COMISSÃO NACIONAL
DE PROTEÇÃO DE DADOS

PARECER/2020/129

I. Pedido

O Presidente da Comissão dos Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República solicitou, em 21 de outubro de 2020, à Comissão Nacional de Proteção de Dados (CNPD) que se pronunciasse sobre a Proposta de Lei n.º 62/XIV/2.ª (GOV), que *determina a obrigatoriedade de uso de máscara ou viseira para o acesso ou permanência nos espaços e vias públicas e a obrigatoriedade da utilização da aplicação STAYAWAY COVID em contexto laboral ou equiparado, escolar e académico*, bem como sobre o Projeto de Lei n.º 570/XIV/2.ª, que determina a imposição transitória da obrigatoriedade de uso de máscara em espaços públicos.

O pedido formulado e o presente parecer enquadram-se nas atribuições e competências da CNPD, enquanto autoridade nacional de controlo dos tratamentos de dados pessoais, nos termos do disposto na alínea *c)* do n.º 1 do artigo 57.º e no n.º 4 do artigo 36.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados – RGPD), em conjugação com o disposto no artigo 3.º, no n.º 2 do artigo 4.º e da alínea *a)* do n.º 1 do artigo 6.º, todos da Lei n.º 58/2019, de 8 de agosto (a qual tem por objeto assegurar a execução, na ordem jurídica interna, do RGPD).

De acordo com as suas atribuições e competências, a CNPD pronuncia-se sobre todas as normas que prevejam ou impliquem tratamentos de dados pessoais.

Uma vez que o Projeto de Lei n.º 570/XIV/2.ª foi, entretanto, aprovado[1], a CNPD limita a sua análise à Proposta de Lei n.º 62/XIV/2.ª, na parte relativa à aplicação STAYAWAY COVID, tecendo apenas recomendações quanto à execução das normas contidas naquele Projeto.

II. Apreciação

A. Obrigatoriedade de utilização da aplicação STAYAWAY COVID e de introdução do código de legitimação

[1] Cf. Lei n.º 62-A/2020, publicada na data da aprovação do presente parecer.

A Proposta de Lei, no artigo 4.º, *determina a obrigatoriedade de uso de máscara ou viseira para o acesso ou permanência nos espaços e vias públicas e a obrigatoriedade da utilização da aplicação STAYAWAY COVID em contexto laboral ou equiparado, escolar e académico.* E vincula *em especial os trabalhadores em funções públicas, funcionários e agentes da Administração Pública, incluindo o setor empresarial do Estado, regional e local, profissionais das Forças Armadas e de forças de segurança.*

Para garantir a exequibilidade desta medida, impõe-se ainda, no n.º 3 do artigo 4.º, o *dever* de o utilizador *proceder à inserção na aplicação do código de legitimação pseudoaleatório, que deve figurar do relatório que contenha o resultado do teste laboratorial de diagnóstico.*

Antes de iniciar a análise do diploma proposto, a CNPD deixa aqui duas observações.

A primeira diz respeito à forma do presente projeto de diploma. Em causa está uma proposta de lei, por se tratar de uma matéria relativa a direitos, liberdades e garantias, reservada à competência legislativa da Assembleia da República, nos termos do disposto na alínea *b)* do n.º 1 do artigo 165.º e do n.º 3 do artigo 18.º da Constituição da República Portuguesa (CRP). A CNPD destaca assim que, desta vez, eventualmente por força do conteúdo altamente restritivo dos direitos que a proposta apresenta, se tenha optado por submeter ao Parlamento nacional a definição do regime deste tratamento de dados pessoais. A definição de regras sobre o exercício de direitos, liberdades e garantias e, de modo particular, de regras restritivas deve ser objeto de um debate público alargado, o qual não pode deixar de ter lugar, desde logo, naquele que é o espaço democrático nacional por excelência. Pena é que a proposta de diploma não tenha sido acompanhada de um estudo de impacto sobre a proteção de dados pessoais, como impõe o n.º 4 do artigo 18.º da Lei n.º 43/2004, de 18 de agosto, alterada por último pela Lei n.º 58/2019, de 8 de agosto.

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

Assim, ciente da necessidade de harmonização dos diferentes valores e direitos em tensão, a CNPD, num esforço de compreensão da finalidade e do alcance (prático) das medidas restritivas agora propostas, procura, através do presente parecer, contribuir para a definição de um regime que acautele na medida adequada e suficiente os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos de dados pessoais.

1. *Ponto prévio: a STAYWAY COVID, a interface GAEN e o caráter voluntário da utilização da aplicação*

A STAYWAY COVID é um sistema digital de rastreio de proximidade (*contact tracing*)[2], disponibilizado para dispositivos móveis pessoais com sistema operativo *iOS* ou *Android*, utilizando como sensor de proximidade a tecnologia *Bluetooth*, mais concretamente de baixo consumo energético (*Bluetooth Low Energy*).

Do ponto de vista técnico, a STAYAWAY COVID assume-se, não tanto como uma *solução de rastreio*, mas mais como uma *aplicação de notificação da exposição individual a fatores de risco de contágio*. O seu objetivo é, precisamente, o de poder informar um utilizador da aplicação que o seu dispositivo móvel esteve a uma distância inferior a 2 metros, durante mais de 15 minutos, do dispositivo de outra pessoa utilizadora da aplicação a quem posteriormente foi diagnosticada a COVID-19, existindo o risco de ter havido contaminação, dada a proximidade física e a duração do contacto.

Recorda-se ainda que a aplicação STAYAWAY COVID assenta num sistema descentralizado de tratamento de dados pessoais (por outras palavras, é no telemóvel de cada utilizador que é gerada e conservada a informação sobre os contactos de proximidade com outros utilizadores, informação essa que se encontra pseudonimizada), o que permite mitigar o impacto sobre a privacidade e o risco de utilização indevida desses dados, os quais, se associados à informação de que o utilizador é portador do vírus, pode gerar tratamentos discriminatórios.

[2] De acordo com a Organização Mundial de Saúde (OMS), o rastreio de proximidade é o processo de identificar, avaliar e gerir pessoas que foram expostas a uma doença de modo a prevenir a sua transmissão; quando sistematicamente aplicado, o rastreio de proximidade irá interromper as cadeias de contágio, tornando-se por isso um instrumento de saúde pública essencial no controlo de surtos de doenças infeciosas – cf.https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1

Importa, por conseguinte, deixar claro que o sistema STAYAWAY COVID trata essencialmente dados pseudonimizados, os quais são dados pessoais, nos termos das alíneas *1) e 5)* do artigo 4.º do RGPD, uma vez que permitem, por relacionamento com outra informação, identificar a pessoa a que dizem respeito.

Mas neste sistema é também especificamente objeto de tratamento o endereço IP (*Internet Protocol*) do equipamento do utilizador sempre que comunica com o Serviço de Legitimação de Diagnóstico e com o Serviço de Publicação de Diagnóstico. Recorda-se que o endereço IP é um dado pessoal, por permitir identificar, sem esforço ou custo desproporcionado, quem foi a pessoa que acedeu via Internet ao servidor (cf. alínea *1)* do artigo 4.º do RGPD e jurisprudência do Tribunal de Justiça da União Europeia (Caso *Breyer*, C-582/14, pontos 44-49, ECLI:EU:C_2016:779).

Note-se que, mesmo sem recorrer a informação detida por terceiros para identificar o utilizador, o endereço IP permite desde logo conhecer uma localização geográfica aproximada dos utilizadores[3]. Sublinhe-se ainda que os utilizadores da aplicação acedem ao Serviço de Publicação de Diagnóstico diariamente, por quatro vezes, e que, acrescidamente, alguns utilizadores podem ser referenciados como pessoas com um diagnóstico positivo de COVID-19, quando se autenticam para envio das respetivas TEK (*Temporary Exposure Key*)[4]. Aliás, a entidade que desenvolveu em Portugal esta aplicação sempre assumiu, na documentação remetida à CNPD, a existência de tratamento de dados pessoais.

Ademais, ainda que o *Bluetooth Device Adress* e o *Rolling Proximity Identifier* sejam atualizados e randomizados, a circunstância de muito dificilmente tais operações ocorrerem em simultâneo (*i.e.*, exatamente no mesmo minuto e segundo) faz com que eles sejam relacionáveis, assim permitindo, por exemplo, a rastreabilidade por terceiros que disponham de sistemas (antenas) que leiam aqueles sinais.

Assim, no âmbito das suas atribuições e competências sobre tratamento de dados pessoais, a CNPD pronunciou-se, em sede de controlo prévio, quanto à avaliação de impacto sobre a

---

[3] No caso de os utilizadores acederem a partir de uma instituição na qual trabalham, por exemplo, o IP pode ainda revelar a associação do utilizador a essa instituição.

[4] A chave TEK inicial é gerada na primeira execução do dispositivo móvel pessoal após entrada em funcionamento da aplicação, a partir dos geradores de números pseudoaleatórios nativos das plataformas *Android* (*Java*) e *iOS* (*Swift*). As chaves TEK são armazenadas no respetivo dispositivo móvel durante 14 dias.

proteção de dados, na Deliberação/2020/277[5]. E emitiu parecer sobre o diploma legal que veio regular alguns aspetos desse tratamento de dados pessoais – cf. Decreto-Lei n.º 52/2020, de 11 de agosto[6].

Todavia, como a CNPD explicou na referida Deliberação[7], embora a utilização da tecnologia *Bluetooth* seja menos intrusiva do que uma tecnologia que permita de imediato registar a localização do utilizador, quanto aos dispositivos eletrónicos *Android* a Google fez depender o funcionamento da tecnologia *Bluetooth* da recolha (permanente) do dado de localização, permitindo, assim, o rastreamento, por parte desta empresa, para outras finalidades da localização e das movimentações dos utilizadores da aplicação.

Na realidade, a Google e a Apple criaram uma interface (GAEN) para habilitar o funcionamento de aplicações de rastreamento de proximidade, disponibilizando o acesso a funcionalidades ao nível do sistema operativo do dispositivo móvel, como sejam o acesso à componente do *Bluetooth*, a geração de chaves e de identificadores pseudoaleatórios e o seu cruzamento para cálculo do risco, as quais não são executadas pela aplicação. Com isto, uma parte substancial do tratamentó de dados não é controlada pelo responsável pelo tratamento (a Direção-Geral de Saúde), mas sim por uma parceria de duas das maiores empresas privadas de tecnologia.

Esta é também uma das razões porque a utilização da aplicação só foi considerada legítima no ordenamento jurídico nacional se dependesse exclusivamente da vontade dos cidadãos a sua utilização, o mesmo se aplicando à introdução do código de legitimação, que desencadeia o alerta de risco de contágio junto dos utilizadores da aplicação que tenham ficado registados como tendo estado próximos do utilizador que é portador do vírus. Inclusive, aquelas empresas só disponibilizam a interface (GAEN) se a instalação da aplicação de *contact tracing* for voluntária.

Aliás, como melhor se explicará *infra*, foi o facto de a utilização da aplicação (e a introdução do código) ser voluntária que permitiu, numa fase inicial da pandemia, em que era geral a incerteza quanto aos meios aptos ao seu combate, não questionar a proporcionalidade da restrição aos direitos fundamentais à reserva da vida privada e à proteção dos dados pessoais, pois a circunstância de o fornecimento dos dados pessoais estar na

[5] Cf. §§ 87 e 89.

[6] Cf. Parecer/2020/82, de 21 de julho, disponível em https://www.cnpd.pt/home/decisoes/Par/PAR_2020_82.pdf

[7] Cf. §§ 87 e 89.

disponibilidade do cidadão suaviza o grau de exigência na demonstração da adequação e da necessidade deste tratamento de dados pessoais para se atingir a finalidade pretendida de mais rapidamente se quebrar a cadeia de contágios.

Por tudo isto, a CNPD insistiu no caráter voluntário da utilização da aplicação na Deliberação já citada, em coerência com a posição assumida nas *Diretrizes n.º 4/2020, do Comité Europeu para a Proteção de Dados, sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19*[8].

Assim, também o Decreto-Lei n.º 52/2020, de 11 de agosto, que veio conferir enquadramento legal a alguns aspetos do tratamento de dados pessoais realizado pela aplicação STAYAWAY COVID, assume no artigo 1.º (parte final) e no n.º 1 do artigo 4.º o caráter voluntário da utilização da aplicação e da inserção da informação de que se está contaminado pelo vírus.

Note-se que no referido diploma legal, no artigo 2.º, prevê-se que a aplicação *deve respeitar a legislação europeia e nacional aplicável à proteção de dados pessoais, e ainda as iniciativas europeias adotadas no âmbito do combate à COVID-19 através do recurso a soluções baseadas em dados pessoais, designadamente [...] as Diretrizes n.º 4/2020, do Comité Europeu para a Proteção de Dados, sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19.*

Estranhamente, a Proposta de Lei faz agora tábua rasa do que se definiu no citado Decreto-Lei e do entendimento, vertido nas Diretrizes que o Governo (no referido diploma) diz seguir, de que um dos requisitos tidos como essenciais, à luz da legislação europeia e nacional de proteção de dados pessoais, é o caráter voluntário da utilização da aplicação[9]. Nestas Diretrizes pode ler-se que o «acompanhamento sistemático e em larga escala da localização e/ou dos contactos entre pessoas singulares constitui uma grave intrusão na sua privacidade. *Tal só pode ser legitimado se contar com uma adoção voluntária pelos utilizadores para cada uma das finalidades respetivas.* Isto implicaria, em particular, que os indivíduos que decidem não utilizar ou não podem utilizar tais

[8] Cf. em especial os §§ 8, 24, 31 e 43 das Diretrizes n.º 4/2020 do Comité Europeu para a Proteção de Dados disponíveis em https://www.cnpd.pt/home/orientacoes/Diretrizes_4-2020_contact_tracing_covid_with_annex_en_PT.pdf

[9] Cf. §§ 8, 24, 31 e 43 das Diretrizes n.º 4/2020 do Comité Europeu para a Proteção de Dados, disponíveis em https://www.cnpd.pt/home/orientacoes/Diretrizes_4-2020_contact_tracing_covid_with_annex_en_PT.pdf

aplicações não devem sofrer qualquer desvantagem.»[10].

Feito este esclarecimento, em particular quanto ao impacto que a utilização da aplicação STAYAWAY COVID, não obstante as medidas mitigadoras adotadas, tem sobre a privacidade das pessoas, importa agora considerar a alteração que a presente Proposta de Lei pretende introduzir, ao eliminar o caráter voluntário da utilização da aplicação e da inserção na aplicação do código de legitimação, impondo a obrigatoriedade de tais medidas.

2. *A obrigatoriedade da utilização da aplicação e os direitos fundamentais à liberdade, ao respeito pela vida privada (nas comunicações eletrónicas) e à proteção dos dados pessoais, bem como o direito fundamental à não discriminação*

Importa, em especial, considerar o impacto da imposição legal de tais deveres nos direitos fundamentais à liberdade, à reserva ou respeito pela vida privada, à inviolabilidade das comunicações eletrónicas e à proteção dos dados pessoais – direitos consagrados nos artigos 26.º, 27.º, 34.º e 35.º da Constituição da República Portuguesa (de ora em diante, CRP) e nos artigos 6.º, 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (doravante, Carta). Nos termos definidos nestes diplomas fundamentais, a restrição de direitos, liberdades e garantias só é admissível se respeitar o princípio da proporcionalidade, o que implica estar demonstrada a adequação, necessidade e o caráter não excessivo da restrição, e desde que não afete o conteúdo essencial dos direitos – cf. n.º 2 e n.º 3 do artigo 18.º da CRP e no n.º 1 do artigo 52.º da Carta.

Ora, a Proposta de Lei, não só impõe o dever de utilização da aplicação e o dever de inserção do código de legitimação (que corresponde a um dado pessoal de saúde), estabelecendo um quadro sancionatório (contraordenacional) para o incumprimento, como também atribui o poder de fiscalização às forças e serviços de segurança e ainda à Polícia Marítima e à Polícia Municipal.

2.1. *A imposição de utilização da aplicação e a previsão do poder de fiscalização*

[10] § 24 das Diretrizes n.º 4/2020 do Comité Europeu para a Proteção de Dados, já citadas, itálico nosso.

O impacto sobre os direitos fundamentais não decorre apenas da imposição da utilização e disponibilização de informação de proximidade (e mesmo de localização dos utilizadores de alguns tipos de *smartphones*) e de informação relativa à saúde dos utilizadores. Vai mais longe, por força do acesso e da consulta, por parte de entidades policiais, da informação relativa ao conteúdo descarregado nos *smartphones* e demais interações realizadas no contexto desta aplicação e, portanto, por força do acesso a comunicações eletrónicas que o referido poder de fiscalização implica. Na verdade, o conceito de comunicação eletrónica abrange «*qualquer informação trocada ou enviada entre um número finito de partes mediante a utilização de um serviço de comunicações eletrónicas acessível ao público*»[11].

Manifestamente, estas são previsões restritivas de direitos fundamentais e que se revelam desproporcionadas, em desrespeito pelo disposto no n.º 2 do artigo 18.º da CRP e no n.º 1 do artigo 52.º da Carta. Vejamos porquê.

Em primeiro lugar, atente-se na *imposição aos cidadãos da utilização de uma aplicação em equipamentos eletrónicos*. Tal imposição implica, obviamente, a restrição do direito à liberdade quanto aos conteúdos dos nossos equipamentos eletrónicos e quanto às interações que no contexto da utilização deles fazemos. No fundo, traduz uma violação do livre-arbítrio que a cada um é reconhecido em qualquer Estado de Direito democrático.

Mas quando a tal imposição se junta a previsão de fiscalização do seu cumprimento por parte de diferentes agentes de entidades policiais (de acordo com o previsto no artigo 5.º da Proposta, a Polícia de Segurança Pública, a Guarda Nacional Republicana, a Polícia Marítima e a Polícia Municipal), significa ainda a restrição do direito à inviolabilidade das comunicações eletrónicas, consagrado no artigo 34.º da CRP e no artigo 7.º da Carta, na medida em que a verificação do cumprimento deste dever implica o poder de um agente de uma entidade policial conhecer ou exigir a qualquer cidadão que:

1.º Mostre se traz consigo um telemóvel;

2.º O desbloqueie, com o risco de o agente conhecer o código, e permita que o agente

[11] Cf. alínea *a)* do n.º 1 do artigo 2.º da Lei da Privacidade nas Comunicações Eletrónicas (Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto, em transposição de Diretivas europeias).

verifique a tipologia do mesmo, em especial se é um *smartphone* e qual a versão deste equipamento (*hardware* e *software*)[12];

3.º Demonstre se descarregou a aplicação, com o risco de dar a conhecer outras aplicações eventualmente instaladas;

4.º Demonstre que mantém o *Bluetooth* ativo.

Tal implica, pois, a obrigação de expor perante um agente policial as interações que cada um faz no seu *smartphone* e, antes disso, a obrigação de demonstrar se é ou não possuidor de um dispositivo deste tipo numa versão do sistema operativo que suporte esta aplicação.

Crê-se que a descrição dos diferentes passos a dar para a efetiva fiscalização do cumprimento deste dever é suficiente para que se compreenda o grau de ingerência nas comunicações eletrónicas dos cidadãos e na sua privacidade. Como também é suficiente para se compreender que a previsão desta obrigação *está em manifesta contradição com* o n.º 4 do artigo 34.º da CRP, onde *é proibida a ingerência de autoridades públicas na correspondência, telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal.*

De resto, se sobrassem dúvidas quanto à inadmissibilidade de tal ingerência nas comunicações eletrónicas para prevenção e deteção de ilícitos de mera ordenação social, bastava atentar no Regime Geral das Contraordenações e Coimas (aqui subsidiariamente aplicável por determinação do artigo 7.º da Proposta de Lei), o qual, no artigo 42.º, proíbe *as intromissões na correspondência e nos meios de telecomunicação.*

Ainda que se encontrasse outra forma de executar a fiscalização prevista na Proposta de Lei, tal implicaria disponibilizar às diferentes entidades policiais (inclusive, à Polícia Municipal) a informação sobre quem instalou a aplicação e sobre quem inseriu o código de legitimação, o que traduz uma ingerência igualmente grave na privacidade dos cidadãos no contexto das comunicações eletrónicas.

A que acresce a circunstância de, atualmente, a vida privada de cada um estar, no essencial ou, pelo menos, em muitos aspetos e dimensões, espelhada no seu telemóvel,

[12] Isto porque, como a CNPD assinalou na sua Deliberação/2020/277, de 29 de junho, nem todos os *smartphones* podem fazer uso desta aplicação, sendo necessárias versões mais recentes dos dispositivos, o que reduz o universo de potenciais aderentes. A Google anuncia que é necessário ter, pelo menos, um dispositivo *Android* versão 6.0. (API versão 23) e a Apple indica a versão *iOS* 13.5 ou posterior.

sobretudo quando este corresponda a um *smartphone*. Consequentemente, a possibilidade de acesso ao dispositivo móvel pessoal e de consulta dos conteúdos tem um impacto muito significativo na reserva de vida privada.

Demais, da conjugação do n.º 1 do artigo 4.º com o artigo 5.º da Proposta parece decorrer que o processo de fiscalização implica o acesso, aparentemente livre, dos agentes das entidades policiais aos estabelecimentos públicos e privados onde se desenrolem as atividades consideradas relevantes para este efeito: para além das *atividades escolares e académicas*, a referência expressa ao *contexto laboral ou equiparado* abrange todo e qualquer estabelecimento ou local (inclusive, o domicílio, no caso dos prestadores de serviço doméstico) onde trabalhadores ou outros profissionais prestem serviço. Neste âmbito sujeita-se *em especial os trabalhadores em funções públicas, funcionários e agentes da Administração Pública, incluindo o setor empresarial do Estado, regional e local, profissionais das Forças Armadas e de forças de segurança*.

A este propósito importa, antes de mais, recordar que o artigo 174.º do Código do Processo Penal, mesmo no contexto da investigação criminal, faz depender o poder de realizar revistas e buscas de prévio despacho de autoridade judiciária, e que só em pressupostos muito apertados e para crimes muito graves, admite que os órgãos de polícia criminal possam tomar tal iniciativa, sujeita a imediata comunicação e apreciação pelo juiz do processo. É bom de ver que um processo de fiscalização (preventiva!) de condutas que correspondem a contraordenações não pode oferecer menores garantias aos cidadãos do que um processo em que se suspeita da prática de crime.

Pelo que não se vê como se possa concretizar este poder de fiscalização nos diferentes tipos de contextos acima enunciados. Sobretudo, quando em causa estejam estabelecimentos onde haja especiais deveres de sigilo profissional, como é o caso de instituições de crédito, redações de órgãos de comunicação social, sociedades de advogados e consultórios de advogados, consultórios médicos, onde, mesmo no contexto da investigação criminal, qualquer busca ou revista tem de ser feita na presença do juiz de instrução criminal.

Aliás, mesmo na Administração Pública há entidades que gozam de independência em relação ao Governo e aos seus ministérios, razão por que a entrada de agentes policiais nas respetivas instalações depende da autorização do dirigente máximo ou representante da entidade, quando não haja mandado judicial. É, por exemplo, o que

sucede com as universidades e institutos politécnicos.

2.2. *A falta de adequação* (e o excesso) *da imposição de utilização da aplicação para a finalidade visada*

Mas a restrição da privacidade não se concretiza somente no plano da fiscalização. Ela é anterior a esse momento. Na verdade, a utilização da aplicação, como se explicou, implica a recolha e subsequente tratamento da informação relativa à proximidade (distância e tempo) em relação a outras pessoas que descarregaram a aplicação. Além disso, pelo menos quanto aos dispositivos *Android*, a interface GAEN implica a recolha permanente do dado 'localização', uma vez que deixa de ficar ao critério de cada um poder desativar essa funcionalidade se e quando o desejar, permitindo assim à Google rastrear as deslocações e movimentos dos cidadãos utilizadores desta aplicação para outras finalidades.

Considerando o universo de pessoas destinatárias desta obrigação, é evidente o impacto que este tratamento tem em termos de exposição da sua vida privada.

Ora, para se compreender se a finalidade de detetar o mais cedo possíveis situações de potencial contágio e de assim se interromper a cadeia de contágio (para salvaguarda do interesse de saúde pública) é suficiente para justificar a restrição dos direitos fundamentais já elencados, imprescindível é avaliar a proporcionalidade desta imposição legal, como impõe o n.º 2 do artigo 18.º da CRP e o n.º 1 do artigo 52.º da Carta, e ainda a alínea *c)* do n.º 1 do artigo 5.º do RGPD.

Neste juízo sobre a proporcionalidade não pode deixar de se começar pela avaliação da *adequação ou aptidão* desta medida para atingir a finalidade visada, antes mesmo de se avaliar da sua necessidade. Como se referiu supra, o caráter voluntário da utilização da aplicação permitiu até agora não questionar a proporcionalidade da restrição dos direitos fundamentais à reserva da vida privada e à proteção dos dados pessoais, pois a circunstância de o fornecimento dos dados pessoais estar na disponibilidade do cidadão (que pode a qualquer momento desativar a aplicação, não introduzir o código, ou mesmo desinstalá-la) suavizava o grau de exigência na demonstração da adequação e da necessidade deste tratamento de dados pessoais para se atingir a finalidade pretendida de mais rapidamente se quebrar a cadeia de contágios.

A partir do momento em que se pretende transformar numa utilização obrigatória o uso de uma aplicação que implica a restrição de direitos, liberdades e garantias, essa restrição só poderia ter-se por admissível se demonstradamente fosse idónea a atingir a finalidade visada.

A verdade é que logo a circunstância, já destacada na Deliberação/2020/277, de 29 de junho, de esta aplicação só poder ser instalada em *smartphones* e em versões mais recentes dos mesmos, que uma parte significativa da população não possui, prejudica fortemente a eficácia desta solução e faz duvidar da adequação da imposição da utilização da mesma quando se sabe à partida – o que é, aliás, assumido pelo legislador – que esta medida não é suscetível de ter aplicação a uma boa parte do universo de pessoas que especialmente se pretende proteger da cadeia de contágios. Aliás, a Organização Mundial de Saúde (OMS), em orientações datadas de 28 de maio deste ano, relativas a considerações éticas para a utilização de tecnologias digitais de rastreio de proximidade[13], afirma que a eficácia deste rastreio digital de proximidade como meio de deteção de cadeias de contágio está ainda por comprovar.

Essa eficácia é ainda posta em causa pelo facto de o *Bluetooth* de baixa energia gerar erros na leitura das distâncias entre pessoas, fazendo aumentar bastante os falsos positivos e fomentando, por conseguinte, alarmes de contágio potencial que não correspondem a uma real probabilidade de risco de contágio, de acordo com os critérios definidos pela DGS[14].

Acresce que a utilidade da pretensa obrigatoriedade de utilização da aplicação (e de introdução do código de legitimação) dependeria de uma capacidade massiva de fiscalização (e, obviamente, da legitimidade de tal fiscalização). E não se vê que seja exequível essa fiscalização em larga escala. Na verdade, isso pressuporia haver agentes policiais em número suficiente para cumprir tal missão e com conhecimentos técnicos suficientes para verificar, antes de mais, se um determinado cidadão integra o universo de pessoas vinculadas por tal obrigação. Só quanto a este ponto, tal passaria por analisar, não apenas se o *hardware* suporta esta aplicação, mas também se o *software* instalado é compatível com a aplicação. Depois, há fatores que dificultam a verificação de que se mantém a aplicação ativa, porque o utilizador pode circular na via pública com os dados

---

[13] Cf. https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1

[14] Cf. artigo da publicação WIRED, de 14/10/2020, relativo a um estudo realizado pelo *Trinity College* de Dublin acessível em https://www.wired.co.uk/article/contact-tracing-app-notification-bluetooth

móveis desligados, e só se ligar à rede da Internet mais tarde (ou no dia seguinte), sem que tal afete a utilização da aplicação.

Demais, não se afigura exequível a verificação do cumprimento da obrigação de introduzir o código de legitimação, imposta no n.º 3 do artigo 4.º da Proposta de Lei. Isto porque se o cidadão tiver introduzido o código de legitimação na aplicação surge no ecrã do telemóvel uma mensagem a informar que a partir daquele momento a STAYAWAY COVID deixa de monitorizar os seus contactos (obviamente, porque supõe que o utilizador passe a estar em situação de isolamento) e indica ainda que, «[*d]epois de recuperado, quando retomar a sua vida normal, deve reinstalar a STAYAWAY COVID para reiniciar o processo de monitorização*». Ou seja, no equipamento móvel do utilizador não é possível demonstrar que se introduziu o referido código.

Face à falta da adequação da norma impositiva dos deveres de utilizar a aplicação e de introduzir o código de legitimação, pode desde já concluir-se que a mesma viola o princípio da proporcionalidade.

Além disso, uma vez que a utilização da aplicação STAYAWAY COVID foi apresentada no Decreto-Lei n.º 52/2020, de 11 de agosto, como *um instrumento complementar de resposta à situação epidemiológica pelo reforço da identificação de contactos*, a restrição dos direitos, liberdades e garantias sempre se teria por *desnecessária*, por existirem outras medidas à disposição das autoridades de saúde suscetíveis de aplicação a todos os cidadãos e que não afetam, ou não afetam com a mesma intensidade, aqueles direitos. Na verdade, a assumida função complementar de um instrumento com um tal grau de intrusão na privacidade no contexto de dispositivos eletrónicos é suficiente para se concluir pela sua desnecessidade, no sentido de com isso se estar a reconhecer existirem mecanismos menos lesivos dos direitos fundamentais dos cidadãos que garantem a mesma finalidade.

Finalmente, ainda que se pretendesse que, nas atuais circunstâncias, o interesse público de saúde pública justificasse qualquer medida restritiva de direitos, liberdades e garantias, mesmo uma restrição cuja adequação e necessidade não esteja demonstrada, estas normas impositivas não passariam pelo crivo da *proibição do excesso*. As normas dos artigos 4.º e 5.º da Proposta de Lei, com o que implicam de restrição do livre-arbítrio

e da liberdade, por um lado, e de ingerência por parte das entidades policiais nas comunicações eletrónicas dos cidadãos e, portanto, na sua esfera de privacidade, por outro lado, significariam um atropelo tal destes direitos fundamentais que se teria de concluir pela afetação do conteúdo essencial dos mesmos.

A que acresce o impacto decorrente de a sua aprovação representar um abrir de portas a restrições futuras do mesmo tipo, em circunstâncias diferenciadas, mesmo que sempre em nome do bem comum.

2.3. O efeito discriminatório das medidas restritivas

A terminar este ponto, importa ainda assinalar a delimitação da imposição daquela obrigação apenas às *pessoas que sejam possuidoras de equipamento que permita cumprir essa obrigação.*

Ainda que, por hipótese absurda, se tivesse como adequada e necessária uma tal imposição, e mesmo considerando que uma obrigação não deva ser imposta a quem não tem meios para a cumprir, não pode deixar de se sublinhar que infligir uma restrição a direitos, liberdades e garantias com este grau de impacto apenas a alguns cidadãos traduz uma restrição desigual e discriminatória.

O reconhecimento legal aos cidadãos de uma esfera jurídico-fundamental diferenciada, em função da propriedade ou posse de dispositivos eletrónicos de determinado tipo – que supõe ou assenta num certo poder económico ou numa determinada situação profissional –, representa um grau de arbitrariedade e de discriminação social incomportável no atual quadro normativo em que vivemos (cf. artigo 13.º da CRP e artigo 21.º da Carta).

Sobre a desigualdade que a imposição da utilização desta aplicação vai objetivamente acentuar, tendo em conta que uma parte da população não dispõe de equipamentos eletrónicos ou não dispõe das versões dos equipamentos que lhes permita descarregar tal aplicação e utilizá-la, a CNPD volta a lembrar as reservas suscitadas pelo Conselho Nacional de Ética para as Ciências da Vida a propósito desta aplicação (mesmo num quadro de utilização voluntária)[15]. Também a OMS, em orientações datadas de 28 de maio

[15] Posição do Conselho Nacional de Ética para as Ciências da Vida, de 29 de junho de 2020, sobre *Aplicações digitais móveis para controlo da transmissão da COVID-19 – aspetos éticos relevantes*, acessível em

deste ano, relativas a considerações éticas para a utilização de tecnologias digitais de rastreio de proximidade[16], entende que este tipo de recursos pode exacerbar desigualdades, pois nem todos os cidadãos têm acesso a estas aplicações e só muito indiretamente poderá beneficiar delas, sublinhando que a aposta no rastreamento digital de proximidade em detrimento das abordagens tradicionais pode reduzir o acesso a serviços essenciais a populações já marginalizadas, em particular os mais velhos ou os que vivem na pobreza.

Face aos argumentos supra expostos, a CNPD só pode concluir pela inconstitucionalidade, e pela violação do Direito da União Europeia, da imposição legal da utilização da aplicação STAYAWAY COVID e da introdução do código legitimador, em face da desproporcionalidade da restrição dos direitos fundamentais à liberdade, à reserva ou respeito pela vida privada, à inviolabilidade das comunicações eletrónicas e à proteção dos dados pessoais, bem como da discriminação de tratamento dos cidadãos daquela decorrente.

3. A alteração do processo de emissão do código de legitimação

Uma última nota sobre a Proposta de Lei, para nos reportarmos à alteração preconizada no n.º 3 do artigo 4.º, quanto ao processo de emissão do código de legitimação. Aí se pode ler que *o código de legitimação pseudoaleatório [...] deve figurar do relatório que contenha o resultado do teste laboratorial de diagnóstico.*

Importa, a este propósito, esclarecer que a solução acolhida no sistema passa por o médico que comunica o diagnóstico emitir, a pedido do cidadão, o código de legitimação, para subsequente submissão na aplicação. Esta solução está seguramente relacionada com o facto de, no ordenamento jurídico português, os diagnósticos clínicos serem da competência exclusiva dos médicos.

Parece pretender-se agora que o código seja emitido no laboratório de análises. Ainda que se possa admitir um processo simplificado de emissão do código, a verdade é que os laboratórios de análises não fazem diagnósticos. De todo o modo, esta alteração parece tornar universal a emissão de um código de legitimação para os resultados analíticos

https://www.cnecv.pt/files/1593523643_62f80ed69c317b6cee76810d493bb77a_posic-a-o-cnecv-apps-mo-veis-controlo-covid19-29-06-2020.pdf

[16] Acessível em https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1

positivos, sem que se explicite ou seja compreensível o procedimento a adotar para o efeito, em particular que sistemas de informação vão interagir. Ora, não tendo sido feito o estudo de impacto sobre a proteção dos dados quanto a esta alteração do sistema, nem apresentadas medidas de segurança adequadas para a adoção deste mecanismo, a CNPD não pode aferir, nem pronunciar-se, sobre as consequências de tal solução.

B. Obrigatoriedade de uso de máscara em espaços públicos

No que diz respeito à imposição legal de utilização de máscara em espaços públicos, considerando que o projeto de diploma foi já aprovado, a CNPD limita-se, na sua pronúncia, a assinalar a necessidade de, na execução e fiscalização de tal dever, se respeitar o princípio da minimização dos dados pessoais, nos termos definidos pela alínea *c)* do n.º1 do artigo 5.º do RGPD.

Assim, a CNPD recomenda que os atestados médicos de incapacidade ou declarações médicas se limitem a declarar que se verifica um fundamento de dispensa de utilização da máscara, sem especificar a causa que justifica tal dispensa. A função de fiscalização pelas autoridades policiais não carece, e nessa medida não justifica, o conhecimento dos fundamentos, relativos à saúde das pessoas, de tal dispensa.

III. Conclusão

A CNPD centra o presente parecer na Proposta de Lei n.º 62/XIV/2.ª, especificamente sobre as previsões relativas ao dever de utilizar a aplicação STAYAWAY COVID. Em relação à imposição do dever de uso de máscara, a CNPD limita-se aqui a alertar para a necessidade de, em sede da sua execução, e por força do princípio da minimização dos dados pessoais e da proteção da reserva da vida privada, nos atestados médicos de incapacidade ou declarações médicas somente se afirmar a existência de um fundamento de dispensa de utilização da máscara, sem o especificar.

Quanto à obrigatoriedade de utilização da aplicação STAYAWAY COVID e da inserção do código de legitimação:

1. A utilização desta aplicação implica uma restrição dos direitos fundamentais à reserva da vida privada e à proteção dos dados pessoais, uma vez que

i. A referida aplicação realiza tratamento de dados pessoais, ainda que a maior parte destes dados se encontre pseudonimizada;

ii. A circunstância de o acesso a funcionalidades ao nível do sistema operativo dos telemóveis, em particular o *Bluetooth,* depender de uma interface disponibilizada pela Google e pela Apple (GAEN) para cumprir a finalidade visada e de nos *smartphones Android* a Google recolher adicionalmente, de modo automático e permanente, o dado 'localização' do telemóvel, potencia o impacto sobre a privacidade (além do aproveitamento que terceiros podem fazer da ativação constante do *Bluetooth*).

2. Contudo, o caráter voluntário da sua utilização – bem como da inserção do código de legitimação (código que confirma o diagnóstico positivo do vírus) –, deixando ao livre-arbítrio de cada cidadão a decisão de facultar os seus dados, suavizou o grau de exigência na demonstração da adequação e da necessidade deste tratamento de dados pessoais para se atingir a finalidade de interrupção mais célere da cadeia de contágios, razão por que, numa fase inicial da pandemia caracterizada pela incerteza quanto aos meios aptos ao seu combate, a CNPD e as demais autoridades de proteção de dados pessoais dos Estados-Membros da União optaram por não questionar a proporcionalidade daquela restrição.

3. Na perspetiva da CNPD, a presente Proposta de Lei, ao eliminar o caráter voluntário da utilização da aplicação e da inserção na aplicação do código de legitimação, impondo a obrigatoriedade de tais medidas, e ao prever a fiscalização do cumprimento desses deveres pelas entidades policiais (sem definir as condições e limites dessa fiscalização), restringe desproporcionalmente os direitos fundamentais à liberdade (livre-arbítrio), à reserva pela vida privada, à inviolabilidade das comunicações eletrónicas e à proteção dos dados pessoais, em termos tais que parece afetar o conteúdo essencial desses direitos, em especial, do direito à privacidade nas comunicações eletrónicas que os artigos 26.º e 34.º da Constituição e o artigo 7.º da Carta dos Direitos Fundamentais da União Europeia consagram.

4. Por um lado, não está demonstrada a adequação da imposição da utilização desta aplicação para atingir a finalidade visada, por três ordens de razão: a aplicação não é suscetível de ser descarregada em qualquer telemóvel, mas somente em *smartphones* com determinado *hardware* e *software*, deixando de fora parte do universo de pessoas que especialmente se pretende proteger da cadeia de contágios; a tecnologia *Bluetooth Low Energy* pode gerar falsos positivos; não é exequível a verificação do cumprimento dessa imposição e da imposição de inserção do código de legitimação, como se explicou supra.
5. Por outro lado, ter-se-ia sempre por excessivo o acesso e a consulta, pelas entidades policiais, de informação relativa ao conteúdo descarregado nos *smartphones* e demais interações realizadas no contexto desta aplicação, por corresponder ao acesso a comunicações eletrónicas onde consta um leque alargado de informação relativa à vida privada dos respetivos utilizadores.
6. Ainda que assim não se concluísse, é inegável que a imposição destes deveres apenas a alguns cidadãos, em função da propriedade ou posse de dispositivos eletrónicos de determinado tipo – que supõe ou assenta num certo poder económico ou numa determinada situação profissional –, representa um grau de arbitrariedade e de discriminação social incomportável no atual quadro normativo em que vivemos, em violação do artigo 13.º da CRP e do artigo 21.º da Carta dos Direitos Fundamentais da União.
7. No que diz respeito à previsão da emissão universal do código de legitimação no laboratório de análises, na falta de indicação dos termos em que tal pode operar, em particular que sistemas de informação vão interagir, e não tendo sido feito o estudo de impacto sobre a proteção dos dados quanto a esta alteração do sistema, nem apresentadas medidas de segurança, a CNPD não pode aferir, nem pronunciar-se, sobre as consequências de tal solução.

Em suma, as normas dos artigos 4.º e 5.º da Proposta de Lei, ao limitarem o livre-arbítrio e a liberdade dos cidadãos, e com o que implicam de ingerência por parte das entidades

policiais nas comunicações eletrónicas e nos dados pessoais aí tratados, impactando fortemente na privacidade daqueles, representam uma restrição desproporcionada destes direitos fundamentais, em termos tais que se pode afirmar estar a ser afetado o conteúdo essencial dos mesmos, em violação do artigo 18.º, n.ºs 2 e 3, da Constituição, e do artigo 52.º da Carta dos Direitos Fundamentais da União Europeia.

A CNPD toma ainda a liberdade de sublinhar que a eventual aprovação de tais normas representaria abrir a porta a restrições futuras do mesmo tipo, em circunstâncias diferenciadas, mesmo que sob a invocação do bem comum. Num Estado de Direito democrático, como o nosso, em que a privacidade e a liberdade são essenciais ao desenvolvimento da personalidade e da identidade de cada um, o recurso a medidas deste teor representa um retrocesso do *acquis* constitucional, com implicações para o futuro da nossa sociedade que não podem deixar de ser ponderadas pelo legislador nacional.

Aprovado na reunião de 27 de outubro de 2020

Filipa Calvão (Presidente)