

## DELIBERAÇÃO/2020/277

### I. Introdução

1. O Instituto de Engenharia de Sistemas e Computadores, Ciência e Tecnologia - INESC TEC submeteu, no dia 15 de junho de 2020<sup>1</sup>, a consulta prévia da Comissão Nacional de Proteção de Dados (CNPD) uma avaliação de impacto sobre a proteção de dados em relação ao sistema STAYWAY COVID, para rastreio da propagação da COVID-19, através da utilização voluntária de uma aplicação para dispositivos móveis pessoais.
2. O sistema é uma iniciativa do INESC TEC e do Instituto de Saúde Pública da Universidade do Porto (ISPUP)<sup>2</sup>, no âmbito do programa INCoDe.2030, tendo os trabalhos começado a ser desenvolvidos a partir da colaboração com o consórcio internacional do projeto DP<sup>3</sup>T<sup>3</sup>, em resposta à situação de pandemia, e coincidindo com o gradual desconfinamento da população em Portugal.
3. Pretendem os seus autores que a aplicação STAYAWAY COVID funcione como uma medida complementar, no âmbito de uma estratégia global de combate à pandemia, procurando assim dar um contributo significativo para a rápida interrupção das cadeias de infeção, colocando à disposição do Estado a possibilidade de alertar um utilizador se este tiver estado em contacto de proximidade com outros utilizadores da aplicação, a quem foi diagnosticada a COVID-19.
4. A avaliação de impacto sobre a proteção de dados (AIPD), prevista no artigo 35.º do Regulamento (UE) 2016/679 – Regulamento Geral sobre a Proteção de Dados (RGPD), diz respeito tão-só ao desenvolvimento de uma solução tecnológica que, a ser utilizada, implicará o tratamento de dados pessoais, embora esse tratamento não seja da responsabilidade do Requerente. Por conseguinte, há certos aspetos do sistema STAYAWAY COVID que não se encontram ainda totalmente definidos, pois dependerão da aplicação concreta que possam vir a ter, a qual deverá ser determinada pelo responsável pelo tratamento de dados.

---

<sup>1</sup> Foi remetida à CNPD em 22/6/2020 uma versão atualizada da avaliação de impacto.

<sup>2</sup> STAYAWAY COVID foi desenvolvido por ambas as entidades com o apoio das empresas Keyruptive e Ubirider.

<sup>3</sup> Sigla de Decentralized Privacy-Preserving Proximity Tracing.

5. Nesse sentido, a análise da CNPD está também condicionada à arquitetura do sistema e ao seu funcionamento essencial, ficando em aberto algumas questões específicas cuja apreciação está sujeita à forma como o sistema STAYAWAY COVID venha a ser operacionalizado. Todavia, a CNPD adianta já algumas considerações sobre os requisitos legais aplicáveis a uma utilização futura deste sistema.

## II. Descrição do sistema STAYAWAY COVID

6. STAYWAY COVID (doravante «STAYAWAY») é um sistema digital de rastreamento de proximidade (*contact tracing*)<sup>4</sup>, que se pretende disponibilizar para dispositivos móveis pessoais com sistema operativo iOS ou Android, e utilizando como sensor de proximidade a tecnologia *Bluetooth*, mais concretamente de baixo consumo energético (*Bluetooth Low Energy* – BLE).

7. Do ponto de vista técnico, a STAYAWAY assume-se não tanto como uma *solução de rastreamento*, 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<sup>5</sup>.

8. O sistema STAYAWAY adota um modelo descentralizado, isto é, os dados não são coligidos, armazenados e processados num servidor central, mas sim no dispositivo móvel do utilizador. O cálculo de risco e notificação do utilizador são efetuados localmente nesse dispositivo.

---

<sup>4</sup> De acordo com a Organização Mundial de Saúde (OMS), o rastreamento 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 rastreamento de proximidade irá interromper as cadeias de contágio, tornando-se por isso um instrumento de saúde pública essencial no controlo de surtos de doenças infecciosas. Ver [https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics\\_Contact\\_tracing\\_apps-2020.1](https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1)

<sup>5</sup> Estas variáveis de distância e tempo, para calcular o risco de contágio, podem ser reconfiguráveis de acordo com as recomendações da OMS. São tidos em conta os contactos de proximidade dos últimos 14 dias.

9. O sistema assenta numa arquitetura semi-descentralizada, constituída pelos dispositivos móveis pessoais (DMP)<sup>6</sup> e por dois servidores centrais: o Serviço de Legitimação de Diagnóstico (SLD) e o Serviço de Publicação de Diagnóstico (SPD), sendo que este último armazena e disponibiliza os dados pseudonimizados dos utilizadores diagnosticados com COVID-19.
10. O STAYAWAY faz uso do sistema de Notificação de Exposição Google-Apple (GAEN)<sup>7</sup>, um projeto conjunto das duas empresas e desenvolvido especificamente para habilitar o funcionamento de aplicações para rastreio de proximidade via *Bluetooth*. No entanto, de acordo com o GAEN, «apenas as autoridades públicas de saúde podem usar este sistema» e apenas uma aplicação por país está autorizada a aceder.
11. O GAEN disponibiliza o acesso a funcionalidades<sup>8</sup> ao nível do sistema operativo do dispositivo móvel (iOS ou Android), que não são, por isso, diretamente executadas pela aplicação.
12. À exceção das funcionalidades disponibilizadas pelo sistema GAEN, todo o software do sistema STAYAWAY é aberto e será tornado público antes do seu lançamento. A Google e a Apple disponibilizam a especificação do protocolo, algoritmos e a respetiva interface<sup>9</sup>, embora o código do sistema GAEN não seja aberto. Além disso, os fabricantes anunciam que a interface está sujeita a alterações.
13. O utilizador que desejar aderir a este sistema de notificação de exposição individual a risco de contágio, descarrega a aplicação STAYAWAY para o seu dispositivo móvel através das lojas oficiais Google Play, se tiver um sistema Android, ou Apple Store, se tiver um sistema iOS, não sendo necessário fazer qualquer registo adicional para esta aplicação ou abrir uma conta específica.

---

<sup>6</sup> A esta componente se junta a interface BLE e a interface para acesso à Internet, com vista à comunicação do DMP com os servidores centrais.

<sup>7</sup> Google-Apple Exposure Notification. Ver <https://www.apple.com/covid19/contacttracing> e <https://www.google.com/covid19/exposurenotifications/>

<sup>8</sup> Tais como, o acesso à componente de Bluetooth, o protocolo de geração de chaves, a divulgação de identificadores pseudoaleatórios entre dispositivos móveis, o cruzamento dos identificadores pseudoaleatórios para cálculo do risco de contágio.

<sup>9</sup> API - Application Programming Interface.



14. Após instalada e configurada, a aplicação vai gerar diariamente, de forma pseudoaleatória, uma chave de identificadores TEK única<sup>10</sup>, a partir da qual são gerados por dia até 144 identificadores pseudoaleatórios de proximidade, designados por RPI<sup>11</sup>, num intervalo de tempo entre 10-20 minutos.
15. Os RPI são difundidos via *Bluetooth* e recebidos pelos dispositivos móveis pessoais dos outros utilizadores da aplicação, que se encontrem geograficamente ao alcance daqueles sinais *Bluetooth*, onde ficam armazenados por um prazo pré-definido de 14 dias<sup>12</sup>. Deste modo, todos os encontros de proximidade entre utilizadores da aplicação ficam registados de forma pseudonimizada nos respetivos dispositivos móveis pessoais.
16. No caso de um utilizador da aplicação STAYAWAY ser diagnosticado com COVID-19, o médico acede ao Serviço de Legitimação de Diagnóstico (SLD) da aplicação, mediante autenticação, e obtém um código<sup>13</sup>, constituído por 12 algarismos, que entrega ao doente, por meio externo ao sistema, isto é, presencialmente, por via telefónica ou outro meio de comunicação. Esta é a forma de validar que o diagnóstico foi feito por um profissional de saúde autorizado.
17. O SLD regista ainda a data dos primeiros sintomas ou, no caso de infetados assintomáticos, a data de realização do teste à COVID-19, bem como a data em que estes dados deverão ser destruídos.
18. Nesta fase, o doente, através da aplicação, introduz o código que lhe foi dado pelo médico, que é válido para uma única interação, pelo prazo de 24 horas, espoletando o envio

---

<sup>10</sup> TEK – Temporary Exposure Key. A chave TEK inicial é gerada na primeira execução do DMP 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 DMP durante 14 dias.

<sup>11</sup> RPI – Rolling Proximity Identifiers

<sup>12</sup> Os RPI são armazenados juntamente com outros dados, designadamente data, duração e distância estimada do contacto.

<sup>13</sup> O SLD gera simultaneamente um código de legitimação (CL) pseudoaleatório e um código de acesso (CA) pseudoaleatório, armazenando localmente o par CL e CA. O profissional de saúde recebe o CL que entrega ao utilizador/doente.

automático das chaves TEK diárias dos últimos 14 dias, armazenadas no seu dispositivo móvel, para o Serviço de Publicação de Diagnóstico da aplicação<sup>14</sup>.

19. O Serviço de Publicação de Diagnóstico (SPD) da aplicação STAYAWAY armazena, no seu servidor, por um período de 14 dias, todas as chaves TEK enviadas pelos utilizadores da aplicação diagnosticados com COVID-19.

20. Para permitir calcular o risco de contágio com uma pessoa infetada, será necessário cruzar os RPI recebidos dos outros dispositivos móveis com os quais cada utilizador esteve geograficamente próximo e que se encontram registados no seu próprio dispositivo com os RPI de utilizadores da aplicação infetados com COVID-19. Para tal, a aplicação descarrega do SPD, quatro vezes por dia, em instantes aleatórios, as chaves TEK aí armazenadas<sup>15</sup>. Estas chaves irão reproduzir os RPI gerados inicialmente e fazer o cruzamento com os RPI armazenados no dispositivo para verificar se são detetadas coincidências entre os RPI. Se assim for, é calculado o nível de exposição individual ao risco, com base na distância física e na duração do contacto de proximidade<sup>16</sup>, e apresentado um alerta ao utilizador.

21. O alerta da existência de um contacto de risco não significa que a pessoa tenha sido infetada. Juntamente com o alerta é fornecida informação ao utilizador sobre como deve proceder.

22. No dispositivo móvel, a aplicação pode apresentar ao utilizador três estados diferentes: sem risco, alerta de potencial contacto de risco, diagnosticado com Covid-19. Em cada um destes estados, é apresentada informação adicional. No caso de diagnóstico positivo, após terem sido comunicadas as chaves TEK, por ação do utilizador, este é informado de que a

---

<sup>14</sup> Nesta etapa, o DMP acede ao SLD sem se autenticar, fornece o CL e obtém o CA respetivo como resposta. Então, o DMP autentica-se no SPD com o CA obtido, o qual também só é válido para uma interação, e submete as chaves de identificadores TEK, as quais são armazenadas localmente no SPD.

<sup>15</sup> Isto é realizado de forma incremental, por referência à última atualização.

<sup>16</sup> Todo este processo é realizado no sistema operativo do DMP através da interface GAEN. O cálculo do risco de contágio tem em conta a intensidade do sinal BLE, bem como as variáveis distância e tempo de contacto, configuráveis em função das recomendações da OMS. Neste momento, estão estabelecidas para um contacto *a menos de 2 metros e que dure mais de 15 minutos*. Os eventuais acertos positivos que não se encontrem nestas condições não são considerados para o cálculo de risco de exposição ao risco.

aplicação STAWAWAY «deixa de monitorizar os contactos», devendo ser reinstalada a aplicação após a recuperação e o regresso à vida normal para reiniciar o processo<sup>17</sup>.

23. Por último, está previsto que a aplicação vá ainda dispor de uma funcionalidade de *Remote Switch*, que permite ao administrador da plataforma suspender provisoriamente o funcionamento do sistema, em caso de necessidade, deixando de recolher e disseminar códigos, e reativá-lo posteriormente.

24. De acordo com a avaliação de impacto realizada, prevê-se a descontinuação do sistema STAYAWAY no final da pandemia e o conseqüente apagamento de todos os dados.

### III. Apreciação

#### a) Da avaliação de impacto sobre a proteção de dados

25. A avaliação de impacto sobre a proteção de dados (AIPD) foi submetida à CNPD, nos termos do n.º 1 do artigo 36.º do RGPD, por ter sido considerado que, apesar de os riscos identificados serem satisfatoriamente mitigados através de medidas proporcionadas ao seu impacto e probabilidade de ocorrência, subsistem ainda riscos potenciais, na sua maioria inerentes às características dos modelos, os quais não devem ser negligenciáveis, principalmente pelo possível universo alargado de utilizadores, a que se somarão outros eventualmente ainda não identificados, podendo tornar o risco elevado.

26. Entende-se que para a realização do tratamento de dados pessoais decorrente do sistema STAYAWAY é legalmente exigível a realização de uma AIPD, em conformidade com a alínea *b)* do n.º 3 do artigo 35.º do RGPD, por haver neste contexto operações de tratamento em larga escala relativas a dados pessoais de saúde, na aceção das alíneas *1), 2), 5) e 15)* do artigo 4.º do RGPD.

27. A AIPD desenvolve vertentes essenciais, como a descrição do sistema, a análise de riscos e vulnerabilidades, a aplicação dos princípios de proteção de dados e a problematização sobre o futuro responsável pelo tratamento de dados, embora alguns aspetos não estejam

---

<sup>17</sup> A aplicação apresenta uma opção de 'rastreo' (ligado/desligado), a qual é automaticamente desligada quando o utilizador comunica as suas chaves TEK ao SPD, o que significa que foi diagnosticado com COVID-19.



suficientemente tratados ou não tenham sido de todo avaliados, o que se assinala mais adiante. Deste modo, e tal como afirmado na própria AIPD, esta deverá ser revista e atualizada para refletir todos os aspetos do tratamento de dados pessoais. Após definição de todas as questões pendentes relativas ao funcionamento do sistema STAYAWAY, impõe-se essa reavaliação para garantir que os pormenores de implementação da aplicação não induzam riscos acrescidos para a privacidade dos titulares dos dados.

28. A AIPD contém o parecer do encarregado de proteção de dados (EPD), nos termos do n.º 2 do artigo 35.º, o qual maioritariamente classificou o tratamento de dados, nas suas diferentes perspetivas, como «aceitável com recomendações».<sup>18</sup>. Além de medidas mitigadoras dos riscos identificados, o EPD recomendou ainda a realização de um teste piloto em condições reais, circunscrito a uma parcela do território nacional, antes da sua disponibilização mais alargada e irrestrita. A CNPD reconhece que a realização de um teste piloto, em que a aplicação esteja disponível apenas para um grupo específico e restrito de utilizadores, pode ser benéfica para identificação e correção de falhas de segurança.

#### b) Do carácter voluntário do uso da aplicação

29. Com a evolução da pandemia do vírus SARS-CoV-2, multiplicaram-se no mundo as soluções tecnológicas, em particular associadas à localização das pessoas como forma de identificar e reduzir a disseminação do contágio, o que suscitou desde logo um grande leque de preocupações do ponto de vista da proteção de dados e da privacidade, por porem em causa estes direitos fundamentais, havendo ainda afetação de outros direitos fundamentais, como sejam o direito de não discriminação, o direito de circular anonimamente, o direito de reunião.

30. Sem dúvida que a adoção de medidas que, independentemente da sua conceção técnica, representam sempre um risco de rastreamento da localização e movimentação dos cidadãos, não devem ter um carácter obrigatório, imposto pelas autoridades públicas, porque claramente violadoras do princípio da proporcionalidade num Estado de Direito democrático. Mesmo estando em causa uma situação excecional de emergência de saúde

---

<sup>18</sup> Numa escala de Aceitável/Aceitável com recomendações/Não aceitável

pública, a imposição de tal tipo de controlo – como se de uma panaceia se tratasse – não cumpriria os princípios da adequação, necessidade e proporcionalidade.

31. A OMS, em orientações datadas de 28 de maio deste ano, relativas a considerações éticas para a utilização de tecnologias digitais de rastreio de proximidade<sup>19</sup>, afirma que a eficácia deste rastreio digital de proximidade como meio de deteção de cadeias de contágio está ainda por comprovar. Por outro lado, enquadra este tipo de soluções como uma forma de intervir num contexto mais alargado de políticas, intervenções e investimentos. De acordo com a OMS, este tipo de recursos pode exacerbar desigualdades, pois nem toda a gente tem acesso a estas aplicações<sup>20</sup> 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.

32. Tendo em consideração todas as razões acima expostas, só se pode pugnar pelo carácter voluntário da aplicação, o qual não faz diminuir a necessidade de garantir a todo o tempo a proteção da privacidade dos utilizadores e dos seus dados pessoais.

33. A aplicação STAYAWAY, na forma como está concebida, reforça a vertente voluntária e a autodeterminação do utilizador, dando-lhe em várias etapas possibilidade de escolha e de controlar os dados, mesmo que pseudonimizados, a serem tratados pela aplicação. A primeira manifestação de vontade exerce-se quando é instalada a aplicação no seu dispositivo móvel pessoal. Posteriormente, caso tenha um diagnóstico positivo para a COVID-19, tem ainda a possibilidade de não comunicar essa informação à aplicação, bastando para tal não informar o médico de que é utilizador da STAYAWAY ou, ainda que

---

<sup>19</sup> [https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics\\_Contact\\_tracing\\_apps-2020.1](https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1)

<sup>20</sup> Nem todos os telefones inteligentes podem fazer uso desta aplicação, sendo necessário 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):

<https://static.googleusercontent.com/media/www.google.com/en//covid19/exposurenotifications/pdfs/Android-Exposure-Notification-API-documentation-v1.3.2.pdf>

A Apple indica a versão iOS 13.5 ou posterior:

[https://developer.apple.com/documentation/exposurenotification/building\\_an\\_app\\_to\\_notify\\_users\\_of\\_covid-19\\_exposure](https://developer.apple.com/documentation/exposurenotification/building_an_app_to_notify_users_of_covid-19_exposure)

o faça, não introduzir posteriormente o código de legitimação no sistema. Este conjunto de ações está na sua inteira disponibilidade e sob o seu total controlo.

34. Além disso, existe ainda a possibilidade de o utilizador desativar em determinados períodos o *Bluetooth* do seu dispositivo móvel, parando de enviar e de receber os códigos RPI (por exemplo, quando está em casa ou em locais em que não há proximidade com outras pessoas), ou de desligar o rastreio de contacto de proximidade na configuração da aplicação, com o mesmo efeito. Por último, pode ainda desinstalar a aplicação em qualquer altura, o que implicaria o apagamento dos seus dados. Todavia, em rigor, o resultado destas ações já não se encontra sob o controlo do utilizador, mas sim essencialmente do sistema operativo gerido pela Apple ou pela Google.
35. Em suma, é imprescindível o carácter voluntário de utilização da aplicação, o qual deve ser sempre apoiado no respeito pelos princípios da transparência, da boa-fé e da licitude dos outros intervenientes no sistema (cf. alínea *a*) do n.º 1 do artigo 5.º do RGPD).

c) Da utilização da tecnologia BLE

36. O desenvolvimento de uma aplicação baseada na tecnologia *Bluetooth Low Energy* (BLE) representa, em geral, uma opção menos intrusiva do que outras tecnologias assentes na geolocalização direta dos seus utilizadores. Tal como é descrita, a STAYAWAY cumpre a sua finalidade de alertar utilizadores do risco de eventual contágio, por proximidade física com pessoa infetada durante mais de 15 minutos, sem que seja necessário conhecer a sua localização ou a de terceiros ou o local onde esse encontro de risco ocorreu, e muito menos a identidade do outro utilizador.
37. Deste modo, verifica-se estar cumprido o princípio da minimização dos dados (cf. alínea *c*) do n.º 1 do artigo 5.º do RGPD), em particular excluindo do tratamento dados que são de grande sensibilidade e especialmente protegidos pela legislação relativa à privacidade nas comunicações eletrónicas<sup>21</sup>.

---

<sup>21</sup> Lei n.º 41/2004, de 18 de agosto, alterada por último pela Lei n.º 46/2012, de 29 de agosto.

38. Todavia, a utilização de BLE não está excluída de riscos de localização do utilizador<sup>22</sup>.

Com efeito, esta tecnologia também permite com elevada precisão a localização dos dispositivos móveis, ademais quando esses dispositivos estão a emitir sinais, como acontece nestes casos, que podem ser lidos por recetores colocados em qualquer sítio (nos centros comerciais, na rua, nos aeroportos, nas estações ferroviárias, etc.).

39. O facto de a aplicação STAYAWAY só funcionar com o BLE ativo<sup>23</sup> força o utilizador, para a poder usar, a deixar ativa a função de Bluetooth, tornando o seu dispositivo visível quase em permanência, com risco de rastreamento da sua localização e das suas deslocações por terceiros; ao contrário do que acontece agora em que o BLE é usado na maior parte das vezes para o emparelhamento de dispositivos, pelo que o seu uso habitual pode ser facilmente controlado pelo utilizador e reduzido no tempo. Mesmo um utilizador cuidadoso que controle criteriosamente as funcionalidades do seu dispositivo móvel que podem indicar a sua localização, como o GPS ou o WIFI, passará a ficar sujeito a rastreamentos de localização através do BLE ao ter a aplicação instalada.

40. Acresce que, de acordo com os protocolos de comunicação sem fios, a transmissão de sinais ativos contém identificadores únicos, como o endereço MAC<sup>24</sup> do controlador da placa de rede sem fios<sup>25</sup>, que mais facilmente permitem reconhecer e monitorizar um dispositivo, logo potencialmente um indivíduo.

41. Contudo, para minimizar o risco de identificabilidade, é possível recorrer a uma funcionalidade conhecida como 'Bluetooth LE Privacy'<sup>26</sup>, que permite aos fabricantes substituir o endereço MAC da interface Bluetooth por um valor aleatório que é mudado a intervalos de tempo, impossibilitando a relação com um único dispositivo e impedindo o rastreamento. As especificações técnicas do sistema GAEN preveem que seja usado um

---

<sup>22</sup> Documento de Trabalho sobre o rastreamento da localização a partir das comunicações dos dispositivos móveis, do *International Working Group of Data Protection in Telecommunications* (IWGDPT), Outubro de 2015, in "Forum de Proteção de Dados", n.º 3, julho de 2016, p. 74 [https://www.cnpd.pt/home/revistaforum/forum2016\\_3/files/assets/basic-html/page-74.html](https://www.cnpd.pt/home/revistaforum/forum2016_3/files/assets/basic-html/page-74.html)

<sup>23</sup> De acordo com o que foi confirmado pelo INESC TEC e que resulta também da informação publicamente disponibilizada pelo GAEN.

<sup>24</sup> MAC address (Media Access Control). Também designado, neste caso, como *advertiser address* ou *Bluetooth device address*.

<sup>25</sup> WNIC – Wireless Network Interface Controller.

<sup>26</sup> <https://www.bluetooth.com/blog/bluetooth-technology-protecting-your-privacy/>

mecanismo daquele género que gera um endereço aleatório para a comunicação dos códigos RPI<sup>27</sup>. Resta saber se, para a Google e a Apple, que têm o verdadeiro endereço da interface Bluetooth, é possível seguir esta cadeia ou reverter o processo. No entanto, este procedimento só se aplica à transmissão de dados no âmbito da aplicação STAYAWAY. Fora desse contexto, é transmitido o identificador único do BLE do dispositivo móvel, o que suscita as questões de privacidade acima descritas nos pontos 38-40.

**d) Do modelo descentralizado do sistema e da sua transparência**

42. A arquitetura semi-descentralizada do sistema STAYAWAY, porque remete para o dispositivo móvel pessoal o armazenamento das chaves e dos identificadores recebidos de terceiros com quem se teve um contacto de proximidade, bem como o cruzamento dos identificadores para calcular o risco de exposição ao contágio, é uma escolha à partida mais adequada do ponto de vista da proteção de dados do que ter a informação centralizada numa única base de dados.
43. Por outro lado, este modelo distribuído apresenta salvaguardas no plano da pseudonimização, oferecendo mais garantias de não re-identificação<sup>28</sup>, e dificulta a utilização de dados para outras finalidades, bem como a sua interconexão com outros tratamentos de dados.
44. Ainda de salientar positivamente a disponibilização pública do código-fonte da aplicação, que permitirá um escrutínio alargado pela comunidade do seu comportamento, detetando eventuais riscos de segurança ou riscos para os direitos, liberdades e garantias.

**e) Do sistema disponibilizado pela Google e pela Apple**

45. A aplicação STAYAWAY está dependente, para o seu funcionamento nos moldes atuais, do sistema GAEN fornecido por estes dois grandes colossos do mundo digital. Se, por um

---

<sup>27</sup> O documento “Exposure Notification – Bluetooth Specification” prevê o seguinte: “The advertiser address type shall be Random Non-resolvable.” Disponível em [https://blog.google/documents/70/Exposure\\_Notification\\_-\\_Bluetooth\\_Specification\\_v1.2.2.pdf](https://blog.google/documents/70/Exposure_Notification_-_Bluetooth_Specification_v1.2.2.pdf)

<sup>28</sup> Sem prejuízo das observações feitas nos pontos 58, 60-61, a propósito dos riscos de re-identificação.

lado, isso traz garantias de robustez e segurança das soluções tecnológicas, ao mesmo tempo que permitiu processar a informação ao nível do sistema operativo, por outro, subtrai uma parte substantiva da operacionalização da aplicação ao controlo dos seus criadores.

46. Por outro lado, o código da GAEN API não é aberto, logo não sujeito a escrutínio, embora estejam publicamente disponíveis as especificações técnicas do protocolo, os algoritmos criptográficos e respetiva interface.

47. Uma das questões que suscita mais reservas prende-se com o facto de o sistema GAEN poder ser alterado, em sentido incerto<sup>29</sup>, por decisão unilateral daquelas empresas, o que poderá pôr em crise o comportamento da interface, com eventuais consequências negativas para a aplicação e para os utilizadores.

48. Tratando-se de empresas que detêm já grandes repositórios de informação e prestam serviços muito variados a nível global, permanece uma dúvida razoável sobre o eventual benefício (atual ou futuro) que possam ficar a retirar da disponibilização desta plataforma para o rastreio de contactos de proximidade, através de uma tecnologia que está em fase ascendente de utilização e que pode constituir, para todos os efeitos, um meio supletivo, porventura mais granular, aos métodos de localização existentes.

49. Se os dados processados no contexto deste tipo de aplicações forem de alguma forma utilizados para outros fins, as garantias do sistema ficam comprometidas, desde logo porque a pseudonimização é prejudicada e o risco de identificabilidade dos utilizadores é muito maior. Admite-se, todavia, que esta é uma questão difícil de ultrapassar, e que só vem acentuar a necessidade de os utilizadores fazerem escolhas informadas.

50. Este aspeto é, evidentemente, um dos pontos críticos deste tipo de aplicações, onde também se inclui a STAYAWAY. De qualquer modo, qualquer alteração a realizar na interface GAEN deverá ser prontamente notificada aos utilizadores, de modo que compreendam em pleno as consequências práticas da mudança.

---

<sup>29</sup> Tal como afirmado na análise preliminar realizada pelos fornecedores do sistema GAEN, este é sujeito a modificação e extensão.

f) Do tratamento de dados pessoais no sistema STAYAWAY

51. O sistema STAYAWAY prevê essencialmente o tratamento de dados pseudonimizados, cuja probabilidade de re-identificação será tratada mais adiante quando nos debruçarmos especificamente sobre a análise de riscos e vulnerabilidades, sem prejuízo das observações críticas realizadas neste capítulo.
52. Os dados pseudonimizados são, no entanto, dados pessoais, e verifica-se também haver tratamento de dados não pseudonimizados. Em termos gerais, considera-se que houve uma preocupação pelo respeito pelo princípio da minimização dos dados, pelo princípio da exatidão, e pelo princípio da limitação da conservação dos dados, os quais têm um período de armazenamento curto<sup>30</sup>, em estrita obediência ao cumprimento da finalidade do tratamento (cf. alíneas *b*), *c*), *d*) e *e*) do n.º 1 do artigo 5.º do RGPD). Contudo, destacam-se algumas insuficiências notórias que precisam de ser supridas.
53. Na AIPD é afirmado que as pessoas que queiram descarregar a aplicação não precisam de criar conta ou de se identificar. Ora, se isto não é especificamente exigido por referência à STAYAWAY, a verdade é que não é possível descarregar qualquer aplicação das lojas oficiais da Google ou da Apple, mesmo as gratuitas, sem o utilizador se autenticar, pelo que passa a ser, pelo menos, do conhecimento direto destas empresas que aquela pessoa, identificada (até eventualmente com cartão de crédito associado), é utilizadora da STAYAWAY.
54. Quanto aos dados tratados durante o funcionamento regular do sistema, verifica-se que os RPI têm associada a data, sendo assim possível saber a data de exposição a pessoa infetada. Admite-se que essa informação seja útil, mas nada é dito quanto ao benefício da sua utilização e de que modo é que essa informação será usada ou transmitida, o que seria naturalmente relevante.
55. Assinala-se também que o alerta de risco de exposição que é apresentado ao utilizador, quando detetado um contacto de proximidade com uma pessoa infetada, com base na última ocorrência, perdura na aplicação até esta ser desinstalada. Ora, essa situação pode

---

<sup>30</sup> Os identificadores são mantidos por um período até 14 dias, em qualquer componente do sistema; os alertas de risco são mantidos no dispositivo móvel com a data de ocorrência do mais recente contacto de proximidade que lhe deu origem até ser desinstalada a aplicação.

já não corresponder à verdade se o utilizador, na sequência da notificação, realizou teste à COVID-19 com resultado negativo, pelo que o estado apresentado deveria ser 'sem risco'. Deve pois ser revisto este procedimento para que a informação se encontra atualizada a todo momento, em cumprimento do princípio previsto na alínea *d)* do n.º 1 do artigo 5.º do RGPD.

56. Quanto aos dados tratados no SLD, sobre a data dos primeiros sintomas ou a data do teste no caso de indivíduos assintomáticos, também nada é adiantado nem explicada a finalidade desta informação. Acresce que se ignora como é essa informação introduzida no sistema, se pelo profissional de saúde e, neste caso, se com conhecimento e autorização prévia do doente; se diretamente pelo doente. Também não é explicado quando é essa informação inserida e, portanto, se o preenchimento desses campos é condição para prosseguir com a obtenção do código de legitimação. Além disso, parece estar previsto um apagamento automático desta informação, uma vez que também é armazenado no SLD uma data de validade para os dados introduzidos, mas desconhece-se qual é esse prazo de conservação. Mesmo admitindo que, no contexto do controlo epidemiológico ou da análise da eficácia da própria aplicação, o conhecimento dessas datas seja relevante, será necessário esclarecer os seus fins e as condições para o tratamento desses dados.

57. Ainda no plano do SLD, entende-se ser de referir que nada é adiantado quanto ao contexto e à forma de autenticação dos profissionais de saúde para obter os códigos CL, embora se admita que essa será uma das questões diferidas para uma fase posterior de enquadramento legal e de definição do responsável pelo tratamento. De qualquer modo, é extremamente importante que a solução que venha a ser adotada não faça perigar a segurança do sistema.

58. No que diz respeito aos dados processados no SLD e no SPD, verifica-se ainda que é tratado um identificador único universal (uuid) sem referência ao que está a identificar. Com efeito, na descrição da estrutura de dados dos servidores<sup>31</sup> da AIPD consta o tratamento

---

<sup>31</sup> Este identificador único universal também está integrado no código de acesso (CA), que fica posteriormente armazenado no SPD, embora não seja descrito durante quanto tempo ou se este é coincidente com o prazo de conservação das chaves TEK, que é de 14 dias.

deste dado. Não se pode deixar de sublinhar que nada é mencionado sobre a finalidade do tratamento deste dado, como é utilizado ou por quanto tempo é conservado.

59. Dependendo daquilo a que este identificador único se refere, o seu tratamento pode ter impacto na privacidade do utilizador se de alguma forma permitir individualizá-lo inequivocamente, e, por conseguinte, poder monitorizar as suas interações com os servidores centrais do sistema STAYAWAY. Para se poder aferir da sua adequação e necessidade, é essencial explicitar o seu objetivo no âmbito da operacionalização do sistema. Tem de ser demonstrado que o tratamento deste dado pessoal no SLD e no SPD cumpre o princípio da minimização dos dados previsto na alínea c) do n.º 1 do artigo 5.º do RGPD.
60. Quanto ao tratamento do dado relativo ao endereço IP do utilizador que comunica com o SPD, é declarado que este é tratado para fins de segurança do sistema e controlo de tentativas de intrusão e apenas acessível pelos administradores de sistema. 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).
61. 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<sup>32</sup>. Tendo em consideração que os utilizadores da aplicação acedem ao SPD diariamente, por quatro vezes, e que, acrescidamente, alguns utilizadores podem ser referenciados como pessoas com um diagnóstico positivo para a COVID-19, quando se autenticam para envio das respetivas chaves TEK, especiais salvaguardas devem ser adotadas quanto ao tratamento deste dado pessoal.
62. Considera-se legítima a finalidade indicada para o armazenamento dos dados IP, por um curto período de tempo, embora deva ser suficiente para permitir cumprir plenamente o objetivo em vista. Contudo, para minimizar os riscos de utilização indevida e em linha com as melhores práticas seguidas neste domínio, o sistema STAYAWAY deve introduzir um mecanismo de *reverse proxy*, mascarando os IPs dos utilizadores, o qual deveria

---

<sup>32</sup> 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.

preferencialmente ser administrado por equipa distinta, isto é, devem ser segregadas as funções de administração e suporte do STAYAWAY das de segurança da infraestrutura.

**g) Dos direitos dos utilizadores enquanto titulares dos dados**

63. Um dos pontos fulcrais para um tratamento de dados pessoais transparente e que permita ao titular dos dados uma escolha esclarecida e, também nessa medida, verdadeiramente livre porque decorre de uma opção consciente, é a informação prévia que lhe é prestada em relação às condições do tratamento que é proposto fazer aos seus dados pessoais.
64. De acordo com a AIPD, prevê-se que seja prestada informação ao utilizador, quer no sítio da Internet da STAYAWAY, quer na própria aplicação. É importante que esta informação seja facultada cumprindo os requisitos de inteligibilidade do artigo 12.º do RGPD e atendendo aos públicos diferenciados que podem estar aqui em causa, em particular grupos mais vulneráveis como as crianças, que detêm dispositivos móveis modernos (em versões necessárias para correr a aplicação) a partir de uma idade inferior a 13 anos<sup>33</sup>.
65. Também a informação relativa ao próprio funcionamento da aplicação deve ser clara, para que os utilizadores a utilizem corretamente, contribuindo assim para o cumprimento do seu objetivo, sem prejuízo naturalmente da sua opção de em qualquer momento não fornecer mais dados ou desinstalar a aplicação.
66. No que diz respeito ao exercício dos restantes direitos previstos no RGPD, por não ser possível a identificação do titular a partir dos dados tratados, os direitos não são aplicáveis por força do artigo 11.º, n.º 2, do RGPD.

**h) De outros riscos e vulnerabilidades**

67. Ao realizar uma análise de riscos e vulnerabilidades do sistema, além de alguns riscos já acima mencionados, a AIPD examina vários cenários de tentativas de re-identificação dos titulares dos dados por recurso a sistemas externos ou por inferência dos próprios

---

<sup>33</sup> Por referência à idade prevista na Lei n.º 58/2019, de 8 de agosto, dando execução ao artigo 8.º do RGPD, para consentir no tratamento dos seus dados pessoais quando lhes são especificamente dirigidos serviços da sociedade de informação.

utilizadores, sendo que, neste último caso, tal é intrínseco a um sistema de notificação de exposição individual, que conduz a uma tentativa de reconstrução dos contactos passados quando existe um caso de infeção. O sucesso deste exercício depende em muito das condições particulares em que se movimenta cada utilizador (número de contactos de proximidade, locais/ritmo de deslocação). De uma maneira geral, a CNPD concorda com o resultado da análise feita e com as medidas previstas para mitigar esses riscos.

68. A gravidade e probabilidade dos riscos enunciados, relativamente a ameaças e fontes de risco, com a execução de determinados controlos e políticas, é classificada pela AIPD como 'limitada' ou 'insignificante'<sup>34</sup>.

69. Também foi analisada a possibilidade de criação de falsos alertas com base em reencaminhamento malicioso de RPI ilegítimos de utilizadores diagnosticados com COVID-19. Uma vez que estas interações se realizam no sistema operativo dos dispositivos móveis, esta vulnerabilidade teria de ser solucionada pelo GAEN, sem prejuízo de outras formas de mitigação que possam ser implementadas ao nível do sistema.

70. Em suma, do ponto de vista da segurança do tratamento de dados, foram adotadas medidas importantes previstas no artigo 32.º do RGPD, em particular a pseudonimização dos dados, a complementar medidas relevantes decorrentes da aplicação do princípio previsto no artigo 25.º do RGPD, quanto à proteção de dados desde a conceção e por defeito. O apagamento automático dos dados e o seu curto armazenamento são essenciais no sentido de minimizar o nível de afetação dos direitos das pessoas em caso de ocorrência de incidentes de segurança. Não deixa de se reforçar que os criadores da aplicação STAYAWAY não detêm o controlo total dos dados tratados, uma vez que o tratamento realizado pelo sistema operativo dos dispositivos móveis do utilizador é da responsabilidade do sistema GAEN.

#### IV. Utilização futura do sistema

71. Como mencionado na Introdução desta deliberação, restam algumas indefinições quanto ao funcionamento da aplicação STAYAWAY, decorrentes não só do desconhecimento do

---

<sup>34</sup> Numa escala de Indefinido/Insignificante/Limitado/Significativo/Máximo.

responsável pelo tratamento e das suas determinações em relação a questões concretas, tais como a intervenção do profissional de saúde neste sistema, mas também da evolução do cenário de interoperabilidade com outras aplicações para fim idêntico no espaço da União Europeia e noutros espaços geográficos.

72. Todavia, a CNPD não pode deixar de, neste contexto, adiantar algumas considerações elementares para uma futura utilização da STAYAWAY ou de outra aplicação similar.

73. De acordo com o que é afirmado pela parceria Apple/Google, o acesso à interface GAEN para a operacionalização de aplicações de notificação de exposição com base no rastreio de contactos de proximidade, só é concedido para uso das autoridades públicas de saúde e apenas a uma única aplicação por país, considerada aplicação oficial.

74. Consequentemente, para o funcionamento da STAYAWAY ser possível terá de haver o envolvimento ativo de autoridade pública de saúde, daí a imprescindibilidade de o responsável pelo tratamento de dados ser uma entidade pública nacional com atribuições na área da saúde e competências específicas ajustadas à finalidade da aplicação.

75. Por outro lado, atendendo ao próprio objetivo da aplicação, que se assume como um meio complementar na estratégia nacional de combate à pandemia, disponibilizando um instrumento adicional para detetar pessoas potencialmente infetadas ou com risco de contágio, direcioná-las para vigilância médica e/ou confinamento e, assim, contribuir para interromper as cadeias de transmissão da doença, a disponibilização pública da aplicação tem de estar integrada num planeamento nacional apropriado a este cenário.

76. Com efeito, do ponto de vista da proteção de dados, à luz do disposto na alínea i) do n.º 2 do artigo 9.º do RGPD, afigura-se necessário que seja dado enquadramento legal ao responsável pelo tratamento que, por sua vez, tem de estar em condições de poder tomar certas decisões, eventualmente com base no interesse público importante de proteção da saúde pública numa situação de pandemia, mas sempre norteadas pelo princípio da proporcionalidade e com salvaguardas adequadas, tal como prescrito pelo RGPD.

77. Até porque, em todo este processo, a intervenção imprescindível de um profissional de saúde (médico), para validar o diagnóstico e poder fazer avançar a deteção de eventuais contactos de proximidade em risco e do correspondente sistema de notificação, também

parece depender de enquadramento legal para que a aplicação possa funcionar, não bastando por isso a adesão voluntária do utilizador.

78. Na verdade, considerando a relevância, para a fidedignidade do sistema de informação, desta intervenção médica, afigura-se imprescindível a sua previsão e regulação no plano legal, não apenas para a legitimar, mas sobretudo para assegurar que ela ocorra, sob pena de ficar na disponibilidade do médico o funcionamento do sistema de notificação.

79. É também muito importante para a segurança global do sistema STAYAWAY e para a manutenção da pseudonimização dos dados tratados na aplicação que a forma de autenticação do médico no SLD, bem como as condições da sua interação com o sistema, sejam devidamente acauteladas.

80. Note-se, porém, que a exigência de normação legal deste tratamento não afasta o carácter voluntário da utilização da aplicação pelo utilizador – e que é indispensável ser mantido, como aliás decorre das recomendações da OMS, da Comissão Europeia<sup>35</sup> e do Comité Europeu de Proteção de Dados<sup>36</sup>; a condição de licitude do tratamento dos dados de proximidade e de saúde é, em primeira linha, o consentimento do titular, correspondendo à sua manifestação de vontade inequívoca à instalação da aplicação no seu dispositivo móvel, desde que cumpridos os quatro requisitos que tornam o seu consentimento válido (previstos na alínea 11) do artigo 4.º do RGPD).

81. Mas como o funcionamento da aplicação implica operações de tratamento distintas que envolvem diferentes categorias de titulares (utilizadores e profissionais de saúde), além da exigência feita pelo sistema GAEN para a operacionalização da aplicação, o tratamento de dados realizado exige uma dupla condição de licitude deste tratamento, o que só reforça a sua legitimidade e torna o tratamento mais proporcional.

82. Por último, é ainda de referir a questão da interoperabilidade da aplicação nacional com outras aplicações no seio da União, no seguimento do acordo alcançado este mês entre os Estados-Membros sobre um conjunto de especificações técnicas<sup>37</sup>, com vista à troca de informações entre as aplicações de contacto de proximidade nacionais baseadas em

---

<sup>35</sup> [https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020XC0417\(08\)&from=EN](https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020XC0417(08)&from=EN)

<sup>36</sup> [https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing\\_en](https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_en)

<sup>37</sup> [https://ec.europa.eu/health/ehealth/key\\_documents\\_en#anchor0](https://ec.europa.eu/health/ehealth/key_documents_en#anchor0)

modelos descentralizados. Está previsto que a Comissão Europeia disponibilize uma plataforma através da qual será trocada a informação relativa às várias aplicações nacionais quando os utilizadores viajarem na União.

83. Nem tudo está ainda definido e há opções diferentes para identificar os países por onde circulou um determinado utilizador. De qualquer modo, é evidente que haverá tratamento de mais dados pessoais. Por outro lado, a interoperabilidade traz riscos adicionais quanto à proteção dos dados pessoais e da privacidade, na medida em que o sistema se torna aberto e interage com outros sistemas que, ainda que com modelos semelhantes, terão estruturas de dados diferenciadas, salvaguardas distintas, formas de administração diferentes.

84. É, pois, da maior relevância garantir que com a interoperabilidade as salvaguardas em matéria de proteção de dados não sucumbem a um mínimo denominador comum; antes pelo contrário, deve procurar atingir-se um nível elevado de proteção, presidido pela transparência de todo o processo e com o escrupuloso respeito pelos princípios da limitação da finalidade, minimização dos dados, limitação da conservação, integridade e confidencialidade.

## V. Conclusões

Com base nos fundamentos acima expostos, a CNPD considera que:

85. O sistema STAYAWAY COVID, da iniciativa do INESC-TEC e do ISPUP, mantém algumas indefinições quanto ao seu funcionamento, as quais dependem da execução concreta que possam vir a ter, a ser determinada pelo responsável pelo tratamento de dados, pelo que a pronúncia desta Comissão sobre algumas questões específicas ficará também diferida para momento posterior;

86. O sistema deve preservar o seu carácter voluntário, devendo ser facultado ao utilizador, tal como previsto, vários momentos em que pode livremente fazer opções quanto ao tratamento dos seus dados, incluindo a possibilidade efetiva de desligar o Bluetooth, configurar a aplicação para não rastrear os contactos de proximidade e desinstalar a

- aplicação, tendo como consequência a interrupção ou o apagamento definitivo dos seus dados pessoais;
87. A utilização da tecnologia Bluetooth afigura-se menos intrusiva do que o recurso a uma tecnologia que permitisse de imediato registar a localização do utilizador; todavia, não está isenta de riscos e, ao ser imprescindível que o BLE esteja ativo para que a aplicação funcione, está a habilitar o rastreamento constante da localização e movimentações dos utilizadores por terceiros;
88. O modelo descentralizado do sistema STAYAWAY é mais adequado do ponto de vista da proteção de dados por dispersar as operações de tratamento, evitando um tratamento centralizado de todos os dados, o que acarretaria riscos adicionais de utilização indevida, interconexão de dados ou re-identificação dos utilizadores. O facto de o código fonte da aplicação ir ser tornado público é um fator importante de transparência;
89. O recurso à interface da Google e da Apple é um dos aspetos mais críticos da aplicação, na medida em que há uma parte crucial da sua execução que não é controlada pelos autores da aplicação ou pelos responsáveis pelo tratamento. Esta situação é ainda mais problemática porque o GAEN declara que o seu sistema está sujeito a modificações e extensões, por decisão unilateral das empresas, sem que se possa antecipar os efeitos que tal pode ter nos direitos dos utilizadores;
90. No respeito pelo princípio da transparência, os titulares dos dados devem estar sempre cientes de todos os aspetos do funcionamento da aplicação e das suas implicações para o tratamento dos seus dados pessoais e para a sua privacidade, e devem manter o controlo dos seus dados. Isto é tanto mais importante quanto muitas interações ocorrem automaticamente, sem que o utilizador se aperceba delas;
91. Apesar de se reconhecer, no desenho do sistema, ter havido uma preocupação pelo princípio da minimização dos dados e pela pseudonimização dos dados, prevê-se o tratamento de alguns dados além dos identificadores pseudoaleatórios que sustentam o sistema de notificação, os quais não são avaliados na AIPD, sendo desconhecida a sua finalidade, a sua inserção no sistema, a sua transmissão ou o seu prazo de conservação, pelo que é essencial que tal seja clarificado;

92. A avaliação de impacto deve ser revista, tendo em conta os aspetos críticos sinalizados pela CNPD e que não foram objeto de análise, designadamente a omissão quanto à finalidade e às condições de tratamento de dados (cf. data do RPI, data de primeiros sintomas ou data de teste COVID para assintomáticos, identificadores únicos universais), bem como atendendo a algumas recomendações adicionais feitas, quanto à indefinição de alguns prazos de conservação ou relativas ao IP dos utilizadores quando comunicam com o Serviço de Publicações de Diagnóstico.

Ainda a propósito da avaliação de impacto realizada, mas quanto a aspetos do tratamento de dados pessoais que não estão ainda definidos, a CNPD recomenda que:

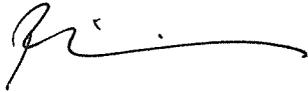
93. Seja dado enquadramento legal para o funcionamento do sistema STAYAWAY, não só porque o acesso à interface GAEN só é concedido às autoridades públicas de saúde, e apenas a uma aplicação por país, como também a fidedignidade do sistema depende da validação do diagnóstico médico, pelo que se afigura imprescindível a previsão e regulação no plano legal da intervenção daquele profissional de saúde. Especiais salvaguardas devem ser adotadas quanto à forma como o médico se autentica e interage com o sistema para garantir a segurança global do STAYAWAY e para a manutenção da pseudonimização dos dados tratados;

94. A exigência de normação legal deste tratamento não afaste o carácter voluntário da utilização da aplicação pelo utilizador. A condição de licitude dos dados pessoais de saúde e dos respetivos contactos de proximidade é, em primeira linha, o consentimento do titular, correspondendo à sua manifestação de vontade inequívoca a instalação da aplicação no seu dispositivo móvel, desde que cumpridos os quatro requisitos que tornam o seu consentimento válido. Atento o modo de funcionamento da aplicação que implica operações de tratamento distintas, envolvendo duas categorias de titulares de dados, o tratamento exigirá uma dupla condição de licitude, o que só reforça a sua legitimidade;

95. A interoperabilidade entre as aplicações nacionais de rastreamento de contactos de proximidade implica o tratamento de mais dados, mais comunicações e mais destinatários, pelo que é preciso garantir que as opções tomadas nesse contexto respeitam os princípios de proteção de dados, em particular o princípio da minimização. Do mesmo modo, há que garantir que, com a interoperabilidade, as salvaguardas em matéria de proteção de dados

não sucumbem a um mínimo denominador comum, mas antes procuram atingir um nível elevado de proteção da privacidade dos seus utilizadores.

Aprovada na reunião de 29 de junho de 2020



Filipa Calvão (Presidente)