político-legislativo – porque esta última, já vimos, está excluída pelo artigo 23.º do RGPD.

De todo o modo, afigura-se que relevante, neste específico quadro excecional de atuação do responsável pelo tratamento, é que a função da avaliação de impacto (função que é a razão de ser da não derogabilidade da obrigação da sua realização por lei nacional) tenha sido promovida por outra via. Ou seja, importante é que, seja prosseguido mesmo que por outra via, o objetivo final da imposição de realização da avaliação de impacto (*i.e.*, a *ratio* do artigo 35.º) para que se possa afirmar uma “legalidade excecional”.

Esse objetivo corresponde à ponderação dos meios a adotar para atingir um determinado fim, no contexto de uma identificação dos riscos e do balanceamento entre os direitos dos titulares dos dados e a finalidade de interesse público. Como, em rigor, é sobre esse juízo de adequação e necessidade entre meios e fins que deve especialmente assentar toda a atuação administrativa em estado de necessidade ou em estado de emergência, não tem a CNPD como afirmar, sem mais, que uma tal ponderação não tenha sido feita pela DGS.

Não terá, como o demonstram os factos averiguados no presente processo, sido feita em termos suficientemente ajustados quanto ao resultado da tutela dos direitos dos titulares dos dados, mas não se pode afirmar não ter sido feita uma ponderação, à luz do princípio da proporcionalidade, da adequação e necessidade dos tratamento dos dados a realizar através da plataforma em relação à finalidade visada.

Deste modo, no caso em apreço, tendo em conta a situação excecional de emergência de saúde pública que justifica o tratamento de dados realizado pela autoridade nacional

¹⁴ Neste sentido, Diogo Freitas do Amaral, *Curso de Direito Administrativo*, II, 2.ª ed., Almedina, Coimbra, 2011, p. 377; Paulo Otero, *Legalidade e Administração Pública. O sentido da vinculação administrativa à juridicidade*, Almedina, Coimbra 2003, pp. 996-997; Pedro Gonçalves, *Manual de Direito Administrativo*, Almedina, Coimbra 2019, pp. 391-392, 396-397.

responsável pela prossecução do interesse público em perigo, e tendo em conta que a CNPD não pode afirmar que a função ou *ratio* da norma do RGPD que impõe a obrigação de proceder à avaliação de impacto não tenha sido, neste específico contexto excecional, prosseguida por uma via diferente, “substitutiva do padrão de conformidade normativa da atuação”¹⁵ da autoridade nacional de saúde (cumprindo uma “legalidade excecional” ou alternativa), não pode concluir-se pela ilicitude do não cumprimento do artigo 35.º do RGPD.

Ainda assim a CNPD recorda que a avaliação de impacto sobre a proteção de dados é um instrumento apto à realização do referido “juízo ponderativo da adequação e necessidade entre meios e fins” no contexto de tratamentos de dados pessoais que apresentem um risco elevado para os direitos dos titulares, revelando-se, por isso, um instrumento adequado à ponderação a fazer em situações administrativas excecionais. Por essa razão, a CNPD sublinha que, em princípio, não deve ser afastada a norma impositiva da sua realização mesmo nos casos de necessidade ou de emergência administrativas¹⁶.

j) Eventual reutilização da base de dados

A terminar importa considerar a hipótese, que estará a ser equacionada pela DGS, de aproveitamento dos dados da base de suporte à ferramenta Trace COVID-19, findo o período de emergência que justificou a sua criação.

A este propósito, recorda-se que os tratamentos de dados pessoais se regem pelo princípio da limitação das finalidades, nos termos previstos na alínea *b)* do n.º 1 do artigo 5.º do RGPD. Ainda que, em determinadas circunstâncias, se possa ter por admissível a reutilização de dados pessoais, a natureza sensível dos dados pessoais aqui em causa, o universo muito alargado de titulares de dados e a situação de emergência que justificou a sua criação são fundamentos bastantes para se exigir aqui uma reforçada contenção na reutilização.

Com efeito, importa ter presente que esta foi uma base de dados criada em circunstâncias excecionais para uma finalidade bem delimitada e previsivelmente transitória, com um enquadramento legal insuficiente, por ausência de previsão de medidas adequadas a

¹⁵ Paulo Otero, *ob. cit.*, p. 908.

¹⁶ Sustentando que a atuação *contra legem* só deve ocorrer quando os valores, bens ou interesses públicos que se visa acautelar não possam ser salvaguardados através de meios que não envolvem o afastar das normas integrantes da legalidade ordinária, Paulo Otero, *ob. cit.*, p. 907.

garantir os direitos dos titulares, e não precedido de uma avaliação de impacto que poderia ter contribuído para suprir essa lacuna. Atento o especial e excecional enquadramento jurídico da sua criação, e considerando o princípio da limitação da conservação dos dados apenas durante o período necessário à finalidade para que foram tratados, consagrado na alínea e) do n.º 1 do artigo 5.º do RGPD, a CNPD recomenda que a conservação desta base de dados esteja limitada ao período de pandemia/epidemia, até porque a informação clínica existe, ou deve ser integrada, no processo clínico de cada doente¹⁷.

Pode, porém, justificar-se a sua reutilização para efeito de investigação científica, mas, na esteira das diretrizes do Comité Europeu para a Proteção de Dados e por força dos princípios da minimização dos dados, da limitação da conservação e da confidencialidade, a CNPD entende que a informação constante da base de dados de suporte à ferramenta Trace COVID-19 apenas pode ser reutilizada para investigação epidemiológica, com garantias reforçadas de proteção dos direitos dos titulares (*v.g.*, pseudonimização)¹⁸. Para as demais finalidades de investigação científica não se afigura indispensável a identificação ou a identificabilidade das pessoas a quem diz respeito a informação, pelo que somente será de admitir a reutilização após uma efetiva anonimização (irreversível) dos dados¹⁹.

III. CONCLUSÕES

Uma vez que no tratamento de dados pessoais realizado através da plataforma Trace-COVID-19, não obstante as medidas entretanto adotadas, estão ainda em crise alguns princípios e regras do regime de proteção de dados pessoais, a CNPD recomenda à DGS:

¹⁷ No sentido de o direito da União exigir que as medidas que representem restrições a direitos dos titulares dos dados, adotadas neste contexto, sejam limitadas no tempo, *v. Statement on restrictions on data subject rights in connection to the state of emergency in Member States*, aprovado pelo Comité Europeu para a Proteção dos Dados, disponível em https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_statement_art_23gdpr_20200602_en.pdf

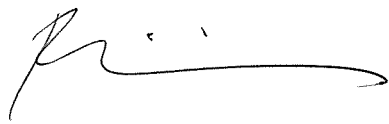
¹⁸ Cf. *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*, aprovado a 21 de abril de 2020, em especial, §§ 44-45 e 51, disponível em https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf

¹⁹ *V. as Diretrizes do Comité Europeu para a Proteção de Dados*, citada na nota anterior, § 46.

1. Para aplicação plena do princípio da minimização dos dados, consagrado na alínea *c)* do n.º 1 do artigo 5.º do RGPD, a adoção de medidas adequadas a garantir que:
 - i. O responsável pelo tratamento só confira acesso a quem seja profissional de saúde sujeito a dever de sigilo profissional, como decorre da alínea *j)* do n.º 2 do artigo 9.º do RGPD;
 - ii. O perfil de acesso conferido a um utilizador de qualquer unidade do ACES não abranja os dados pessoais de todos os doentes registados no conjunto das unidades funcionais do mesmo agrupamento, mas apenas aos da unidade funcional respetiva;
 - iii. Os dados de doentes recuperados e falecidos sejam eliminados da base de dados;
 - iv. Não estejam disponíveis, aos utilizadores que não tenham privilégios de alteração de dados, os dados “número fiscal”, “número de cartão do cidadão” ou “número da segurança social”, de modo a cumprir também o princípio da confidencialidade, consagrado na alínea *f)* do n.º 1 do artigo 5.º do RGPD;
2. Por razões de segurança e de confidencialidade da informação pessoal, nos termos do artigo 32.º do RGPD, a adoção de medidas adequadas a garantir que:
 - i. Se proceda à alteração do conteúdo dos registos de auditoria em conformidade com os requisitos especificados supra, no ponto II, alínea *f)*.
 - ii. Seja avaliada a informação apresentada no URL dos utilizadores;
3. Para cumprimento do disposto no n.º 6 do artigo 29.º da Lei n.º 58/2019, de 8 de agosto, a criação de mecanismos de rastreabilidade e notificação ao titular de qualquer acesso aos seus dados pessoais;
4. Para garantir o respeito pelos princípios da minimização dos dados, da limitação da conservação e da confidencialidade, consagrados nas alíneas *c)*, *e)* e *f)*, do n.º 1 do

artigo 5.º do RGPD, a conservação desta base de dados restrita ao período de pandemia/epidemia, com a ressalva de possibilidade da sua reutilização para a investigação epidemiológica, com específicas garantias, em especial, de pseudonimização.

Aprovado na reunião de 17 de junho de 2020

A handwritten signature in black ink, appearing to be 'Filipa Calvão', with a long horizontal stroke extending to the right.

Filipa Calvão (Presidente)