Avaliação de Impacto sobre a Proteção de Dados

SISTEMA STAYAWAY COVID

Porto

11 de agosto de 2020

STAYAWAY COVID

Controlo do documento

Documento	Avaliação de Impacto sobre a Proteção de Dados - SISTEMA STAYAWAY COVID
Nível de distribuição	Público
Data do documento	11 de agosto de 2020
Versão atual	v.2.0
Versões anteriores	v.1.0 (15/06/2020); v.1.1 (22/06/2020); v.1.2 (07/07/2020); v.1.3 (17/07/2020)
Responsáveis pelo documento	INESC TEC e ISPUP
Autores	Vasco Dias [(EPD) INESC TEC e ISPUP]; Jaime Dias [INESC TEC]; Rita Barros [INESC TEC]; Tiago Freire [INESC TEC]; José Orlando Pereira [INESC TEC]; Rui Oliveira [INESC TEC]; Henrique Barros [ISPUP]; Francisco Maia [Keyruptive]
Revisores	Ana Alonso [INESC TEC]; Rogério Pontes [INESC TEC]; Lino Santos [CNCS]; Mariana Meira [SPMS]
Contactos	dpo@inesctec.pt proteccao.dados@spms.min-saude.pt

Nota de apresentação

O presente relatório, preparado pelo INESC TEC, ISPUP e Keyruptive, serve o intuito de proceder a uma primeira avaliação de impacto sobre a proteção de dados (AIPD) relativa ao sistema informático designado STAYAWAY COVID. O sistema é uma iniciativa do INESC TEC e do ISPUP no âmbito do programa INCoDe.2030 para rastreio da propagação da COVID-19, através da utilização voluntária de uma aplicação para dispositivos móveis pessoais**.** A sua elaboração acompanhou o desenvolvimento breve e particularmente intenso deste sistema cujos trabalhos iniciais remontam a abril de 2020, a partir da colaboração com o consórcio internacional do projeto DP^3T, e em resposta ao urgente desafio sanitário colocado pela pandemia da COVID-19, antecipando a entrada numa nova fase da mesma, coincidindo com o gradual desconfinamento da população, na sequência do fim da vigência do Estado de emergência e do Estado de calamidade em Portugal.

O presente relatório serve a documentação consolidada da avaliação de impacto sobre a proteção de dados, que deve ser realizada nos termos do artigo 35.º do RGPD, numa fase em que as características principais da aplicação podem já considerar-se definidas, sem prejuízo dos trabalhos de desenvolvimento ainda em curso e da indefinição quanto à entidade ou entidades a quem será, em concreto, acometida a tarefa de operacionalizar o sistema, e bem assim, que venham a assumir-se como responsáveis pelo tratamento de dados, na aceção legal do termo.

Tal como a própria aplicação STAYAWAY COVID, também esta avaliação de impacto deverá continuar a ser atualizada e ampliada. A este propósito, será de sublinhar que a presente avaliação deverá ser entendida como um processo que nunca estará completo enquanto a aplicação for desenvolvida ou permanecer disponível para utilização. Por conseguinte, esta avaliação deverá ser vista como um "documento vivo", constantemente atualizado.

As futuras revisões e a sua final publicação poderão, deste modo, ser conduzidas por outras entidades sob cuja alçada venha a ser colocada a fase de operacionalização do sistema, desenhado para constituir um recurso adicional ao serviço de uma estratégia global de saúde pública, fazendo face à evolução da epidemia da COVID-19 no território nacional.

Nota relativa às versões anteriores:

Na sequência da versão 1.1., que foi objeto da Deliberação 2020/277 da CNPD, de 29 de junho, a versão 1.2, constituiu uma mera revisão daquela versão, não deixando, porém, de endereçar algumas das recomendações e questões suscitadas pela CNPD na citada Deliberação.

Desta forma passou inclui-se em apêndice (Apêndice D), uma tabela alusiva às principais questões e recomendações elaboradas pela CNPD, acompanhadas de esclarecimentos e notas informativas relativas a medidas implementadas ou cuja implementação se encontra planeada. Para facilitação da leitura, na mesma tabela incluem-se referências aos pontos da Deliberação em questão, bem como às passagens do texto da AIPD onde poderão ser encontradas indicações mais completas sobre alguns dos tópicos assinalados. Para além disso, e de revisões formais do texto, foi acrescentado o Apêndice C que contém ilustrações gráficas da análise de risco elaborada na secção 6.4, com base na tríade CIA.

De fora da versão 1.2. ficaram os aspetos relacionados, por um lado, com o sistema de autenticação dos profissionais de saúde para a obtenção de códigos de legitimação e, por outro, com a interoperabilidade com sistemas similares de outros Estados membros da UE.

A versão 1.3. procedeu a muito ligeiras correções formais, incluindo uma referência à designação da DGS como responsável pelo tratamento de dados.

A versão 2.0. inclui as atualizações necessárias na sequência do desenho e implementação da solução que preside à integração da aplicação com o sistema Tracecovid-19, a cargo dos SPMS, bem como dos pormenores da forma de autenticação dos profissionais de saúde (apenas médicos), designadamente com vista à obtenção dos códigos CL, componentes estas que não se encontravam ainda descritas nas versões anteriores. Também se especificam, nesta versão, aspetos relativos ao alojamento e operação dos servidores SLD e SPD bem como, a título processual, o circuito previsto ao nível da intervenção dos médicos no sistema STAYAWAY COVID. Atualizam-se, finalmente, as referências feitas ao enquadramento legal do sistema fruto da publicação do Decreto-Lei 52/2020, de 11 de agosto, que estabelece a DGS como o responsável pelo tratamento de dados e regula a intervenção do médico no sistema.

Abreviaturas e acrónimos

AEPD	Autoridade Europeia da Proteção de Dados
AIPD	Avaliação de Impacto sobre a Proteção de Dados
APP	Aplicação
BLE	Bluetooth Low Energy
CA	Código de Acesso
CDFUE	Carta dos Direitos Fundamentais da União Europeia
CEPD	Comité Europeu para a Proteção de Dados
CL	Código de Legitimação
CNCS	Centro Nacional de Cibersegurança
CNIL	Commission Nationale de l'Informatique et des Libertés
CNPD	Comissão Nacional de Proteção de Dados
CRP	Constituição da República Portuguesa
DDoS	Distributed Denial of Service
DGS	Direção-Geral da Saúde
DMP	Dispositivos Móveis Pessoais
DP^3T	Decentralized Privacy-Preserving Proximity Tracing
EPD	Encarregado da Proteção de Dados
GAEN	Google Apple Exposure Notification API
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GT29	Grupo de Trabalho do Artigo 29.º
ICO	Information Commissioner's Office
IMEI	International Mobile Equipment Identity
INCM	Imprensa Nacional-Casa da Moeda
INESC TEC	Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência
IP	Internet Protocol
ISPUP	Instituto de Saúde Pública da Universidade do Porto
OMS	Organização Mundial da Saúde
PRVR	Portal de Requisição de Vinhetas e Receitas

PS	Profissional de Saúde
RGPD	Regulamento Geral de Proteção de Dados
RPI	Rolling Proximity Identifier
SLD	Serviço de Legitimação de Diagnóstico
SPD	Serviço de Publicação de Diagnóstico
SPMS	Serviços Partilhados do Ministério da Saúde
TC-19	Trace COVID-19
TEK	Temporary Exposure Key
TFUE	Tratado sobre o Funcionamento da União Europeia
TI	Tecnologias de Informação
UE	União Europeia

Sumário:

1. Introdução

O sistema STAYAWAY COVID é uma iniciativa no âmbito do programa INCoDe.2030 para o desenvolvimento de uma solução de rastreio da propagação da COVID-19, através da utilização voluntária de uma aplicação para dispositivos móveis pessoais com sistema operativo iOS ou Android. Esta aplicação destina-se, num pressuposto de utilização estritamente voluntária, a ser um meio complementar ao serviço de uma estratégia global de resposta a uma situação de emergência de saúde pública determinada pela pandemia da COVID-19, tendo por funcionalidade principal alertar o seu utilizador se este tiver estado em contacto de proximidade com outros utilizadores da aplicação a quem foi diagnosticada COVID-19. Em rigor, mais do que de uma solução de rastreio, do ponto de vista técnico, trata-se de uma aplicação de notificação da exposição individual a fatores de risco de contágio. Nessa medida servirá de complemento aos esforços tradicionalmente levados a cabo pelas autoridades de saúde no intuito de rastrear e interromper cadeias de transmissão da doença.

As entidades responsáveis pelo desenvolvimento desta solução são o INESC TEC e o ISPUP com o apoio das empresas Keyruptive e Ubirider e a colaboração da SPMS.

1.1. Propósitos e objetivos

O sistema STAYAWAY COVID foi concebido com a constante preocupação de conciliar a sua utilidade com a preservação da privacidade dos utilizadores. Este equilíbrio, norteou, desde o início, as opções de arquitetura que determinam a transmissão, armazenamento e processamento dos dados em todo o sistema.

Não obstante, embora de formas diferentes, tanto o rastreio tradicional, como o rastreio digital de contactos de proximidade não deixam de envolver o tratamento de dados pessoais, na aceção legal do conceito, ainda que sob a forma de pseudónimos, não constituindo exceção uma solução assente num modelo descentralizado como é o caso da STAYAWAY COVID.

Acresce que, sempre que digam respeito a pessoas diagnosticadas com COVID-19, os dados pessoais em causa qualificados, igualmente, como dados de saúde, merecem uma tutela especial ao abrigo da legislação aplicável em matéria de dados pessoais, designadamente, o regime de proibição de tratamento por princípio, resultante do artigo 9.º do RGPD.

O registo de informação sobre um encontro de proximidade entre dois utilizadores da aplicação é efetuado através da tecnologia Bluetooth, especialmente Bluetooth Low Energy (BLE). Não existe qualquer registo da localização do utilizador, permitindo apenas que as instâncias da aplicação instaladas nos dispositivos móveis dos utilizadores mantenham um registo dos encontros de proximidade com dispositivos móveis de outros utilizadores. Em nenhum momento a identidade de um utilizador será revelada, seja pela instância da aplicação instalada num dispositivo móvel, seja pela base de dados alojada num servidor central, como adiante melhor se explicará.

Embora os dados tratados pelo sistema não revelem a identidade dos utilizadores, consideramos que o conjunto de códigos aleatórios, mas únicos e necessários ao seu funcionamento dizem respeito a pessoas singulares identificáveis, que poderão vir a ser notificadas por um alerta de exposição de risco como decorrência da respetiva utilização da aplicação. Por esta razão, apesar de insuscetível de identificar diretamente uma pessoa singular, entendemos que os referidos dados, enquanto pseudónimos ou dados pseudonimizados,

devem ser classificados como dados pessoais, aos quais se aplicam as disposições do RGPD e demais legislação de proteção de dados pessoais vigente.

Dado o funcionamento do sistema envolver o tratamento de dados pessoais, incluindo dados de saúde ou dados relativos à saúde de pessoas singulares, concluímos, assim, pela necessidade de conduzir a presente AIPD.

Como determina o artigo 35.º do RGPD, uma avaliação deste tipo é necessária perante certo tipo de tratamento de dados, em particular, os que utilizem novas tecnologias, quando considerando a sua natureza, âmbito, contexto e finalidades, o mesmo seja suscetível de implicar riscos elevados para os direitos e liberdades das pessoas singulares. A obrigatoriedade de uma tal avaliação resulta de forma expressa do n.º 3 do referido artigo, já que os tratamentos de dados em causa preenchem as hipóteses das duas primeiras alíneas. Com efeito, poderão aqueles, por um lado, implicar a avaliação sistemática e completa de aspetos pessoais relativos a indivíduos, baseada em tratamentos automatizados, podendo conduzir a decisões que produzam efeitos jurídicos ou os afetem significativamente.

A este título, cumpre dizer que o cariz voluntário da utilização da aplicação deverá, em nossa opinião, abranger todo o ciclo da sua utilização, inviabilizando a produção de efeitos jurídicos na esfera das pessoas singulares que a utilizem. Neste sentido, a única consequência a que poderão estar sujeitos os utilizadores será, nesse caso, a receção de alertas de exposição a um risco de contágio derivado da proximidade com uma pessoa diagnosticada com COVID-19. Ademais, estamos perante operações de tratamento de dados potencialmente em larga escala (sendo este, de resto, um dos fatores que contribuirá para a eficácia da solução) e, como vimos, de categorias especiais de dados à luz do artigo 9.º do RGPD.

Uma AIPD, genericamente, tem por essenciais propósitos: descrever de forma sistemática as operações de tratamento de dados previstas; avaliar se essas operações de tratamento são necessárias e proporcionais em relação às finalidades para as quais o sistema será aplicado; e identificar os riscos para os direitos e liberdades das pessoas singulares decorrentes daquelas operações de tratamento de dados, bem como, as medidas que devem ser adotadas por forma a mitigá-los ao ponto de se tornarem aceitáveis no contexto considerado.

Reconhecemos que a confiança do público na aplicação é fundamental para o seu êxito e que a mencionada confiança dependerá, em larga medida, da transparência em torno do funcionamento do sistema e dos seus controlos de privacidade.

1.2. Metodologia utilizada para elaboração da Avaliação de Impacto sobre a Proteção de Dados

Para efetuar a presente AIPD, de acordo com o artigo 35.º do RGPD, utilizou-se uma abordagem holística e integradora de contributos de várias das metodologias mais relevantes, incluindo os principais standards internacionais de análise de risco como a ISO 27001, ISO 27701, ISO 29134 e ISO 31000, orientações do Comité Europeu para a Proteção de Dados e do Grupo de Trabalho do Artigo 29.º (GT Art. 29.º) que lhe precedeu, bem como metodologias e orientações desenhadas por autoridades de supervisão nacionais, com destaque para as da CNIL[1] e da ICO[2]

[1] Podem ser consultadas mais informações sobre a metodologia da CNIL em: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf.

[2] Podem ser consultadas mais informações sobre a metodologia da ICO em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/.

para análise dos riscos do sistema para os titulares de dados pessoais. Diversos documentos foram utilizados para suportar a análise efetuada, destacando-se os seguintes:

- Parlamento Europeu e Conselho da União Europeia. 2016. "Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)". https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016R0679.
- Assembleia da República. 2019. "Lei n.º 58/2019 de 8 de agosto". Diário da República I Série, 151 (agosto): 3 – 40. https://dre.pt/pesquisa/-/search/123815982/details/maximized.
- Comissão Nacional de Proteção de Dados. 2018. "Regulamento n.º 798/2018 de 30 de novembro". Diário da República II Série, 231 (novembro): 32031 – 32032. https://dre.pt/home/-/dre/117182365/details/maximized.
- Article 29 Data Protection Working Party. 2017. "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679". Working Paper WP 248. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.
- ISO (International Organization for Standardization). 2013. Information technology — Security techniques — Information security management systems — Requirements. ISO/IEC 27001. (s.l.): ISO.
- ISO (International Organization for Standardization). 2017. Information technology — Security techniques — Guidelines for privacy impact assessment. ISO/IEC 29134. (s.l.): ISO.
- ISO (International Organization for Standardization). 2019. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. ISO/IEC 27701. (s.l.): ISO.
- ISO (International Organization for Standardization). 2009. Risk management — Principles and guidelines. ISO 31000. (s.l.): ISO.
- Centro Europeu de Prevenção e Controlo das Doenças. 2020. Rastreio de contactos: gestão da saúde pública de pessoas, incluindo profissionais de saúde, que tiveram contacto com casos de COVID-19 na União Europeia – segunda atualização. Estocolmo. https://www.ecdc.europa.eu/sites/default/files/documents/Public-health-management-people-in-contact-with-COVID19-cases_PT_0.pdf.
- Comissão Europeia. 2020. Orientações respeitantes a aplicações móveis de apoio à luta contra a pandemia de COVID-19 na perspetiva da proteção de dados (2020/C 124 I/01). https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN.
- Comité Europeu para a Proteção de Dados. 2020. Diretrizes 4/2020 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19. https://edpb.europa.eu/our-work-tools/our-documents/usmernenia/guidelines-042020-use-location-data-and-contact-tracing_pt.
- DP^3T Project. 2020. Data Protection Impact Assessment Report. https://github.com/DP-3T/documents/blob/master/data_protection/DP-3T%20Model%20DPIA.pdf.
- Bock, Kirsten. [et al.]. 2020. "Data Protection Impact Assessment for the Corona App". Versão 1.6: Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V. https://www.fiff.de/presse/dsfa-corona-english.

2. Descrição do sistema

Os sistemas digitais para rastreio de proximidade, *contact tracing*, com recurso a dispositivos móveis pessoais, que têm vindo a ser desenvolvidos no contexto da emergência de saúde pública resultante da pandemia da COVID-19, podem ser agrupados em três categorias, consoante o tipo de dados dos sensores utilizados para a avaliação de proximidade:

- Processamento de dados de localização (dados de GPS e meta-dados do dispositivo móvel).
- Processamento de dados de deslocação (dados agregados de GPS e meta-dados do dispositivo móvel).
- Processamento de dados de contacto (sensores de proximidade, e.g. Bluetooth).

O sistema STAYAWAY COVID corresponde à terceira categoria, recorrendo exclusivamente a sensores de proximidade, especificamente à comunicação de curta distância utilizando BLE. Neste grupo, a arquitetura dos sistemas atualmente propostos subdividem-se ainda segundo o modelo:

- Centralizado: todos os dados de contactos são coligidos, armazenados e processados num servidor central do sistema. O servidor calcula as funções de risco e notifica os utilizadores considerados em risco de contágio.
- Descentralizado: todos os dados são armazenados e processados no dispositivo móvel que os recolhe. Os pseudónimos ou dados pseudonimizados de um utilizador diagnosticado com COVID-19, são armazenados e disponibilizados num servidor central do sistema. O cálculo de risco e notificação do utilizador são efetuados localmente no dispositivo móvel.

O STAYAWAY COVID adota o modelo descentralizado desenvolvido no projeto DP^3T (https://https://github.com/DP-3T), posteriormente também adotado para o sistema de Notificação de Exposição Google-Apple (GAEN)[3][4][5] para Android e IOS.

A abordagem baseia-se na troca de identificadores alfanuméricos aleatórios (pseudónimos) entre os dispositivos móveis que se cruzam. Se e quando a um destes identificadores for associado um utilizador diagnosticado com COVID-19, os dispositivos móveis que o receberem podem levar a cabo uma avaliação de risco dependente da proximidade física e da duração da exposição. Para a sua implementação, o sistema, para além dos dispositivos móveis dos utilizadores, inclui dois servidores, sob controlo de uma entidade oficial, que disponibilizam os pseudónimos dos dispositivos móveis dos utilizadores com diagnóstico de COVID-19 legitimado.

A conceção do sistema STAYAWAY COVID foi iniciada antes da disponibilização da interface de Notificação de Exposição Google-Apple (GAEN API), tendo, entretanto, sido adaptado para a utilização das novas funcionalidades que esta permite. O protocolo implementado pela GAEN API é muito próximo do protocolo DP^3T. Contudo, ao contrário deste último, o protocolo de

[3] Exposure Notification - Bluetooth Specification. April 2020 v1.2. Google, Apple. Accessed 25 May, 2020. https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf.

[4] Exposure Notification - Cryptography Specification. April 2020 v1.2. Google, Apple. Accessed 25 May, 2020. https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-CryptographySpecificationv1.2.pdf.

[5] Exposure Notification - Frequently Asked Questions. May 2020 v1.1. Google, Apple. Accessed 5 June, 2020. https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.1.pdf.

geração de chaves, a divulgação de pseudónimos entre dispositivos móveis e a gestão das chaves/identificadores no dispositivo móvel deixaram de ser implementadas pela aplicação e passaram a ocorrer ao nível do sistema operativo (Android e iOS).

Com a exceção das funcionalidades disponibilizadas pelos sistemas operativos dos dispositivos móveis, IOS e Android, onde se inclui o sistema GAEN, todo o software do sistema é aberto e estará publicamente acessível antes do lançamento público do sistema.

2.1. Componentes do sistema

O sistema STAYAWAY COVID é composto por 3 tipos de componentes de software independentes:

- DMP - Dispositivos Móveis Pessoais com sistema operativo iOS ou Android, interface Bluetooth Low Energy (BLE) e interface (dados móveis ou WiFi) para acesso à Internet. Executam a aplicação móvel STAYAWAY COVID, partilham o modelo de dados e intervêm no mesmo fluxo de dados.
- SLD - Serviço de Legitimação de Diagnóstico, sob controlo oficial, produz Código de Legitimação (CL) e Código de Acesso (CA). Modelo de dados próprio.
- SPD - Serviço de Publicação de Diagnóstico, sob controlo oficial, recebe e publicita diagnóstico positivo confirmado após autenticação por CA. Modelo de dados próprio.

Estes componentes, juntamente com o Profissional de Saúde (PS) com credenciais para se autenticar e interagir junto do SLD, constituem os atores do sistema.

2.2. Modelo de dados

2.2.1. Dados transmitidos

Chave de Identificadores TEK (Temporary Exposure Key): número pseudoaleatório.

Exemplo: “oZXRCXGZmWUDC1cPsxSxTPogQ\/ltJHdkoZ3Grw8gWVY=”.

Identificador Aleatório RPI (Rolling Proximity Identifier): número pseudoaleatório gerado com base numa Chave de Identificadores TEK.

Exemplo: “1wSc1eXgMhm8wml6GqgB+Q==”.

Código de Legitimação (CL): número pseudoaleatório.

Exemplo: “288 357 974 611”.

Código de Acesso (CA): JSON Web Token (RFC 7519) com a seguinte estrutura, exemplificada:

“jti”:	"d18ec885-3ee0-4006-bdcb-98e181bd170d"
“iss”:	"STAYAWAYCOVID Autoridade (TESTE)"

“iat”:	1589288835
“sub”:	"00f3bd45-d780-40db-9266-f8430c22ee0a"
“typ”:	“Bearer"
“scope”:	"exposed"
“fake”:	“0”
“onset”:	"2020-05-09"
“azp”:	"pta-app-backend"
“auth_time”:	0
“acr”:	“1”
“nbf”:	0
“uuid”:	"6b7e23ff-eb33-40f3-8589-c29b4eb2e55e"
“exp”:	1589289135

2.2.2. Estruturas de dados locais

DS-DMP: Estruturas de dados do DMP definidas e geridas pela GAEN API.

Status

status	String

Exposure Configuration

minimumRiskScore	Int
attenuationScores	Array
daysSinceLastExposureScores	Array
durationScores	Array
transmissionRiskScores	Array
durationAtAttenuationThresholds	Two-value Array

TemporaryExposureKey

keyData	Usada para gerar os dados de disseminação
rollingStartNumber	Data de geração da chave
rollingPeriod	Data de expiração da chave
transmissionRiskLevel	Nível de risco de exposição cruzada para o tempo de interação entre dispositivos

ExposureSummary

daysSinceLastExposure	Int
matchedKeyCount	Int
maximumRiskScore	Nível de risco máximo de todas as exposições
attenuationDurations	Array
summationRiskScore	Soma de todos os riscos de todas as exposições

ExposureInformation

dateMillisSinceEpoch	Data
durationMinutes	Int
attenuationValue	Int
transmissionRiskLevel	Int

DS-SLD: estrutura de dados do SLD.

authorization_code	
id	uuid
code	character varying (12)
creation_date_time	timestamp without time zone
expiry_date	timestamp without time zone (data igual ao campo *creation_date_time* mais 24 horas)
original_onset_date	date
call_count	integer
onset_date	date

DS-SPD: estruturas de dados do SPD.

t_exposed	
pk_exposed_id	integer
key	text
received_at	timestamp with time zone
key_date	timestamp with time zone
app_source	character varying (50)

t_redeem_uuid	
pk_redeem_uuid_id	integer
uuid	character varying (50)
received_at	timestamp with time zone

2.3. Cenários de interação

O sistema compreende 3 cenários de interação entre os diversos atores, descritos em seguida.

2.3.1. Difusão

Atores: DMP.
Interação: Neste cenário, o DMP difunde por BLE Identificadores Aleatórios RPI. Estas mensagens são recebidas por DMP geograficamente próximos.
Informação manipulada: O DMP gera diariamente, sem relação com qualquer informação pessoal ou outra, de forma pseudoaleatória, uma Chave de Identificadores TEK única. Neste cenário, o DMP difunde periodicamente Identificadores Aleatórios RPI gerados pseudoaleatoriamente com base na Chave de Identificadores TEK previamente gerada. Os Identificadores Aleatórios RPI recebidos são armazenados localmente no DMP (DS-DMP) por um

período limitado pré-definido. O DMP não manipula quaisquer dados que identifiquem direta ou indiretamente pessoas singulares, para além dos referidos Chaves de Identificadores TEK e Identificadores Aleatórios RPI.

2.3.2. Diagnóstico (A)

Atores: PS e SLD.
Interação: Neste cenário, o PS acede ao SLD e obtém um CL.
Informação manipulada: O PS autentica-se junto do SLD. O SLD gera i) um CL pseudoaleatório sem relação com qualquer informação pessoal ou outra, e ii) um CA pseudoaleatório com relação ao instante corrente. O SLD armazena localmente o par CL e CA (DS-SLD). PS recebe um CL.

2.3.3. Diagnóstico (B)

Atores: PS, DMP, SLD e SPD.
Interação: Neste cenário, o DMP obtém um CL do PS por canal externo ao sistema. O DMP acede ao SLD sem se autenticar, fornecendo um CL e obtém um CA como resposta. O DMP autentica-se junto do SPD com o CA obtido e submete as Chaves de Identificadores TEK diárias dos últimos 14 dias.
Informação manipulada: O CL é válido para uma única interação e num intervalo temporal pré-definido (24 horas). O CA é válido para uma única interação e num intervalo temporal pré-definido. O SPD armazena localmente Chaves de Identificadores TEK em SD-SPD e regista os CA que foram usados para evitar a sua reutilização.

2.3.4. Alerta

Atores: DMP e SPD.
Interação: Neste cenário, o DMP obtém por acesso não autenticado Chaves de Identificadores TEK disponíveis em SPD.
Informação manipulada: Chaves de Identificadores TEK de acesso público em SPD. Cada DMP descarrega as Chaves de Identificadores TEK disponíveis em SPD de forma incremental. A aplicação guarda a data da última atualização e pede apenas as chaves publicadas após essa data, para cada um dos dias relevantes (v.g. últimos 10).

2.4. A instalação e configuração da aplicação

Cada utilizador, após descarregar a aplicação STAYAWAY COVID das lojas oficiais, Apple Store e Google Play, procede à sua instalação e configuração, recebendo uma breve descrição do seu funcionamento e algumas características dos tratamentos de dados pessoais efetuados, designadamente através de infografias, e de apontadores para a "Política de Privacidade" e para os "Termos de Utilização" do serviço.

Nesta fase preliminar, o utilizador dá o consentimento e concede autorização para o acesso à interface Bluetooth, que inclui BLE. A instalação da aplicação STAYAWAY COVID não requer qualquer tipo de identificação do utilizador, criação de conta ou registo. Uma vez em funcionamento, a sua configuração restringe-se à ativação ou inibição do envio e receção de mensagens BLE.

A utilidade da aplicação STAYAWAY COVID exige a interface Bluetooth ativa para poder difundir os Identificadores Aleatórios RPI quando os DMPs estão próximos, aproximadamente 2 metros em linha de vista. Este requisito é explicito e frontalmente apresentado ao utilizador e solicitado, também explicita e previamente, o seu consentimento para a utilização da interface Bluetooth. Posteriormente, e em qualquer momento, é dada ao utilizador, de forma simples, a opção de suspender a utilização da interface Bluetooth por parte da aplicação e com isso cessar a emissão de quaisquer dados.

2.5. Interface da aplicação

A aplicação apresenta essencialmente 3 estados diferentes: sem risco, alerta de potencial contacto de risco, diagnosticado com COVID-19. Estes estados são apresentados graficamente e associados a recomendações a ter por parte dos utilizadores. Abaixo são apresentados os ecrãs dos diferentes estados e também do ecrã que permite desligar o rastreio.

2.5.1. Sem risco

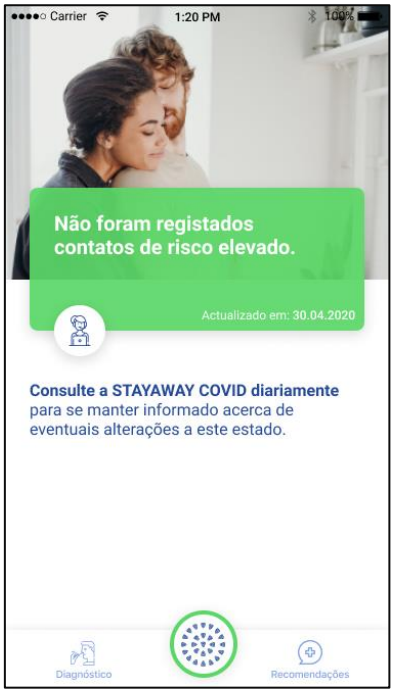


Figura 1 - Ecrã quando não foram registados contactos de risco elevado

Figura 2 - Ecrã com recomendações

2.5.2. Detetado contacto de risco

Figura 3 - Ecrã com alerta de contacto com pessoa diagnosticada com COVID-19

Figura 4 - Ecrã com recomendações em caso de contacto com infetado

2.5.3. Submissão de Chaves de Identificadores TEK após diagnóstico positivo

Figura 5 - Ecrã para introdução de chave facultada pelo médico após diagnostico com COVID-19

2.5.4. Diagnosticado com COVID-19 e com as Chaves de Identificadores TEK comunicadas

Figura 6 - Ecrã apresentado após introdução da chave

2.5.5. Controlo de rastreio - ligar/desligar

Figura 7 - Opção ativar e desativar rastreio

2.5.6. Permissões/Autorizações

Figura 8 - Permissão para acesso ao Bluetooth

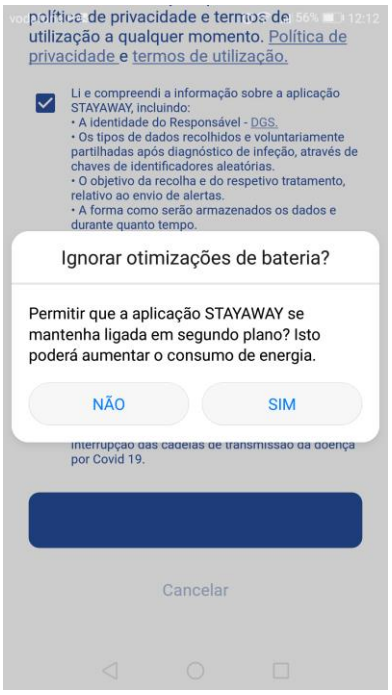


Figura 9 - Permissão para executar aplicação em segundo plano

2.5.7. Consentimento

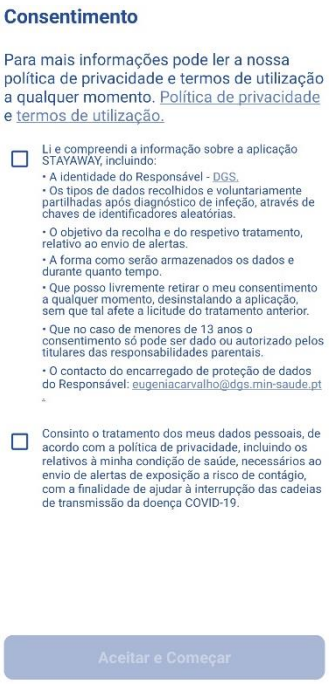


Figura 10 - Consentimento na aplicação

2.5.8. Menu opções

Figura 11 - Menu de opções da aplicação

2.6. Interação entre os dispositivos móveis dos utilizadores

Uma vez concluídas a instalação e a configuração, a aplicação entra em funcionamento. Na primeira execução, o DMP gera uma Chave de Identificadores TEK inicial, pseudoaleatória, com base na qual serão gerados os números pseudoaleatórios usados nas interações de difusão subsequentes. Para a geração da Chave de Identificadores TEK inicial são utilizados os geradores de números pseudoaleatórios nativos das plataformas Android (Java) e iOS (Swift).

Diariamente, é gerada uma Chave de Identificadores TEK nova. A partir da Chave de Identificadores TEK diária é gerado, em média a cada 15 minutos, um Identificador Aleatório RPI a partir da Chave de Identificadores TEK corrente. Estes Identificadores Aleatórios RPI são transmitidos em modo de difusão e recebidos por DMP geograficamente próximos. Os Identificadores Aleatórios RPI são armazenados pelos DMP juntamente com outros dados acessórios (e.g. data, duração e distância estimada do contacto). Desta forma, cada DMP armazena a lista das suas Chaves de Identificadores TEK diárias e a lista dos Identificadores Aleatórios RPI recebidos dos DMP com quem esteve em contacto próximo. As Chaves de Identificadores TEK e os Identificadores Aleatórios RPI são automaticamente apagados do DMP 14 dias após terem sido armazenados.

Os RPIs são gerados com base nas respetivas Chaves de Identificadores TEK e no intervalo temporal durante os quais são válidos. Os RPIs e os referidos intervalos são difundidos pelos DMPs. De acordo com a especificação GAEN, a utilização e divulgação dos intervalos temporais, juntamente com os RPIs, tem como objetivo mitigar ataques de repetição: evita que um atacante possa gravar e enviar mais tarde RPIs de utilizadores diagnosticados com COVID-19 com o objetivo de criar falsos positivos (falsos alertas). Os intervalos temporais recebidos são

também usados para calcular o período de armazenamento dos RPI, que são apagados ao fim de 14 dias.

No caso de ser detetada uma exposição, a GAEN disponibiliza a data do contacto mais recente. Essa informação é apresentada pela STAYAWAY COVID ao utilizador que, voluntariamente, poderá transmitir às entidades de saúde.

2.7. Submissão das Chaves de Identificadores TEK do dispositivo do utilizador diagnosticado com COVID-19

Na eventualidade de o utilizador da aplicação STAYAWAY COVID ser diagnosticado com COVID-19, pretende-se que, de forma simples, segura e anónima, submeta as Chaves de Identificadores TEK armazenadas no seu DMP ao SPD.

Garantir que apenas utilizadores diagnosticados com COVID-19 por uma entidade oficialmente autorizada (PS) submetem Chaves de Identificadores TEK é crucial para a correção do sistema. À data, consideramos que um PS é qualquer Médico registado na Ordem dos Médicos. Consideramos ainda que o diagnóstico fornecido pelo PS é exato e definitivo.

De forma a garantir que apenas utilizadores a quem é diagnosticada COVID-19 por um PS estão habilitados a submeter as suas Chaves de Identificadores TEK, foram consideradas várias abordagens.[6] Estas, para além de norteadas pela segurança e privacidade, consideram sobremaneira o equilíbrio com a voluntariedade da ação e a exequibilidade do processo tendo em conta o espetro de literacia digital dos utilizadores. Neste sentido, optou-se por uma abordagem que i) coloca no utilizador a decisão unilateral e privada da submissão das suas Chaves de Identificadores TEK ao SPD e ii) simplifica particularmente a interação do utilizador com o sistema.

O método implementado consiste em fornecer ao utilizador a quem foi diagnosticado COVID-19 um código numérico (CL) que este deverá inserir na aplicação STAYAWAY COVID se desejar submeter as suas Chaves de Identificadores TEK ao sistema. O CL, sendo numérico, permite que o utilizador o receba de variadas formas conforme atualmente é realizada a transmissão do resultado dos testes à COVID-19: oralmente por telefone ou por escrito utilizando um qualquer meio de comunicação eletrónico. Na posse do CL, em privado se o desejar, cabe ao utilizador utilizá-lo ou não. O risco que esta abordagem introduz, e para o qual o sistema STAYAWAY COVID não prevê mitigação, é o da utilização do CL, consentida ou não pelo utilizador legítimo, por outro utilizador saudável.

Em detalhe, a um utilizador diagnosticado com COVID-19 ser-lhe-á fornecido, por canal externo ao sistema STAYAWAY COVID, um CL, número pseudoaleatório de 12 algarismos, pelo PS. Ao ser introduzido no DMP, este código permitirá à aplicação STAYAWAY COVID submeter ao SPD as Chaves de Identificadores TEK do utilizador. Tendo obtido um CL, o DMP submete-o ao SLD, por canal de comunicação seguro. Em resposta, o DMP recebe um Código de Acesso (CA) que tem a forma de um *JSON Web Token* (RFC 7519). Este CA permite ao DMP autenticar-se perante o SPD e submeter as Chaves de Identificadores TEK. O Código de Acesso é registado pelo SPD, para não poder ser reutilizado.

[6] Cfr. Secure Upload Authorisation for Digital Proximity Tracing https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Upload%20Authorisation%20Analysis%20and%20Guidelines.pdf.

O acesso ao SLD por parte do DMP para obtenção do CA não requer autenticação de modo a salvaguardar o anonimato do utilizador. O CL pode, porém, apenas ser utilizado durante um curto período após ser gerado e apenas uma vez: os códigos CL são válidos por 24 horas.

De modo a prevenir ataques de força bruta, em que um atacante tenta obter um CA mediante a apresentação de CLs criados aleatoriamente por um software dedicado num ou mais computadores, em que tenta acertar num CL válido (durante um dado período), é instalado um serviço de anti-DDoS na infraestrutura de perímetro (entre a Internet e o SLD), que limita a quantidade de pedidos que podem ser realizados ao SLD por cada cliente durante um curto período. Desta forma, salvaguardam-se os casos em que o utilizador insere o CL errado, por falha na inserção dos algarismos, dos casos de tentativa de força bruta, em que são feitas dezenas a milhares de tentativas por minuto.

A limitação do número máximo de pedidos que podem ser feitos num curto período de tempo, associado à extremamente baixa probabilidade de acertar num CL (na ordem dos 10^{-12}), e à limitação de um CA por CL válido, mitiga os ataques por força bruta.

O acesso do DMP ao SPD utiliza canais de comunicação seguros e um processo de autenticação standard com certificados *JSON Web Token* (RFC 7519).

2.8. SPD, SLD e sistema de autenticação de utilizadores médicos

A Imprensa Nacional-Casa da Moeda (INCM) irá alojar o servidor SPD e o INESC TEC será responsável pela sua operação, enquanto que a SPMS terá a seu cargo o alojamento e operação do servidor SLD. A SPMS será também responsável pelo desenvolvimento dos mecanismos técnicos necessários ao acesso ao SLD, limitando o referido acesso aos médicos que se autentiquem num sistema de autenticação/autorização gerido pela SPMS, independente do SLD.

O sistema utilizado como contexto para acesso ao SLD será o Trace COVID-19 (TC-19), atestando-se a categoria profissional com recurso ao Portal de Requisição de Vinhetas e Receitas (PRVR), de forma a que o acesso seja circunscrito a médicos.

A integração será efetuada garantindo o princípio de segregação entre o SLD e o Trace COVID-19, de forma a que não se verifiquem trocas de informação desnecessária entre os sistemas, protegendo a privacidade dos dados sem comprometer a imprescindível vertente de usabilidade.

A título processual, o circuito previsto ao nível da intervenção dos médicos contempla os seguintes passos:

- Os médicos responsáveis pela legitimação acedem ao Trace COVID-19;
- Mediante verificação de caso confirmado, o médico (validado pelo PRVR) seleciona a opção disponível para geração de CL.
- O médico insere a data dos primeiros sintomas ou data do teste (em caso de utente assintomático).
- O Trace COVID-19 autentica-se no SLD recorrendo a um token e pede um Código de Legitimação (CL), indicando a data identificada no ponto anterior.
- O SLD valida o token, gera o CL e respetivo Código de Acesso (CA) e envia o CL ao TC-19.
- O CL (código com 12 algarismos) é apresentado ao médico numa caixa específica da interface gráfica do TC-19.

- O médico transmite o CL ao utilizador da aplicação STAYAWAY COVID, através de um canal externo, para que este o possa inserir no seu DMP.
- O utilizador insere o CL no DMP, o qual usa o CL para se autenticar no SLD e obter o respetivo CA.
- O dispositivo móvel (DMP) do utilizador autentica-se no SPD através do CA e envia as Chaves de Identificadores TEK geradas desde a data designada "*onset*", a qual é a data introduzida pelo médico subtraída de dois dias (de acordo com a Norma de rastreio da DGS). A data *onset* fica guardada no SLD antes mesmo de o utilizador receber o CL.
- O DMP recebe esta data como parte do CA e envia para o SPD as chaves TEK relevantes, isto é, entre *"onset date"* e a data atual, inclusivamente. Estas são as chaves TEK publicadas pelo SPD para o utilizador em causa.

2.9. Cruzamento dos códigos aleatórios no dispositivo do utilizador

Diariamente, a aplicação acede até duas vezes, em instantes aleatoriamente determinados, ao SPD e obtém todas as Chaves de Identificadores TEK disponíveis, ou seja, relativas a utilizadores a quem nos últimos 14 dias foi diagnosticada COVID-19. Para cada Chave de Identificadores TEK obtida, a aplicação, ao nível da API GAEN, gera 144 Identificadores Aleatórios RPI e verifica se coincidem com algum Identificador Aleatório RPI armazenado localmente, no DMP[7].

Havendo coincidência, a aplicação, ao nível da API GAEN, calcula uma função de risco que, seguindo as diretrizes atuais da Organização Mundial de Saúde, avalia a existência de contactos a menos de 2 metros e por mais de 15 minutos.

2.10. Interoperabilidade da aplicação

O sistema STAYAWAY COVID deverá ser interoperável com sistemas similares desenvolvidos noutros Estados-Membros da União Europeia com o mesmo propósito. Futuras versões da presente AIPD não deixarão de explicitar detalhadamente por que forma este aspeto será acautelado em termos europeus.

[7] Mais detalhes técnicos podem ser consultados no apêndice E.

3. Descrição do tratamento de dados

3.1. Âmbito e contexto

O contexto geral do desenvolvimento do sistema STAYAWAY COVID e dos tratamentos de dados implicados no seu funcionamento é o da emergência de saúde pública decorrente da pandemia da COVID-19. Conforme acima referido, este sistema destina-se a ser usado como um meio complementar ao serviço de uma estratégia global de resposta à pandemia, especialmente pertinente como meio auxiliar no contexto da fase de desconfinamento que vivemos.

O sistema tem por principal funcionalidade o envio de alertas a utilizadores que tenham estado em contacto de proximidade com outros utilizadores da aplicação a quem foi diagnosticada COVID-19. O seu contexto é também o de uma utilização estritamente voluntária, em linha com as orientações que foram sendo emanadas da Comissão Europeia e do Comité Europeu para a Proteção de Dados sobre este tipo de recurso. Em rigor, mais do que uma solução de rastreio, do ponto de vista técnico, tratar-se-á de uma aplicação de notificação da exposição individual a fatores de risco de contágio. Nessa medida servirá de complemento aos esforços tradicionalmente levados a cabo pelas autoridades de saúde no intuito de rastrear e interromper cadeias de transmissão da doença. Relativamente ao âmbito, importa, igualmente, e novamente, sublinhar, que as notificações de exposição apenas poderão ter lugar após validação por profissional de saúde e com base na iniciativa do próprio utilizador que tenha sido diagnosticado com COVID-19.

3.2. Finalidade do tratamento

A aplicação pretende dar um contributo significativo para a rápida interrupção das cadeias de infeção no decurso da epidemia provocada por COVID-19, procurando detetar, apoiada pela automatização, os chamados contactos intensivos. Em causa estão os contactos entre pessoas singulares que duram mais de 15 minutos e em que a distância física entre os utilizadores da aplicação é inferior a 2 metros.

Embora a Organização Mundial de Saúde (OMS) recomende o denominado "distanciamento social", ou seja, a distância entre pessoas a fim de evitar uma potencial transmissão do vírus,[8] nem sempre é possível evitar atualmente contactos intensivos, que envolvam um risco significativamente mais elevado de infeção. Devido à abertura gradual das atividades económicas, como comércio, empresas de retalhos, fábricas, por exemplo, desde meados de maio de 2020, e à flexibilização das medidas de combate à propagação da COVID-19, nos termos dos Decreto-Lei n.º 22/2020, de 16 de maio, prevê-se que a população portuguesa se torne cada vez mais móvel, o que poderá conduzir a um aumento dos cenários de infeção possíveis.

O registo voluntário destes contactos destina-se a facilitar a determinação de contactos dos últimos dias e a servir de lembrete às pessoas em potencial risco. A aplicação oferece a possibilidade de informar diretamente as pessoas sobre uma situação de risco devido a um contacto intensivo recente. Deste modo, procurar-se-á auxiliar na gestão de esforço do sistema nacional de saúde. Ademais, através do subsequente auto-isolamento voluntário, as cadeias de

[8] Cfr. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public.

infeção poderão ser interrompidas antes, fornecendo um apoio essencial para a manutenção da saúde pública através da contenção da epidemia provocada pela COVID-19.

A finalidade da aplicação prende-se, por isso, com a conservação dos contactos dos utilizadores que poderão ter sido expostos à COVID-19 de modo a alertá-los da suscetibilidade de risco, sem com isso revelar a identidade do contacto ou do local onde o contacto poderá ter ocorrido.

O objetivo da aplicação prende-se com uma atuação preventiva, procurando, através do alerta de contactos intensivos, minimizar os riscos de infeção por potenciais agentes de contágio. Deste modo, procurando contribuir para o retardamento da propagação da COVID-19, com base nos conhecimentos científicos atuais dos epidemiologistas.

3.3. Legitimidade da finalidade

A aplicação revela-se particularmente relevante a partir do momento em que são levantadas as medidas de contenção, dado o aumento do risco de infeção, à medida que cada vez mais pessoas entram em contacto umas com as outras. Neste sentido, como vêm referindo as autoridades europeias, designadamente nas orientações emitidas pela Comissão Europeia no contexto da pandemia, aplicações deste tipo poderão auxiliar na interrupção de cadeias de infeção, de forma mais rápida e eficaz do que as medidas gerais de contenção. A aplicação poderá contribuir para a redução significativa do risco de propagação do vírus. Por este motivo, dado o seu caráter complementar em relação a tantas outras medidas, como a higienização das mãos ou o aumento da capacidade de realização de testes de diagnóstico, constitui um importante elemento da estratégia de saída[9].

Realce-se, novamente, que a aplicação STAYAWAY COVID não deverá ser vista, nem deverá funcionar, como uma medida autónoma, mas antes enquanto medida complementar de outras tantas medidas como a mobilização do pessoal de saúde e dos investigadores sanitários, a disponibilidade de máscaras e testes ou a sensibilização para higienização, todas elas cruciais para colher os benefícios positivos da utilização da aplicação. Esta mobilização de recursos faz, portanto, parte de um plano global, que a aplicação integrará.

O objetivo da aplicação de *contact tracing* é, concretamente, o de poder informar um utilizador da aplicação de que o seu *smartphone* (ou outro dispositivo móvel) esteve muito próximo, nos dias anteriores, de o de uma pessoa que posteriormente foi diagnosticada com COVID-19, existindo o risco de, por sua vez, ter sido contaminada.

Neste sentido, a aplicação não se destina a controlar o cumprimento das medidas de confinamento ou outras obrigações sanitárias, nem tão-pouco a identificar as zonas para onde essas pessoas se deslocaram.

Tão-pouco deverão ser extraídos quaisquer efeitos jurídicos (ou outros de importância equivalente na esfera dos utilizadores) a partir dos resultados atingidos através da utilização da aplicação. Esta conclusão deve ser vista como um corolário natural do cariz voluntário e não discriminatório, erigido em requisito essencial da aplicação e respetiva disponibilização pública.

Com efeito, o caráter voluntário não se deve manifestar apenas no momento em que o utilizador descarrega a aplicação, ou seja, na sua instalação, na verificação da habilitação do Bluetooth ou ainda na capacidade de a desinstalar. O caráter voluntário também será assegurado por garantir

[9] COMUNICAÇÃO DA COMISSÃO, Orientações respeitantes a aplicações móveis de apoio à luta contra a pandemia de COVID-19 na perspetiva da proteção de dados (2020/C 124 I/01).

ao utilizador a inexistência de consequências negativas associadas ao não descarregamento da aplicação ou à não utilização da aplicação, não sendo o acesso a testes e a cuidados de saúde, de forma alguma, condicionado à respetiva instalação. A utilização da aplicação não pode condicionar, nem a possibilidade de circular quando o bloqueio é levantado, nem o acesso a determinados serviços, como os transportes públicos, por exemplo, sendo todos estes aspetos determinantes da legitimidade reconhecida à finalidade da aplicação.

3.4. Categorias de dados alvo de tratamento

Os códigos aleatórios são gerados pela aplicação sem qualquer relação com o dispositivo ou o seu utilizador. A aplicação recebe e partilha estes códigos com outros utilizadores que estiveram em contacto próximo. Só em caso de aceitação prévia e legitimação do médico é possível recolher os códigos recebidos pelo seu dispositivo para um servidor do sistema. Os códigos gerados são únicos e, em última instância, servem a autoidentificação de um contacto próximo estabelecendo, portanto, uma relação entre cidadãos. Por esta razão, formalmente consideramos estes dados como pseudonimizados, mesmo que o sistema não consiga nunca revelar a identidade dos utilizadores.

Na medida em que reportem a utilizadores diagnosticados com COVID-19 ou a utilizadores alertados de potencial risco de contágio, consideramos que aqueles identificadores se referem a dados de saúde ou a dados relativos à sua saúde.

Além dos identificadores referidos, conforme melhor se detalhará na tabela abaixo, são recolhidos e armazenados alguns dados e meta-dados relevantes para a finalidade prosseguida, em particular no servidor SLD (ver estrutura de dados DS-SLD, na secção 2.2.2), no contexto da voluntária submissão de Chaves de Identificadores TEK por um utilizador infetado, especificamente: a data dos primeiros sintomas ou a data de teste para indivíduos assintomáticos; a data em que estes dados deverão ser destruídos no SLD; o número de vezes que o CL foi utilizado (0 ou 1, já que é de utilização única).

A obtenção da data dos primeiros sintomas ou de teste para assintomáticos destina-se a limitar os contactos que poderão receber avisos de exposição aos que ocorreram após a data de 2 dias antes da referida data, que corresponde ao consenso atual (de acordo com a Norma de Rastreio de Contactos da DGS) sobre o período pré-sintomático em que há a possibilidade de contágio. Quando se trata de um caso assintomático, é da responsabilidade do médico usar a data do teste ou determinar a data mais adequada. A data é inserida pelo profissional de saúde no SLD para emissão do CL. Após ter sido inserida, esta data só pode ser obtida com o conhecimento do CL, que é apenas do conhecimento do doente e do profissional de saúde.

Por exemplo, imagine-se que um cidadão tem os primeiros sintomas no dia 19, faz o teste no dia 20 e recebe os resultados no dia 21. A aplicação tem a possibilidade de enviar Chaves de Identificadores TEK para o SPD desde o dia 7, ou seja, 14 dias antes. No entanto, o profissional de saúde irá emitir um CL com a data de 19, pelo que a aplicação estará autorizada apenas a publicar chaves desde o dia 17. Desta forma não são publicadas chaves de dias cuja infeção não é confirmada pelo profissional, correspondentes aos contactos entre os dias 7 e 17, minimizando-se significativamente a partilha de pseudónimos e bem assim de potenciais falsos positivos (falsos alertas) em obediência ao princípio da privacidade por omissão.

Os registos de dados para o CL e do CA, guardados no SLD, tem uma validade de 24 horas. Após terem expirado a validade, são apagados pela tarefa diária de manutenção.

Dados	Definição	Finalidade	Conservação
Dados pseudonimizados (Chaves de Identificadores TEK e Identificadores Aleatórios RPI)	O dispositivo móvel gera diariamente uma Chave de Identificadores TEK. A partir da Chave de Identificadores TEK diária é gerado, a cada 15 minutos, em média, um Identificador Aleatório RPI a partir da Chave de Identificadores TEK corrente e do intervalo temporal durante o qual o RPI é válido. Os Identificadores Aleatórios RPI são transmitidos em modo de difusão e recebidos pelos dispositivos móveis geograficamente próximos.	Permite sinalizar a proximidade do utilizador com alguém durante pelo menos 15 minutos a 2 metros de distância, sem que a aplicação possa identificar o utilizador ou rastrear o local onde o contacto teve lugar.	Apagados automaticamente do dispositivo móvel 14 dias após terem sido armazenados.
Dados pseudonimizados (Identificador único universal)	Identificador produzido no Serviço de Legitimação de Diagnóstico (SLD) como parte do Código de Acesso (CA).	É armazenado no Serviço de Publicação de Diagnóstico (SPD) quando o CA é criado e usado depois para garantir que cada CA não é usado mais do que uma vez dentro do seu período de validade.	É eliminado pela tarefa diária de manutenção da base de dados após o fim da sua validade, que é no máximo de 24 horas.
Dados de saúde (Chaves de Identificadores TEK partilhadas após diagnóstico de infeção)	São as chaves submetidas pelos utilizadores diagnosticados por COVID-19 ao servidor central do sistema. Estas chaves são descarregadas periodicamente pelos dispositivos com a STAYAWAY. A aplicação guarda a data da última atualização e pede apenas as chaves publicadas após essa data, para cada um dos dias relevantes.	O DMP calcula os Identificadores Aleatórios RPI associados a estas chaves para os comparar com os RPIs recebidos de DMPs próximos durante os últimos 14 dias. Depois, calcula uma função de risco que avalia a existência de contactos a menos de 2 metros e por mais de 15 minutos mediante os RPIs, distâncias estimadas e tempos de exposição.	O período de conservação é 14 dias.

Dados de saúde (data, duração e distância estimada do contacto)	A partir dos Identificadores Aleatórios RPIs recebidos dos DMPS próximos e das Chaves de Identificação TEK, dos utilizadores infetados, recebidas do SPD, bem como dos metadados temporais associados, o DMP calcula uma função de risco que, seguindo as diretrizes atuais da Organização Mundial de Saúde, avalia a existência de contactos a menos de 2 metros e por mais de 15 minutos.	A aplicação alerta de que o utilizador esteve em contacto com alguém a quem foi diagnosticada COVID-19, durante pelo menos 15 minutos a 2 metros de distância.	O período de conservação é 14 dias.
Dados de saúde (Data dos primeiros sintomas ou data do teste no caso de indivíduos assintomáticos)	Informação inserida pelo profissional de saúde no sistema no momento de geração do Código de Legitimação. Esta data só pode ser obtida com o conhecimento do CL, que é do conhecimento apenas do doente e do profissional de saúde.	Esta data destina-se a limitar os contactos que desencadeiam avisos aos que ocorreram após a data de 2 dias antes da data dos primeiros sintomas, que corresponde ao consenso atual sobre o período pré-sintomático em que há a possibilidade de contágio. Quando se trata de um caso assintomático, é da responsabilidade do médico usar a data do teste ou determinar a data mais adequada. É relevante conservar a data de início de sintomas e de diagnóstico para que seja possível à aplicação alertar apenas aquelas pessoas que contactaram com alguém diagnosticado com infeção por SARS-CoV-2 nos 2 dias antes do início de sintomas, ou de diagnóstico, quando estes estão assintomáticos. Pretende-se desta forma reduzir o número de falsos positivos, minimizando a procura aos cuidados de saúde, sem comprometer a eficácia do sistema, os custos inerentes com esta procura e	Logo que o CL tenha esgotado a sua validade, que é de 24 horas, é apagado da base de dados pela tarefa diária de manutenção.

		com a realização de testes, o número de pessoas em isolamento sem indicação, e, por fim, o stress psicológico inerente à (falsa) suspeita de contacto de alto risco com um doente COVID-19. A data é enviada para o SLD, aquando da geração do CL pelo médico, e guardada no registo associado ao CL no SLD e no respetivo CA, depois usado pelo SPD para determinar as Chaves de Identificadores TEK que devem ser difundidas pelos DMPs. O critério das 48 horas está em consonância com a Norma de Rastreio de Contactos da DGS.	
Endereço IP	O SLD armazena os endereços IP para fins de segurança. No caso do SPD não está previsto o armazenamento de endereços IP ou outro identificador diretamente associado ao dispositivo móvel.	O endereço IP é armazenado durante um curto período pela infraestrutura de perímetro com o único objetivo de garantir a segurança informática, nomeadamente contra ataques DDoS. Os equipamentos da infraestrutura de perímetro são independentes do SLD e não há cruzamento de dados.	O período de conservação dos endereços IP nos equipamentos de perímetro é não superior a 1 hora.

Para além dos dados dos utilizadores da STAYAWAY COVID, conforme já se referiu, são intervenientes no sistema os profissionais de saúde envolvidos na validação da informação do contágio e na consequente geração do CL. Por conseguinte, e conforme especificado no ponto 2.8, será usado um sistema de autenticação e autorização a cargo da SPMS, que funcionará de forma separada de outros sistemas, garantindo a privacidade de ambas as categorias de titulares (utilizadores e profissionais de saúde). Neste contexto, a única informação guardada no Trace COVID-19 corresponde a logs aplicacionais, que identificam eventos de autenticação no SLD.

3.5. Designação de um responsável pelo tratamento

Como vem referindo o Comité Europeu para a Proteção de dados, a responsabilidade do tratamento de dados deve ser claramente definida, sobretudo num contexto em que a monitorização sistemática e em grande escala de dados pessoais, como os relativos aos contactos entre pessoas singulares ainda que codificados, constitui forçosamente uma invasão

da sua privacidade que só pode ser legitimada se tiver por base a adoção voluntária por parte dos utilizadores para cada uma das respetivas finalidades.

Por este motivo, autoridades de controlo de vários Estados-Membros, assim como o próprio Comité Europeu para a Proteção de Dados, têm entendido que entidades como o Ministério de Saúde dos Estados-Membros ou as respetivas autoridades de saúde, deviam ser designados como os responsáveis pelo Tratamento, sem prejuízo da previsão de outros responsáveis de tratamento.[10]

Este mesmo entendimento foi acompanhado pela Comissão Nacional de Proteção de Dados, na Deliberação 2020/277, de 20 de junho, tendo sido objeto de normação legal, através do Decreto-Lei 52/2020 de 11 de agosto, que estabelece a Direção-Geral da Saúde (DGS) como o Responsável de Tratamento de Dados, bem como pela operacionalização do sistema.

Avaliação EPD

Sublinhe-se a necessidade de garantir, na sua máxima extensão, e ao longo de todo o ciclo da utilização da tecnologia, o respeito pelo princípio do uso voluntário e o seu cariz não discriminatório, enquanto requisitos da própria legitimidade da finalidade declarada. Tais princípios do uso voluntário e da igualdade deverão, em obediência a um terceiro princípio, o da transparência, ser comunicados e suficientemente explicitados ao universo de utilizadores, seja por via das políticas de privacidade para o efeito construídas, seja através das campanhas de informação que desejavelmente acompanharão a fase da sua disponibilização pública.

No tocante à referida designação do responsável, ou dos responsáveis, pelo tratamento de dados, esta deverá ser feita, em todo o caso, antes que sejam iniciadas as operações de tratamento. Concordamos com a abordagem citada que privilegia a escolha de determinadas entidades públicas ou com competências delegadas, especialmente, na área da saúde pública, sem prejuízo das várias alternativas existentes a considerar nesta sede. Com efeito, o propósito determinante do desenvolvimento da solução é, atente-se, o de colocar à disposição do Estado uma solução que seja incluída pelas autoridades competentes num plano de resposta global à pandemia, numa perspetiva de saúde pública. Num cenário em que não se verificasse aquele pressuposto, a disponibilização da solução tecnológica em apreço deveria ser reequacionada e reponderada à luz dos princípios da limitação das finalidades, licitude e proporcionalidade, sendo certo, porém, que, mantendo-se a finalidade declarada, a sua utilização apenas se justificaria no exercício de funções de interesse público (concretamente, de proteção da saúde pública), portanto, sob a responsabilidade de uma entidade que tenha a seu cargo aquele tipo de funções.

Aceitável	☐	Aceitável com recomendações	☒	Inaceitável	☐

[10] Comunicação da Comissão Europeia — Orientações respeitantes a aplicações móveis de apoio à luta contra a pandemia de COVID-19 na perspetiva da proteção de dados, C(2020) 2523 final, 16.4.2020, Bruxelas; Diretrizes 4/2020 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19 do Comité Europeu para a Proteção de Dados; CNIL, Deliberation N°. 2020-046 of April 24, 2020 delivering an opinion on a proposed mobile application called "StopCovid", página 8.

4. Ciclo de vida dos dados

Desde a recolha até o apagamento

Os dados pessoais recolhidos pela aplicação nunca permitem identificar diretamente utilizadores ou os seus dispositivos. Para proteger a privacidade dos utilizadores apenas são usados identificadores alfanuméricos efémeros e gerados aleatoriamente, os quais, conforme acima referido, legalmente consideramos dados pseudonimizados.

A aplicação difunde e recebe estes identificadores aleatórios de outros dispositivos que estejam próximos. Os identificadores aleatórios difundidos (nunca os recebidos) poderão ser partilhados publicamente pela aplicação num servidor oficial e localizado em território nacional. Nenhum identificador é armazenado no sistema por um período superior a 14 dias.

Como resultado do processamento dos identificadores aleatórios, o utilizador poderá receber um alerta com informação de potencial risco de contágio e a data de ocorrência do mais recente contacto de proximidade que lhe deu origem. Esta informação é mantida pela aplicação até ser desinstalada.

Recolha e processamento de dados

O sistema é composto por dois sub-sistemas:

- um sub-sistema de avaliação de contactos de proximidade, que compreende a aplicação e um servidor (SPD);
- um sub-sistema de gestão de códigos de legitimação de diagnóstico, que compreende um cliente web e um servidor (SLD).

Ambos os servidores estarão em território nacional e sob o controlo de uma entidade pública ou de uma entidade privada com competências delegadas. Estas entidades serão, para o Servidor SPD, o INCM e para o Servidor SLD, a SPMS.

A aplicação utiliza a tecnologia Bluetooth de baixo consumo (BLE) para difundir e receber identificadores aleatórios de dispositivos próximos. Quando sob o alcance de um outro dispositivo a executar a aplicação, a aplicação armazena os seguintes dados:

- os identificadores aleatórios difundidos pelo outro dispositivo;
- a potência do sinal;
- a data e a duração estimada do contacto.

No caso de um utilizador ser diagnosticado com COVID-19 os seguintes dados são armazenados no SLD:

- o CL, para obtenção de certificado de acesso ao SPD;
- a data dos primeiros sintomas ou a data de teste para indivíduos assintomáticos;
- a data em que estes dados deverão ser destruídos no SLD;
- o número de vezes que o CL foi utilizado (0 ou 1, já que é de utilização única).

O servidor SPD contém uma lista com os seguintes dados:

- os identificadores aleatórios de utilizadores diagnosticados com COVID-19;
- a data de cada identificador.

Apagamento dos dados, desinstalação e descontinuação da aplicação

Nenhum identificador é armazenado no sistema por um período superior a 14 dias.

Conforme acima referido, na sequência do processamento dos identificadores aleatórios, os utilizadores poderão receber alertas com informação de potencial risco de contágio e a data de ocorrência do mais recente contacto de proximidade que lhe deu origem. Esta informação é mantida pela aplicação até ser desinstalada.

O utilizador pode a qualquer momento desinstalar a aplicação. A desinstalação vai resultar no apagamento de todos os dados locais da aplicação.

Resultado idêntico ocorre no contexto da voluntária submissão do código de legitimação por parte de um utilizador diagnosticado com COVID-19. Neste caso a aplicação deixará de funcionar, apresentando apenas o ecrã exemplificado em 2.5.3 “Diagnosticado com COVID-19 e com as suas Chaves de Identificadores TEK comunicadas”. Para funcionar novamente a aplicação deverá ser apagada e novamente instalada, com a consequente geração de novas Chaves de Identificadores TEK.

Todo o sistema será descontinuado assim que for declarado em Portugal o fim da pandemia.

4.1. Ativos de informação

Para além dos dispositivos móveis pessoais, expectavelmente *smartphones* com sistema operativo Android ou iOS, o sistema STAYAWAY COVID consiste em dois serviços centralizados: Servidor de Legitimação de Diagnóstico e Servidor de Publicação de Diagnóstico. Estes serviços serão operacionalizados em computadores tradicionais, dimensionados de acordo com o tipo de carga estimado e configurados em cluster assegurando a replicação necessária a responder a eventuais aumentos de carga e à falha de até um computador. Todo o software instalado nestes computadores deverá ser de código aberto.

Os ativos de informação para estes serviços serão alojados em centros de dados em território nacional. O SPD será alojado num centro de dados da INCM e o SLD será alojado num centro de dados da SPMS. O serviço de publicação de diagnóstico é alojado na INCM que está em conformidade com a norma ISO 27001.

4.2. Transferências de dados para países terceiros em relação à União Europeia ou organizações internacionais

Não estão previstas transferências internacionais de dados para além das implicadas pelo cariz público dos dados constantes do servidor SPD e do armazenamento local de informação ao nível dos próprios dispositivos móveis dos utilizadores.

Apesar da irrestrita faculdade de desinstalação da aplicação por parte do utilizador, a título complementar, seria desejável prever-se uma data limite quanto à descontinuação do sistema (um prazo máximo razoável), ultrapassando dessa forma a incerteza adveniente da dependência de uma declaração oficial de fim da pandemia. Importa, igualmente, assegurar a eliminação definitiva dos dados aquando daquela descontinuação ou em prazo ulterior, mas determinado ou determinável.

Aceitável	☒	**Aceitável com recomendações**	☐	**Inaceitável**	☐

5. Princípios Fundamentais e direitos dos titulares

5.1. Limitação das finalidades - remissão

Considerado como uma verdadeira trave mestra do regime jurídico europeu da proteção de dados pessoais, o princípio da finalidade[11] *"funciona como a primeira justificação para a realização de um tratamento de dados, impondo-se até ao consentimento"*[12].

Como ficou dito acima, na Secção 3, a aplicação pretende dar um contributo significativo para a rápida interrupção das cadeias de infeção no decurso da epidemia provocada por COVID-19, procurando detetar, apoiada pela automatização, os chamados contactos intensivos. A finalidade invocada prende-se, portanto, e fundamentalmente, com um desiderato sanitário ou de saúde pública. A este propósito remete-se para o supra exposto na referida secção.

Tal caraterística reflete-se, mormente, no cariz assumidamente temporário e excecional da medida, sendo que a utilização da tecnologia deve ter por limite a própria declaração do fim da pandemia pelo Estado. O cumprimento rigoroso deste princípio releva, de resto, para evitar um possível efeito banalizador da utilização deste tipo de tecnologias de monitorização, especialmente quando efetuada em larga escala, apenas justificável, como veremos adiante, à luz do princípio da proporcionalidade, atendendo à excecionalidade das circunstâncias presentes.

5.2. Base jurídica do tratamento

Ultrapassado o período pré-tecnológico, o atual estado tecnológico é caracterizado por apresentar meios mais sofisticados e multiplicar os meios de deteção, difusão e reprodução audiovisual e informático. O grande desafio passou a ser o de garantir o controlo sobre a privacidade dos dados nesta sociedade de informação. O RGPD trouxe um conjunto de novos desafios para a tutela dos direitos de personalidade, como o direito à reserva sobre a intimidade da vida privada, passando a disciplinar o tratamento dos dados pessoais nos meios automatizados (parcial ou totalmente).

A importância atribuída à privacidade e proteção dos dados pessoais em Portugal não é de agora, tendo em conta a sua inclusão na Lei Fundamental, a CRP, desde a sua primeira versão, e sucessivos diplomas que regulam a sua aplicação, como a recente Lei Nacional de Proteção de Dados que vem assegurar a execução, na ordem jurídica nacional, do RGPD, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, no decorrer, desde logo, do preâmbulo da Carta dos Direitos Fundamentais da

11 O Tribunal de Justiça tem considerado que o conteúdo essencial do direito à proteção dos dados pessoais, garantido no artigo 8.° da Carta, é preservado quando as finalidades do tratamento estão circunscritas e o tratamento é acompanhado de regras destinadas a garantir, nomeadamente, a segurança, a confidencialidade e a integridade destes dados, bem como a protegê-los contra os acessos e os tratamentos ilegais. Cfr. Data Protection Commissioner c. Facebook Ireland Limited, Maximillian Schrems, Proc. n.º C-311/18, de 9 de maio de 2018; Conclusões do Advogado-Geral HENRIK SAUGMANDSGAARD ØE apresentadas em 19 de dezembro de 2019; Parecer 1/15: Parecer do Tribunal de Justiça (Grande Secção) de 26 de julho de 2017 — Parlamento Europeu [Parecer proferido nos termos do artigo 218.°, n.° 11, TFUE (n.º 150).

12 ALEXANDRE SOUSA PINHEIRO, *Privacy e Proteção de Dados Pessoais - a construção dogmática do direito à identidade informacional*, Lisboa, AAFDL, 2015, página 826.

União Europeia, "a União baseia-se nos valores indivisíveis e universais da dignidade do ser humano, da liberdade, da igualdade e da solidariedade; assenta nos princípios da democracia e do Estado de direito. Ao instituir a cidadania da União e ao criar um espaço de liberdade, segurança e justiça, coloca o ser humano no cerne da sua ação".

Temos assistido nas últimas décadas a um desenvolvimento acentuado da tecnologia com evidentes repercussões no processamento da informação e no tratamento de dados pessoais. A aplicação de ferramentas tecnológicas que permitem pesquisar, relacionar, agrupar indexar e contextualizar dados pessoais registou um aumento exponencial. As vantagens da utilização destas tecnologias são inegáveis para a eficiência nos processos decisórios nos vários planos em que os mesmos se encontrem, científico, económico, de gestão pública, de garantia pública da segurança.

Todavia, o processo de circulação e análise de informação tem impacto na vida das pessoas, por dificultar o respetivo controlo ou mitigação, colocando em risco a vida privada de cada um de nós e condicionando a liberdade individual[13]. Neste sentido, o RGPD veio apresentar-se, no seguimento da anterior Diretiva, com a intenção de reforçar os direitos dos titulares dos dados e assegurar a livre circulação dos dados no espaço europeu, para cumprimento de finalidades económicas e de investigação, apesar de destacar que o direito à proteção dos dados pessoais não consubstancia um direito absoluto[14], devendo, como sublinha o considerando 4 do RGPD, ser considerado em cada caso em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade[15].

Neste contexto, importa recordar que o artigo 52.º, n.º 1, da Carta de Direitos Fundamentais da União Europeia admite a introdução de restrições ao exercício de direitos como os consagrados pelos seus artigos 7.º e 8.º, desde que essas restrições sejam previstas por lei, respeitem o conteúdo essencial dos referidos direitos e liberdades e, na observância do princípio da proporcionalidade, sejam necessárias e correspondam efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e das liberdades de terceiros.

O Tratado de Lisboa apresenta o inegável valor acrescentado resultante da luta contra os flagelos com dimensão transfronteiriça, fomentando a investigação sobre as respetivas causas, incluindo iniciativas para definir orientações e indicadores, organizar o intercâmbio das melhores práticas e preparar os elementos necessários à vigilância e à avaliação periódicas. A UE tem vindo a fazer um caminho de proteção da Saúde cada vez mais largo e profundo, desde as iniciais preocupações com a saúde dos trabalhadores até ao atual elevado nível de proteção da saúde que inclui a vigilância, alerta e combate contra as ameaças de saúde pública e o incentivo à cooperação entre os Estados-Membros, a fim de aumentar a complementaridade dos seus serviços de saúde.

É elementar reconhecer a importância do tratamento de dados de saúde para a proteção da saúde individual e para a saúde pública, bem como para a melhoria dos sistemas de saúde.

---

13 FILIPA URBANO CALVÃO, «Garantia de direitos: a proteção de dados pessoais perante os desafios tecnológicos», in Garantia de Direitos e Regulação: Perspetivas de Direito Administrativo, AAFDL Editora, 2020, página 224.

14 Sobre a diferença entre direitos aboslutos e direitos sujeitos a limitações ver Commission Staff Working Paper, Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments, SEC (2011) 567 final, page 9 and FRA handbook "Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level", Guidance, May 2018, página 70.

15 Acórdão Volker und Markus Schecke e Eifert, Proc. n.º C-92/09 e de 9 de novembro de 2010 (n.º 48); Acórda GC e o. c. Commission nationale de l'informatique et des libertés (CNIL), Proc. n.º C-136/17, de 24 de setembro de 2019.

O Regulamento define dados relativos à saúde como "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, que revelam informações sobre o seu estado de saúde". A regra quanto ao tratamento de dados de saúde é a proibição do seu tratamento, nos termos do artigo 9.º, n.º 1 do RGPD. O n.º 2 do mesmo artigo enuncia, porém, os fundamentos de licitude[16] para o tratamento de dados pessoais que, feita a ponderação abstrata perante os conflitos normativos em presença, o legislador europeu entendeu preservar.

Sem prejuízo da enorme relevância de cada um dos fundamentos constantes das alíneas do n.º 2 do artigo 9.º do RGPD, analisemos a alínea i). No quadro da COVID-19, a compreensão de como a saúde pública pode constituir fundamento de tratamento de dados pessoais das categorias especiais de dados tem sido generalizadamente aceite. Atentemos, no artigo 168.º, n.º 1 do TFUE, na Convenção Europeia de Direitos Humanos, ou no Relatório Sanitário Internacional que colocam em evidência os deveres estatais de vigilância, de cooperação, bem como a importância de mecanismos de alerta e de respostas adequadas[17].

De um lado, temos a necessidade de configurar com precisão a colisão entre os bens em causa, configuração esta que não pode deixar de apelar a um referente constitucional, mais precisamente, ao campo dos direitos fundamentais, com vincados problemas de interpretação e integração constitucional, na ausência ou presença de lei, como a seu tempo veremos, com enfoque nos artigos 18.º, 27.º e 35.º da CRP. Por outro lado, a localização sistemática da temática de proteção de dados e da saúde pública não se afigura tarefa fácil ou livre de polémica, a exigir uma atenta delimitação dos respetivos âmbitos.

Podemos caracterizar o bem jurídico saúde pública como o interesse comunitário numa existência livre de doenças, a exigência da salubridade essencial às relações intersubjetivas. "Falamos de um bem jurídico coletivo que não se materializa na lesão da vida ou da integridade física do cidadão individualmente considerado, mas que respeita às condições mínimas de salubridade necessárias ao tráfico jurídico, comercial, laboral, ao lazer, enfim, à fruição de uma vida, entendida em todas as suas fases e dimensões, livre — atendendo às actuais possibilidades tecnológicas — de patologias."[18]

A epidemia de SRA, a Gripe das Aves, e a Gripe A, vieram corroborar o cenário de difusão e profusão à escala global de riscos vários. Neste contexto a OMS adotou na 58ª Assembleia Mundial da Saúde, os International Health Regulations (2005). Este diploma evidenciava como objetivo principal "*prevent, protect against, control and provide a public health response to the international spread of disease in ways that are commensurate with and restricted to public health risks, and which avoid unnecessary interference with international traffic and trade*". A preocupação subjacente prendia-se com o respeito pelos perigos advindos do comércio internacional e da circulação de pessoas entre Estados. Apesar da clara orientação para a obtenção do consentimento, o diploma prevê, no art.º 31.º, n.º 2, c), a possibilidade de recurso a medidas compulsivas (rastreio, vacinação, isolamento, quarentena) no caso de recusa de um viajante de um Estado-Membro em ser examinado, vacinado, ou sujeito a outra medida

[16] Ou, caso se prefira, exceções ao princípio de proibição, sempre carecendo da devida articulação com os fundamentos de licitude previstos no artigo 6.º do mesmo Regulamento. No caso vertente, o fundamento invocável em articulação com a disposição do artigo 9.º, recorde-se, seria o constante da alínea e) do nº.1, pressupondo um responsável pelo tratamento que seja um ente público ou atuando sob uma veste de autoridade pública.

[17] CLÁUDIA MONGE, «Proteção de dados de saúde nos hospitais públicos», *in Revista de Direito Administrativo*, n.º 8, 2020, página 81.

[18] PEDRO JACOB MORAIS, «O internamento compulsivo do portador de doença infecto-contagiosa notas de andar e ver», *in Lex Medicinae*, Ano 10, n.º 20 (2013) — páginas 148-149.

profilática, quando desta recusa de consentimento resulte um risco iminente para a saúde pública[19].

Caberia ainda referir, a este respeito, os Princípios de Siracusa, resultantes da conferência ocorrida entre 30 de abril e 4 de maio de 1984 na Cidade italiana de Siracusa, tendo reunido algumas das principais organizações votadas ao estudo e defesa dos Direitos Humanos e que são fundamentais para a interpretação do Pacto Internacional Sobre os Direito Civis e Políticos. No âmbito dos princípios elencados encontramos uma especial preocupação com a tutela da saúde pública permitindo, quando este bem jurídico se encontre ameaçado, a limitação de direitos.

Façamos, ainda, uma curta incursão de Direito Comparado. No ordenamento jurídico germânico, os meios de prevenção e controlo de doenças infecto-contagiosas encontram-se previstos na *Infektionsschutzgesetz* (IfSG), de 20 de julho de 2000. Este diploma é particularmente restritivo do direito à liberdade (*das Grundrecht der Freiheit der Person*), prevendo no §29 a possibilidade de rastreios. A Ley Orgánica de Medidas Especiales en Matéria de Salud Pública admite a possibilidade "de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas oportunas para el control de los enfermos" (Artigo 3.º).

Voltemos agora a nossa atenção para o panorama legal e jurisprudencial português, de forma a entendermos em que medida possui algum arrimo no nosso ordenamento jurídico o recurso a medidas norteadas por preocupações de saúde publica, incluindo aquelas que poderão considerar-se restritivas de direitos fundamentais. A Lei n.º 81/2009 prevê, no art.º 17.º, que o "membro do Governo responsável pela área da saúde pode tomar medidas de exceção indispensáveis em caso de emergência em saúde pública", independentemente de nos encontramos em estado de emergência, nos termos do 18.º da CRP (os conceitos não podem aqui ser confundidos).

O art.º 17.º, n.º 1 da Lei n.º 81/2009 deve ser lido em conjunto com a Base 34 da Lei de Bases da Saúde, Lei n.º 95/2019, de 4 de setembro, de acordo com a qual para a defesa da saúde pública a autoridade de saúde pública pode, nos termos da alínea c) "exercer a vigilância sanitária do território nacional e fiscalizar o cumprimento do Regulamento Sanitário Internacional ou de outros instrumentos internacionais correspondentes, articulando-se com entidades nacionais e internacionais no âmbito da preparação para resposta a ameaças, deteção precoce, avaliação e comunicação de risco e da coordenação da resposta a ameaças". Além de prever a possibilidade de, em situação de emergência de saúde pública, o membro do Governo responsável pela área da saúde, poder tomar as medidas de exceção indispensáveis, se necessário mobilizando a intervenção das entidades privadas, do setor social e de outros serviços e entidades do Estado (n.º 3).

Como daqui se retira, a Lei de Bases da Saúde apresenta um leque de instrumentos de controlo de doenças mais amplo do que a Lei n.º 81/2009, permitindo e prevendo a adoção de um vasto conjunto de instrumentos, aplicáveis, desde logo, a casos de epidemias.

5.2.1. Fundamento de licitude do tratamento

O CEPD vem observando a este propósito que o simples facto de a utilização de aplicações de rastreio de contactos ter lugar numa base voluntária não significa que o tratamento de dados

[19] IDEM, Ibidem, página 151.

pessoais se baseie necessariamente no consentimento. Efetivamente, voluntariedade e consentimento não se confundem a este respeito, como melhor se explicitará infra, muito embora o cariz voluntário e não discriminatório das aplicações de rastreio deva ser assumido como um requisito determinante da opção pelo acolhimento de soluções tecnológicas deste tipo, sempre em obediência aos princípios fundamentais que devem reger uma sociedade democrática. Importa lembrar, de resto, a relação existente entre o direito à proteção de dados e outros direitos e liberdades fundamentais como a liberdade de circulação ou de associação. Como apontou recentemente a Comissão Europeia nas suas orientações acerca da adoção de aplicações de rastreio no combate à pandemia do COVID-19:

"*The functionalities included in the apps can have different impact on a wide range of rights enshrined in the Charter of Fundamental Rights of the EU, such as human dignity, respect for private and family life, protection of personal data, the freedom of movement, non- discrimination, freedom to conduct a business, and freedom of assembly and of association*"[20].

Ora, como ainda recentemente referiu o Comité Europeu para a Proteção de Dados nas suas orientações, quando as autoridades públicas prestam um serviço com base num mandato conferido por e em consonância com os requisitos previstos na lei, afigura-se que a base jurídica mais pertinente para o tratamento é a necessidade de exercer funções de interesse publico, nos termos do disposto no artigo 6º, n.º 1, alínea e), do RGPD. Como já se assinalou, tal conclusão pressupõe a designação de um responsável pelo tratamento que, atenta a finalidade da aplicação de rastreio em análise, tenha por mandato o exercício de funções de interesse público ou de autoridade pública.

A este propósito o artigo 6.º, nº. 3, do RGPD esclarece que o fundamento jurídico em questão é definido pelo Direito da União ou do Estado-Membro ao qual o responsável pelo tratamento está sujeito. A finalidade do tratamento deve, pois, enquadrar-se no âmbito do exercício das funções de interesse público assinaladas. Neste sentido, o tratamento de dados pessoais pode, desde logo, ser lícito, nomeadamente, se no Direito nacional estiverem previstas garantias adequadas e específicas.

Para além disso, a base jurídica ou medida legislativa que fornece o fundamento legal para a utilização de aplicações de rastreio de contactos deve incorporar salvaguardas significativas e, conforme prevê o artigo 9.º. n.º 2. i) (aplicável, como vimos, aos dados de saúde ou relativos à saúde, cujo tratamento é necessário por motivos de interesse público no domínio da saúde pública), prever medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional.

Tal ocorreu, ainda recentemente, em Portugal, de resto, num contexto de utilização de uma aplicação móvel relacionada com o que aqui nos ocupa. Aludimos ao designado sistema Smart Crowd, da responsabilidade da Agência Portuguesa do Ambiente, I.P, consistindo o mesmo numa solução tecnológica, com recurso a uma aplicação móvel, que, no âmbito da pandemia da Covid-19, visa permitir a identificação da "taxa de ocupação das praias de maior pressão", para dotar a população com informação que lhe permita, sem necessidade de deslocação, tomar a decisão de escolher uma determinada praia que garanta o distanciamento social fixado.

Tendo em vista garantir o controlo da pandemia da Covid-19, o fundamento de licitude do tratamento baseou-se na necessidade para o exercício de funções de interesse público de prevenção de risco e de proteção da saúde pública, atribuído à APA pelo Decreto-Lei n.º. 24/2020, de 25 de maio, no específico contexto do acesso, ocupação e utilização das praias na

[20] Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, C(2020) 2523 final, Brussels, 16 April 2020, p. 4.

época balnear de 2020. No caso do sistema STAYAWAY COVID, não restam dúvidas de que a mesma solução se adequaria, por maioria de razão, atenta a respetiva finalidade, em linha, de resto, com o recomendado pela Comissão Europeia e pelo Comité Europeu para a Proteção de Dados.

No entanto, com outra finalidade declarada, não seria de excluir a invocação de uma outra base jurídica, designadamente o consentimento, *in casu*, com base no artigo 6.º, n.º 1, alínea a) e o artigo 9.º, n.º 2, alínea a) do RGPD. Caberia ao responsável pelo tratamento de dados, em tal contexto, assegurar o cumprimento dos exigentes requisitos legais da validade do consentimento.

Com efeito, apenas em muito contados casos, as aplicações desenvolvidas por outros Estados-Membros têm por base o consentimento. Acresce que, no que diz respeito à possibilidade de invocar o consentimento como base jurídica das atividades de tratamento, nos termos do artigo 6.º, n.º 1, alínea a), do RGPD, devem ser tidos em conta alguns aspetos.

O consentimento implica "qualquer indicação livre, específica, informada e inequívoca da vontade da pessoa em causa, através da qual esta, por declaração ou ação afirmativa clara, manifesta o seu acordo quanto ao tratamento dos dados pessoais que lhe dizem respeito". Por seu turno, a voluntariedade pressupõe uma escolha genuína para a pessoa em causa[21], só então cumprindo a sua função protetora. A fim de avaliar as opções, o contexto em que o consentimento deve ser dado deve ser analisado de forma mais pormenorizada. O objetivo do sistema é o de permitir reduzir o risco de infeção devido ao contacto com uma pessoa que tenha apresentado resultados positivos, para conter a pandemia. O argumento contra a validade deste consentimento é a existência de uma clara diferença de poder entre o responsável pelo tratamento e a pessoa em causa, o que é classicamente o caso da relação entre os cidadãos e as autoridades públicas, por defeito, de subordinação. Nesta linha argumentativa, se for dado consentimento a uma autoridade pública, presume-se geralmente que este não é dado voluntariamente (*vide* considerando 43 do RGPD). Pelo contrário, deve ser demonstrado, em cada caso individual, que o desequilíbrio que tipicamente existe na situação em causa não se aplica. Por conseguinte, devem ser estabelecidos requisitos especiais aquando da concessão do consentimento a uma autoridade pública.

Não por acaso, sublinha-se novamente, o CEPD observa que o simples facto de a utilização de aplicações de rastreio de contactos ter lugar numa base voluntária não significa que o tratamento de dados pessoais se baseie necessariamente no consentimento[22].

Este desequilíbrio apenas poderia vir a ser compensado pelo facto de a utilização não ser obrigatória e não implicar quaisquer consequências jurídicas diretas, antes a ausência de desvantagens normativas diretas no caso de não utilização.

Ora, na hipótese em apreço, haveria ainda de ser considerada a possibilidade de que a pressão social pudesse ser exercida de forma não negligenciável para o indivíduo se comportar de acordo com as expectativas do ambiente social, do Estado ou dos operadores da app e para utilizar a app em conformidade[23].

Em suma, para que um consentimento possa ser considerado válido, o responsável deve provar a possibilidade de oposição ao consentimento e que este possa ser retirado sem consequências

[21] Grupo de Trabalho de Protecção de Dados do artigo 29º, Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679, p. 5.

[22] Diretrizes 4/2020 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19, de 21 de abril de 2020, ponto 29.

[23] "Data Protection Impact Assessment for the Corona App", página 52.

negativas. Para além disto, recorde-se, o consentimento deve ser dado de forma informada. Para tal, o responsável pelo tratamento deve fornecer à pessoa em causa as seguintes informações: a identidade do responsável pelo tratamento, as finalidades do tratamento para o qual se pretende obter o consentimento, as categorias de dados a serem tratados, o direito de retirada se os dados forem utilizados para a tomada de decisão automatizada nos termos e a utilização e os riscos das transferências para países terceiros que não tenham um nível adequado de proteção de dados. Esta informação deve, na medida do possível, ser fornecida em linguagem clara e simples e ser fácil de encontrar e não escondida entre outros textos[24].

Traçado o presente enquadramento cabe, finalmente, referir que a decisão final quanto ao fundamento de licitude concretamente invocado deverá competir ao responsável pelo tratamento de dados que venha a ser designado, em todo o caso sempre antes do início das operações de tratamento e, portanto, da disponibilização da solução tecnológica em avaliação.

A este propósito, a Deliberação 2020/277 da CNPD, de 20 de junho, relembra que o consentimento do titular, enquanto manifestação de vontade inequívoca à instalação da aplicação no seu dispositivo móvel, será fundamento de licitude desde que cumpridos os quatro requisitos que tornam o seu consentimento válido (previstos na alínea 11 do artigo 4º do RGPD). Acrescenta, ainda, a Deliberação que "(...) 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 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.".

A STAYAWYAY COVID seguirá de perto as orientações veiculadas pelas autoridades europeias quanto ao fundamento de licitude de tratamento de dados no âmbito de aplicações com a mesma finalidade,[25] bem como a deliberação da CNPD quanto à pertinência em assegurar um duplo fundamento de licitude, como reforço da legitimidade e proporcionalidade das operações de tratamento de dados levadas a cabo. Destarte, é implementado um mecanismo para a prestação de consentimento prévio à instalação da aplicação, cumprindo com os requisitos de validade previstos no RGPD, segundo o qual o consentimento deverá ser uma manifestação de vontade livre, específica, informada e explícita, expressa através de um ato positivo inequívoco.

Acresce que numa fase preliminar da instalação, o utilizador deve declarar ter pelo menos 13 anos (idade mínima para aceder ao serviço) e conceder as autorizações necessárias para o funcionamento da aplicação.

Nota de atualização - versão 2 da AIPD:

O Decreto-Lei de enquadramento legal do sistema STAYAWAY COVID foi promulgado dia 4 de agosto de 2020 e publicado a 11 de agosto. O Decreto-Lei 52/2020 de 11 de agosto estabelece como responsável pelo tratamento de dados a Direção-Geral de Saúde e regula a intervenção do médico no sistema.

[24] Grupo de Trabalho de Proteção de Dados do artigo 29º, Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679, 2018, p. 14.

[25] Communication from the Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 16.04.2020; Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 21-04-2020.

5.3. Princípio da responsabilidade

Já no quadro da anterior Diretiva 95/46/CE, era aceso o debate acerca do conceito funcional de responsável do tratamento, enquanto conceito atribuidor da fundamental responsabilidade legal pelo incumprimento dos normativos aplicáveis em matéria de proteção de dados pessoais.

Os artigos 24.º e 25.º do RGPD espelham bem a relevância nuclear da figura do responsável pelo tratamento no quadro jurídico da proteção de dados pessoais, ao detalharem as obrigações legais que sobre o mesmo impendem, designadamente, as de adotar as medidas organizativas e técnicas e as políticas adequadas por forma a demonstrar o cumprimento do Regulamento e assegurar, "desde a conceção e por omissão", isto é, desde a determinação dos fins e meios do tratamento e no seu decurso, o respeito pelos princípios fundamentais contidos nos artigos 5.º e 6.º e o respeito pelos direitos dos titulares dos dados previstos nos artigos 13.º e seguintes.

O conceito de responsável pelo tratamento encontra as suas origens históricas no de "responsável pelo ficheiro", da Convenção 108 do Conselho da Europa, relativamente ao qual constitui um nítido avanço no sentido em que possui um escopo muito mais alargado correspondendo-lhe um papel bem mais relevante.

Desta feita é responsável pelo tratamento "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro".

A noção decompõe-se em três elementos nucleares.

Do seu elemento subjetivo destacamos a ideia de que tanto pessoas singulares, como coletivas poderem assumir esse estatuto.

O elemento essencial concerne à determinação das finalidades e dos meios de tratamento dos dados pessoais e, reconduz-se fundamentalmente, à influência de facto exercida relativamente à escolha daquelas finalidades bem como dos meios do tratamento que possam qualificar-se, em dado contexto, como essenciais. Na esteira do Acórdão do Tribunal de Justiça da União Europeia (TJUE) proferido no processo C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein[26] diremos que a avaliação das circunstâncias de facto de que depende a aferição, perante uma dada atividade de tratamento de dados, daquela influência determinante (definidora do estatuto de responsável pelo tratamento) remete para as razões que conduziram ao próprio tratamento de dados e ao ente que o decidiu em primeira linha e que do mesmo beneficia. Com efeito, para além dos casos em que tal determinação deriva de uma competência legalmente atribuída (pelo Direito de um Estado Membro ou da União) ou meramente implícita através da atribuição de uma competência que implica ou envolve forçosamente a realização de operações de tratamento de dados pessoais, aquela avaliação reside, não na aplicação de um critério formal, mas na análise do circunstancialismo de facto de cada caso concreto. Assim, e em suma, o responsável pelo tratamento é aquele que decide o porquê e o como de uma dada operação de tratamento de dados pessoais.

[26] Acórdão proferido no contexto de um reenvio prejudicial referente ao caso de uma página de fãs na rede social Facebook e ao estatuto de responsável pelos tratamentos de dados efetuados através daquela página.

A jurisprudência do mesmo TJUE, através, designadamente, dos casos Jehovan todistajat[27] e mais recentemente do caso Fashion ID[28] veio igualmente firmar a noção de que o acesso aos dados pessoais, em si mesmo considerado, não deve ser interpretado como uma condição s*ine qua non* da qualificação enquanto responsável pelo tratamento de dados pessoais de um determinado interveniente numa operação de tratamento de dados.

Finalmente, um terceiro elemento da definição em apreço (que se antolha no segmento "individualmente ou em conjunto com outras") refere-se à possibilidade da existência de situações de responsabilidade partilhada por parte de uma pluralidade de intervenientes numa operação de tratamento. Esta possibilidade já era admitida pelo regime da Diretiva 95/46/CE, mas mereceu no RGPD um tratamento mais rigoroso e exaustivo, sendo-lhe dedicado o artigo 26º. Nos termos deste artigo com a epígrafe "Responsáveis conjuntos pelo tratamento", define-se esta tipologia como aquela em que dois ou mais responsáveis pelo tratamento determinam conjuntamente as finalidades e os meios desse tratamento, sendo por isso responsáveis conjuntos relativamente ao mesmo.

Recentemente, em novembro de 2019, a Autoridade Europeia da Proteção de Dados (AEPD), Autoridade independente com o mandato de assegurar o cumprimento por instituições e organismos da UE do Regulamento EU 2018/1725 (instrumento que em muito se assemelha ao RGPD) emitiu orientações no sentido de aconselhar as instituições e organismos da UE nas suas atividades de tratamento de dados pessoais acerca da aplicação dos conceitos de responsável pelo tratamento, subcontratante e de responsáveis conjuntos. Dada a referida e notória aproximação entre os regimes de ambos os regulamentos, as orientações em questão fornecem um recurso útil para a compreensão atualista daqueles conceitos, numa altura em que se aguardam também (previsivelmente em 2020) orientações de idêntico teor por parte do Comité Europeu da Proteção de Dados, na sequência da aprovação do RGPD e da consequente extinção do GT29.

Estas orientações vêm agora, fundamentalmente, confirmar vários dos entendimentos e critérios que já resultavam em larga medida da opinião 1/2010 do GT29, e que ao longo da última década foram sendo densificados pela jurisprudência do TJUE. Segue-se, em suma, a mesma abordagem funcional aos dois conceitos nucleares em apreço.

Contudo, interessantes exemplos ilustrativos são propostos, aclarando os referidos conceitos em áreas não cobertas pela citada opinião do GT29. Assim, e em resumo, torna-se inequívoco que cabe apenas ao responsável pelo tratamento a determinação das finalidades do mesmo, bem como, pelo menos, dos meios essenciais utilizados. Por outro lado, na esteira da jurisprudência supracitada, é confirmado o entendimento segundo o qual a qualificação enquanto responsável pelo tratamento não depende do seu acesso aos dados pessoais. Este critério aplica-se igualmente às situações de responsabilidade conjunta, sendo prescindível que ambos os responsáveis tenham acesso aos referidos dados.

Relativamente ao subcontratante sublinha-se o reconhecimento da sua margem de autonomia e capacidade para determinar os meios do tratamento (desde que não essenciais), admitindo-se até que aconselhe o responsável quanto à respetiva adoção, distinguindo-se, portanto, claramente de um mero subordinado do responsável.

[27] Acórdão proferido a 10 de julho de 2018 no caso C-25/17, processo referente à responsabilidade pelo tratamento de dados pessoais implicado nas comunicações porta-a-porta realizados por testemunhas de jeová, e à possibilidade de responsabilidade conjunta com a respetiva comunidade religiosa.

[28] Acórdão de 29 de julho de 2019 no processo C-40/17, proferido no contexto de um reenvio prejudicial referente ao caso de uma página de fãs na rede social Facebook e ao estatuto de responsável pelos tratamentos de dados efetuados através daquela página.

Um interessante exemplo é o da responsabilidade de um subcontratante pelo integral desenvolvimento, gestão e manutenção de uma ferramenta de TI a usar por outra entidade (organismo), responsável pelo tratamento, a quem caberia, no entanto, e sempre, a determinação dos já aludidos elementos essenciais dos meios do tratamento (prazos de conservação de dados, destinatários dos dados e acessos). No caso de o referido subcontratante extravasar o seu papel (definido contratualmente ou legalmente) participando na determinação da finalidade ou dos meios essenciais do tratamento, será tido como responsável ou responsável conjunto do tratamento.

No entanto, ainda neste caso, importará aferir da natureza e extensão do desvio em causa, dado que o mesmo poderá, por exemplo, servir unicamente um propósito de cumprimento de certos princípios de proteção de dados, não implicando a determinação de uma finalidade de tratamento própria. Finalmente, vale a pena destacar, entre os critérios definidores do subcontratante apresentados sinteticamente numa *checklist*, para além dos mais frequentemente utilizados, o requisito da não decisão acerca do fundamento de licitude do tratamento, bem como a ausência de decisão quanto à divulgação dos dados e respetivos prazos de conservação.

Sem prejuízo do debate acerca do papel assumido pelos vários intervenientes no processo de conceção, desenvolvimento, implementação e manutenção de uma solução do tipo aqui analisado, em particular quando gizada a partir de contribuições múltiplas e provenientes de entidades de diferente natureza, tanto académicas, como empresariais, e de diversos contextos colaborativos ou espontâneos[29], cabe assinalar, como já se fez na anterior secção 3, a importância da definição clara das responsabilidades do tratamento de dados, no intuito da defesa dos direitos dos titulares.

A designação de um ou vários responsáveis é tanto mais relevante quanto está em causa uma solução de rastreio que inevitavelmente passa por uma monitorização sistemática e em grande escala de dados pessoais relativos aos contactos entre pessoas singulares ainda que codificados. Por este motivo, os reguladores de vários Estados-Membros, assim como o Comité Europeu para a Proteção de Dados, têm entendido que o Ministério de Saúde dos Estados-Membros ou as respetivas autoridades de saúde, deviam ser os responsáveis pelo Tratamento, sem prejuízo de previsão de outros responsáveis de tratamento. Atendendo à finalidade do tratamento em questão, diremos concordar com a asserção segundo a qual se justificaria plenamente a atribuição de tal responsabilidade a uma entidade pública ou no exercício de funções de interesse público, a quem seja atribuído o mandato de operar o sistema em causa no contexto específico do controlo da pandemia do COVID-19, e de acordo com critérios e salvaguardas previamente definidos, em linha com os requisitos emanados das autoridades europeias supra citados.

Nota de atualização - versão 2 da AIPD:

[29] A este título tem sido muito discutido o papel das empresas Google e Apple na perspetiva da proteção de dados, sendo defensável a sua qualificação como responsáveis pelo tratamento de dados (e não como meros fornecedores de tecnologia, afastando-se igualmente a hipótese de serem subcontratantes) atenta a autonomia com que definem finalidades e meios essenciais dos tratamentos de dados em questão. Neste sentido poderá, efetivamente, argumentar-se que o desenvolvimento da sua API correspondeu a uma iniciativa unilateralmente planeada e financiada por aquelas empresas, sendo que várias das suas configurações são, igualmente, por si determinadas unilateralmente, incluindo no que concerne à definição de prazos de conservação de dados, mesmo que de forma alinhada com parâmetros propostos por terceiras entidades, designadamente organizações supranacionais como a OMS ou a própria União Europeia, através da Comissão Europeia. Por outro prisma, mas com menor relevância prática, os próprios utilizadores finais da aplicação, na medida em que os respetivos dispositivos processam localmente dados pseudonimizados de outros utilizadores, poderiam, também, em certa asserção, ser considerados como responsáveis pelo tratamento de dados relativamente àqueles dados.

O entendimento sufragado nas versões anteriores da AIPD foi acompanhado pela Comissão Nacional de Proteção de Dados, na Deliberação 2020/277, de 20 de junho, tendo sido, entretanto, objeto de normação legal, através do Decreto-Lei 52/2020 de 11 de agosto, o estabelecimento da Direção-Geral da Saúde como o Responsável de Tratamento de Dados bem como pela operacionalização do sistema.

Nesta sequência, os demais intervenientes que sejam envolvidos na operacionalização do sistema, assumirão, em princípio, o papel de subcontratantes do responsável pelo tratamento designado.

5.4. Exatidão e limitação da conservação

Como forma de controlar a exatidão da informação relativa ao contágio, e do mesmo passo mitigar a possibilidade de falsos positivos de notificação, na eventualidade de o utilizador da aplicação STAYAWAY COVID ser diagnosticado com COVID-19, pretende-se que, de forma simples, segura e anónima, submeta as Chaves de Identificadores TEK armazenadas no seu DMP ao Servidor de Publicação de Diagnóstico (SPD). Porém, para este efeito, requer-se que lhe seja fornecido, por canal externo ao sistema STAYAWAY COVID, um número aleatório de 12 algarismos (CL), pela entidade responsável pelo diagnóstico. Esta validação por um profissional de saúde (médico) autenticado, é essencial à garantia de exatidão da referida informação.

Apenas após cumprido este procedimento, o DMP o submete ao Servidor de Legitimação de Diagnóstico (SLD), por canal de comunicação seguro. Em resposta, o DMP recebe um Código de Acesso (CA) que tem a forma de um *JSON Web Token* (RFC 7519). Este CA permite ao DMP autenticar-se perante o SPD e submeter as Chaves de Identificadores TEK, que por sua vez, através do processamento de dados realizado localmente nos DMP permitirá o envio de alertas de exposição a um potencial risco de contágio. Em suma, as notificações de exposição apenas poderão ter lugar após validação por profissional de saúde autenticado e com base na iniciativa do próprio utilizador que tenha sido diagnosticado com COVID-19.

No que concerne à limitação da conservação dos dados, este princípio surge refletido desde logo na funcionalidade que determina que nenhum identificador é armazenado no sistema por um período superior a 14 dias.

Por outro lado, todo o sistema será descontinuado assim que for declarado em Portugal o fim da pandemia, não se justificando a conservação de dados por mais tempo, atenta a inexistência de outra finalidade que a fundamente.

Para além disto, como se explicita na secção 4, ao utilizador é permitido a qualquer momento desinstalar a aplicação. A desinstalação vai resultar no apagamento de todos os dados processados pela aplicação, incluindo os dados armazenados no servidor do sistema.

Resultado idêntico ocorrerá no contexto da voluntária submissão do CL por parte de um utilizador diagnosticado com COVID-19.

5.5. Privacidade desde a conceção e por omissão

Uma primeira medida organizativa fundamental que assegura, desde a conceção, o respeito pelos princípios e requisitos da proteção de dados pessoais, refere-se ao *supra* aludido cariz

voluntário da adoção e utilização da aplicação em causa. Este requisito essencial, que vem sendo destacado por governos nacionais, autoridades e instituições europeias[30] e autoridades de controlo nacionais, deve ser interpretado num sentido maximalista, como impondo a observância do princípio ao longo de todo o ciclo do tratamento de dados, o mesmo é dizer, da utilização da tecnologia, e não apenas no momento da sua instalação.

Neste sentido, os cidadãos não serão obrigados a descarregar a aplicação, mas tão pouco deverão ser obrigados a mantê-la ativa no seu dispositivo terminal, sendo-lhe possível, a qualquer momento, sem dificuldade ou consequência outra que não seja a de prescindir da respetiva utilização, proceder à desinstalação da aplicação. Acresce que o sistema tal como desenhado na solução STAYAWYAY COVID, baseia-se no respeito integral pela vontade dos utilizadores / titulares dos dados, também no momento da inserção dos códigos de legitimação por utilizadores diagnosticados como positivo, requerendo-se que esta ação individual, tomada de forma livre e à margem de constrangimentos ou pelas sociais, seja levada a cabo, isoladamente, pelo próprio utilizador, para que só então seja despoletado o mecanismo conducente à publicação, em servidor dedicado, das Chaves de Identificadores TEK do infetado.

No mesmo sentido aponta a natureza intrínseca do modelo distribuído baseado no protocolo DM3P cujas virtualidades, reconhecidamente, assentam largamente no contexto mais limitado em que ocorrem os tratamentos de dados realizados através de um servidor central. Ao invés, neste sistema, os tratamentos de dados, com destaque para os cruzamentos de dados necessários à finalidade prosseguida, ocorrem maioritariamente ao nível dos próprios dispositivos móveis. o que é comummente visto como uma forma de implementar o respeito pelo princípio da minimização de dados.

A pseudonimização, ela própria, (e não a anonimização de dados), surge expressamente referida no artigo 25º do RGPD como um dos mais relevantes exemplos de uma medida de privacidade desde a conceção, com o fito de assegurar o respeito e a aplicação efetiva dos princípios da proteção de dados pessoais, incorporando as garantias necessárias à tutela dos direitos dos titulares. Recorde-se, ainda, a este título, que as descritas medidas de pseudonimização adotadas na implementação deste sistema prefiguram-se como medidas de pseudonimização forte, de assinável robustez, visando possibilitar a partilha / intercâmbio de chaves (códigos aleatórios) aos demais participantes no sistema com preservação de anonimato.

Finalmente, as funcionalidades do sistema foram desenhadas para permitir um tratamento de dados limitado, por omissão, ao estritamente necessário para o cumprimento da respetiva finalidade, recorde-se: a da notificação de exposição a um potencial risco de contágio. Não são recolhidos, nem o sistema o permite, a recolha de dados adicionais de cariz epidemiológico, estatístico ou outro com objetivos distintos do enunciado.

5.6. Decisões individuais automatizadas, incluindo definição de perfis

Deve ser transparente para os utilizadores que a receção de uma notificação de alerta está longe de significar que aqueles se encontrem infetados. A aplicação tem como único desiderato alertar para a eventual existência de um risco potencial de contágio, com base em critérios probabilísticos baseados na mais atual evidência científica, mas que inevitavelmente

[30] A Comissão Europeia, o Comité Europeu para a Proteção de Dados e o Conselho da Europa emitiram orientações para utilização de aplicações móveis para rastreio de contactos. No Apêndice A é possível conferir os requisitos comuns definidos por estas organizações europeias e a respetiva implementação no sistema STAYAWAY COVID.

comportam alguma margem de erro a que se somam as possibilidades de falsos positivos enumeradas na presente avaliação.

Uma das formas mais relevantes de limitar em número aqueles falsos positivos prende-se com a intervenção assegurada por um médico, no sentido de validar a informação de contágio, previamente à partilha e publicação no servidor dedicado, das chaves que desencadeiam o processo de notificação automática. Acresce que esta publicação apenas ocorre após a inserção de um código no dispositivo do utilizador do sistema efetuada pelo próprio utilizador, conforme descreve em pormenor a secção 2 da presenta avaliação.

Esta dupla intervenção humana garante que no caso do sistema STAYAWAY COVID o tratamento de dados não é totalmente automatizado, caindo fora do âmbito de aplicação do artigo 22.º do RGPD.

5.7. Direito à informação

De modo a respeitar os princípios de tratamento previstos no artigo 5.º n.º 1 do RGPD, o responsável pelo tratamento deverá assegurar que o tratamento é realizado e explicado de modo transparente e claro ao utilizador. O responsável pelo tratamento, deste modo, fornecerá aos utilizadores em causa todas as informações necessárias ao cumprimento dos artigos 13.º e 14.º e do artigo 34.º do RGPD.

Neste sentido, serão dadas a conhecer as finalidades do tratamento, as medidas utilizadas para esses fins, em especial a duração do armazenamento dos dados pessoais, as transmissões de dados e os seus destinatários, e a forma como as pessoas em causa podem exercer eficazmente os seus direitos perante o responsável pelo tratamento, nomeadamente através do recurso à autoridade de controlo competente em matéria de proteção de dados.

A informação será disponibilizada ao utilizador antes da recolha dos dados, de forma gradual, principalmente através do fornecimento de informações sobre as principais características do tratamento, através quer da informação e política de privacidade existente na aplicação quer da informação e política constante do website do sistema STAYAWAY COVID. Neste sentido, os utilizadores deverão receber informações claras e transparentes antes de o pedido de acesso ser ativado, a fim de obter um conhecimento completo, nomeadamente sobre as finalidades e as operações de tratamento, sobre as técnicas de pseudonimização utilizadas para proteger a sua identidade e sobre os prazos de conservação dos dados. Serão fornecidos contactos do responsável ou responsáveis pelo tratamento bem como dos respetivos encarregados de proteção de dados.

Ademais, importa reforçar que utilizadores deverão ter acesso a informação específica e transparente sobre o caráter voluntário da aplicação nos vários momentos da sua utilização, incluindo a livre desinstalação em qualquer momento sem acarretar consequências negativas para o utilizador.

Conforme já ficou referido acima, a confiança do público no sistema é um fator fundamental para o seu êxito. Assim sendo, a transparência em torno do funcionamento do sistema e dos seus controlos de privacidade é fundamental para gerar essa mesma confiança. Por conseguinte é recomendável que a adoção e disponibilização pública de uma ferramenta com a natureza e finalidade assinaladas seja acompanhada de campanhas de informação e incentivo à sua utilização (tanto mais que a sua eficiência será tanto maior quanto o for o número de

utilizadores), com o envolvimento, entre outras, das entidades responsáveis pela condução das políticas públicas na área da saúde pública.

De resto, conforme refere a recomendação da CNPD na sua Deliberação 2020/277 de 29 de junho, no seu ponto 64, "(...) É importante que esta informação seja facultada cumprindo os requisitos de inteligibilidade do artigo 12º 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 a partir de uma idade inferior a 13 anos".

Esta recomendação da CNPD, é plenamente justificada e concordante com as preocupações dos promotores, reforçando a relevância do requisito da inteligibilidade da informação providenciada aos utilizadores da aplicação.

"Sendo certo que os remédios do passado já não são eficazes, é preciso repensar e reinventar o Estado de Direito, tornando o imbróglio algorítmico transparente e as suas decisões compreensíveis"[31]. Esta necessidade é tanto mais pertinente quanto um sistema como o STAYAWYAY se destinar, por natureza, a uma utilização alargada, a um heterogéneo universo de possíveis destinatários. A inteligibilidade encontra-se intrinsecamente relacionada com a necessidade de utilização de uma linguagem clara e simples[32]. Com efeito, no âmbito do tratamento de dados pessoais, tendo em conta as finalidades do tratamento, o responsável pelo tratamento de dados terá sempre ao seu dispor informação que lhe permita determinar em que moldes a informação deverá ser passada para ser percetível pelo público potencialmente alvo do tratamento. No caso em apreço pretender-se-á que todos os utilizadores de dispositivos móveis ao acederem à aplicação compreendam o seu alcance, bem como os limites inerentes à sua utilização.

Neste sentido, a informação disponibilizada procurará ser o mais concisa e compreensível quanto possível, assegurando de modo eficaz a compreensão por parte do utilizador das funcionalidades da aplicação e dos limites à sua utilização, de modo a proteger a liberdade individual e os direitos de cidadania.

Relativamente ao direito à informação, acrescente-se, finalmente, que durante o teste Piloto foi realizado um inquérito de satisfação de resposta opcional relativo à experiência como utilizador da STAYWAY COVID, refletindo a preocupação com a transparência do seu funcionamento, a opinião e a informação dos participantes.

Será também mantido um serviço de helpdesk (e-mail e telefone).

5.8. Direitos dos titulares

O Regulamento Europeu de Proteção de Dados assegura aos utilizadores, enquanto titulares de dados pessoais, além do direito de informação, os direitos de acesso, retificação, modificação ou apagamento e oposição ao tratamento. No entanto, atendendo à impossibilidade de o responsável pelo tratamento identificar os utilizadores, neste caso, em princípio, não serão aplicáveis os artigos 15.º a 20.º do Regulamento, em especial os relativos aos direitos de acesso, retificação, limitação do tratamento e portabilidade, em conformidade com o disposto

[31] Mireille Hildebrandt, "The New Imbroglio – Living with Machine Algorithms", in The Art of Ethics in the Information Society, 2016, p. 5. Disponível em https://works.bepress.com/mireille_hildebrandt/75/.

[32] Grupo de trabalho do artigo 29.º, Orientações relativas à transparência na aceção do Regulamento 2016/679, 29 de novembro de 2017, Revistas e adotadas pela última vez em 11 de abril de 2018, página 7.

no n.º 2 do artigo 11.º do mesmo regulamento. Tal deve-se ao facto de as próprias características intrínsecas ao sistema, em particular no que tange às técnicas de pseudonimização usadas.

Já o direito de oposição será facilmente exercido desinstalando a aplicação. Por sua vez esta vai coincidir com o apagamento de todos os dados processados pela aplicação, incluindo os dados armazenados no servidor do sistema.

O titular dos dados pessoais deverá poder exercer os seus direitos bem como solicitar qualquer informação respeitante ao tratamento dos seus dados pessoais mediante solicitação ao responsável pelo tratamento ou ao respetivo encarregado de proteção de dados.

A política de privacidade da aplicação deverá ser clara em matéria de direitos dos titulares e quanto às formas do seu exercício.

Como é sabido o RGPD garante, ainda, ao titular dos dados, nos termos do seu artigo 77.º, o direito de apresentar uma queixa junto de uma autoridade de controlo na União Europeia. Deverá, igualmente ser incluída esta informação nas políticas de privacidade disponibilizadas aos titulares, incluindo a referência à CNPD enquanto a entidade de controlo competente em Portugal.

5.9. Opinião dos titulares de dados sobre o tratamento previsto

A aplicação STAYAWAY COVID tem como finalidade contribuir para um rastreio mais rápido, amplo e eficaz da COVID-19 em Portugal, almejando uma adesão em massa na sociedade portuguesa por forma a maximizar os seus esperados benefícios para a saúde pública.

Em virtude do esperado elevado número de utilizadores e do consequente impacto potencial que uma tal utilização pode acarretar, tanto em termos societais, como no âmbito da proteção de dados pessoais, sem esquecer a dimensão ética presente nas discussões públicas acerca da adoção deste tipo de soluções de rastreio digital, foi incluída nos questionários efetuados no âmbito do projeto de investigação Diários de uma Pandemia[33], organizado pelo Instituto de Saúde Pública da Universidade do Porto e pelo Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência, uma questão dedicada aos sistemas de *contact tracing*.

O RGPD no n.º 9 do artigo 35.º, recomenda, caso seja adequado, a solicitação da opinião dos titulares de dados ou dos seus representantes sobre o tratamento previsto. Tendo em consideração as preocupações enunciadas anteriormente, considerou-se apropriada a realização neste inquérito de uma questão sobre a disponibilidade dos titulares de dados para utilizarem uma aplicação de rastreio, de natureza voluntária e gratuita, capaz de informar sobre a possibilidade de ter estado em contacto com alguém infetado.

O estudo contou com uma amostra de cerca de dez mil pessoas com todas as faixas etárias representadas. Os resultados da pesquisa efetuada estão organizados por escolaridade, região, sexo e grupo etário, permitindo uma melhor análise da disponibilidade dos portugueses para utilizarem a aplicação. Podem ser consultados estes resultados no apêndice do presente documento.

A conclusão que se retira do estudo é que uma parte considerável dos inquiridos (66,9%) utilizaria a aplicação, sendo que 58,5% usariam a aplicação condicionalmente, enquanto 8,4%

[33] Mais informações sobre o projeto de investigação em: https://diariosdeumapandemia.inesctec.pt/.

usariam a aplicação incondicionalmente. Em contraste, um terço dos inquiridos não demonstra grande interesse na aplicação. Aliás, 15,2% afirmam que não vão utilizar a aplicação e 17,9% afirmam que não têm a certeza quanto à utilização da aplicação.

Estes resultados demonstram que existe uma quantidade assinalável de pessoas com interesse na aplicação e que a maior parte dos inquiridos respondeu que a usaria condicionalmente, daqui sobressaindo a importância de um esclarecimento claro e transparente sobre as funcionalidades do sistema e dos tratamentos de dados pessoais efetuados.

Uma conclusão adicional que se retira do estudo é a de que não existe grande discrepância nos números quando estes são observados por escolaridade, região, sexo e grupo etário. Porém, é interessante verificar que o grupo etário dos 0 aos 29 anos é o que possui a maior taxa de possível utilização da aplicação (73,7%), não sendo a diferença significativa para o grupo etário dos 30 aos 39 anos, que tem a menor taxa de utilização (65,1%) do estudo.

Os resultados extraídos dos Diários de uma Pandemia estão em consonância com outros estudos recentes elaborados em países europeus onde a aplicação oficial já se encontra em fase de testes numa parte da população. Na Suíça[34], uma parte significativa da população concorda com a introdução da aplicação (70%) e no Reino Unido[35], seis em cada dez pessoas (62%) afirmam que provavelmente vão fazer o *download* da aplicação após o seu lançamento.

Durante o desenvolvimento da aplicação também existiu um acompanhamento constante das preocupações dos titulares de dados expressas nos diversos meios de comunicação social, as quais foram tidas em conta no momento de implementação de medidas que minimizem os riscos inerentes à adoção desta aplicação.

Durante a fase de testes da aplicação, será dada continuação a este exercício de acompanhamento da experiência de utilização e das opiniões manifestadas pelos primeiros utilizadores da aplicação, de modo a serem identificados problemas técnicos, bem como preocupações relativamente ao tratamento dos dados pessoais.

5.10. Princípio da Proporcionalidade

O tratamento de dados pessoais deverá ser proporcional e adequado às finalidades, artigo 6.º do RGPD. Uma operação de tratamento só é proporcional se sem aquela o objetivo não puder ser alcançado, ou não puder ser alcançado de forma confiável ou apenas com esforço desproporcional, o que exige uma ponderação alicerçada em critérios objetivos, devendo existir uma estreita conexão entre os dados e a finalidade do tratamento.

Por obediência ao princípio da proporcionalidade deverão ser escolhidos, dentro dos diversos meios ou medidas idóneas e congruentes existentes à disposição, aqueles que sejam menos gravosos ou que causem menos danos. Estamos aqui no domínio do princípio da intervenção mínima por forma a que se consiga compatibilizar o interesse público e os direitos dos particulares, de modo a que o princípio da proporcionalidade jogue como um fator de equilíbrio, garantia e controlo dos meios e medidas empregues.

[34] Resultados do estudo na Suíça: https://sotomo.ch/site/wp-content/uploads/2020/05/sotomo_BAG_TracingApp.pdf.

[35] Resultados do estudo no Reino Unido: https://www.health.org.uk/sites/default/files/2020-06/Health-Foundation-polling-contact-tracing-app-May-2020.pdf.

A proporcionalidade terá de se verificar, i) entre o fim da lei e o fim do ato; ii) entre o fim de lei e os meios escolhidos para atingir tal fim; iii) entre as circunstâncias de facto que dão causa ao ato e as medidas tomadas. A proporcionalidade em sentido amplo compreende, em primeiro lugar a congruência, adequação ou idoneidade do meio ou da medida para atingir o fim legalmente proposto, e em segundo lugar, engloba a proporcionalidade em sentido estrito, a proibição de excesso[36].

A matéria de proteção de dados, genericamente, implica, num primeiro momento, uma descrição do conteúdo semântico da informação e de qualquer tratamento que possa ser previsto; num segundo momento, uma descrição da finalidade do tratamento e; num último momento, uma descrição do grau de dependência da prossecução dessa finalidade do tratamento efetivo dos dados pessoais em questão, de uma forma que torne esse grau de dependência objetivamente sustentável e racionalmente discutível.

Em conformidade com o artigo 52.º, n.º 1, da CDFUE, qualquer restrição ao exercício dos direitos e liberdades reconhecidos deve estar prevista na lei, respeitar o conteúdo essencial desses direitos e liberdades, e, em observância do princípio da proporcionalidade, permitir apenas a introdução de restrições se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União ou à necessidade de proteção dos direitos e liberdades de terceiros[37].

O CEPD veio esclarecer as condições e os princípios para a utilização proporcional de dados de localização e meios de rastreio de contactos para dois fins específicos, desde logo prosseguidos de modo claro e transparente pela presente aplicação, "a utilização de dados de localização para apoiar a resposta à pandemia, através da modelização da propagação do vírus de modo a avaliar a eficácia global das medidas de confinamento; o rastreio de contactos, que visa notificar os cidadãos do facto de terem estado na proximidade imediata de alguém que veio a confirmar-se ser portador do vírus, a fim de quebrar as cadeias de contaminação o mais rapidamente possível".[38]

Neste sentido, a necessidade e a proporcionalidade da recolha de dados assentam em fatores como a medida em que as instalações de testagem estão disponíveis, em especial quando já tiverem sido ordenadas medidas como o confinamento[39].

5.10.1. Necessidade

A dimensão da necessidade pressupõe que a medida seja aquela que lese em menor medida os direitos e interesses dos particulares. Deste modo, do ponto de vista do princípio da proporcionalidade a medida necessária é a que corresponder à menos lesiva. A medida julgada adequada em fase anterior é, em seguida, sujeita ao teste da necessidade ou exigibilidade.

36 J.J. GOMES CANOTILHO, *Direito Constitucional e Teoria da Constituição*, Almedina, 7.ª Edição, páginas 315 e seguintes.

37 Ac. Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, The Attorney General, Proc. n.º C-293/12 e C-594/12, de 8 de abril de 2014. (Ponto 38).

38 Diretrizes 4/2020 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19, de 21 de abril de 2020, ponto 5.

39 COMUNICAÇÃO DA COMISSÃO Orientações respeitantes a aplicações móveis de apoio à luta contra a pandemia de COVID-19 na perspetiva da proteção de dados (2020/C 124 I/01), página 6.

A ideia da necessidade esteve na origem do próprio princípio da proporcionalidade, decorrendo do direito do cidadão à menor desvantagem possível – o Estado deve empregar, dentro do possível, as medidas menos lesivas ou onerosas para o cidadão. Esta dimensão visa assim assegurar que os meios empregues são absolutamente necessários à prossecução dos fins.

O juízo da necessidade faz-se, não em termos absolutos, mas em termos relativos, pois pressupõe uma comparação entre uma medida adequada e outras medidas também adequadas. Numa palavra, uma medida será necessária se, em comparação com outras medidas idóneas a atingir o mesmo fim, se revelar a menos lesiva. Por outro lado, será desnecessária se não resistir a esta comparação, chegando-se à conclusão que existiriam outros meios que atingiriam o mesmo fim com menor desvantagem para o cidadão. Pelo que a avaliação da necessidade se afigura mais complexa do que a da adequação. Com efeito, a comparação do grau de lesividade de duas medidas não se basta com critérios empíricos e quantitativos, sendo necessário recorrer a instrumentos de ordem qualitativa que atendam à natureza dos direitos e interesses em causa e, aos bens a sacrificar, devendo ser tidos em conta critérios de ponderação valorativa que permitam optar entre eles[40].

Face ao carácter relativo desta operação, a doutrina avançou critérios densificadores que permitem uma "maior operacionalidade prática". Assim, a máxima da necessidade desdobra-se em quatro requisitos: a necessidade material, que exige que as restrições aos direitos fundamentais sejam mínimas; a necessidade espacial, que limita o âmbito de intervenção da medida; a necessidade temporal, respeitante à delimitação da medida no tempo; e a necessidade pessoal, exigindo que as pessoas afetadas sejam apenas aquelas cujos interesses devem ser efetivamente lesados[41].

A este respeito, a fim de avaliar a proporcionalidade do processamento efetuado, é importante, entre outras coisas, que os dados armazenados nos dispositivos móveis dos utilizadores sejam automaticamente eliminados após 14 dias; os dados dos utilizadores positivos COVID-19 que tenham carregado no *backend* (SLD, SPD) da aplicação sejam igualmente eliminados após 14 dias.

O objetivo de controlar o efeito de contágio da epidemia, controlar a capacidade do sistema nacional de saúde, através da quebra de redes de contágio, implica a restrição de direitos e liberdades. Restrições estas impostas para salvar vidas em situações de emergência - incluindo as aplicadas através da vigilância tecnológica através de dispositivos móveis. Todavia, de modo a assegurar a proporcionalidade da medida implementada através da aplicação, os dados têm de ser destruídos logo que a emergência termine ou que os condicionalismos deixem de ser proporcionais.

5.10.2. Adequação

A avaliação da adequação desenrola-se em territórios estranhos a quaisquer aspetos normativos, recorrendo antes a critérios empíricos e qualitativos. A racionalidade que convoca é, por isso, a do "discurso de referência objetiva" de que nos fala Castanheira Neves[42], com

[40] LAURA NUNES VICENTE, *O Princípio da Proporcionalidade - Uma Nova Abordagem em Tempos de Pluralismo,* Faculdade de Direito da Universidade de Coimbra - Instituto Jurídico, 2014, páginas 28-29.

[41] J. J. GOMES CANOTILHO, *O problema da responsabilidade do Estado por actos lícitos*, Almedina, 1974, página 270.

[42] ANTÓNIO CASTANHEIRA NEVES, *Metodologia Jurídica: Problemas fundamentais*, Coimbra Editora, 2013, página 36: "O discurso, por último, que se mantém numa referência objectiva à realidade, mas em que a realidade é apenas considerada como condição e possibilidade para a consecução de certos fins propostos ou programados, segundo uma relação funcional (função-efeitos) ou o esquema "técnico" (meio-fim), e no qual a validade é a adequação

maior relevo para a sua modalidade técnico-finalística. Esta racionalidade teórica caracteriza-se por uma perspetiva funcional da realidade, que se organiza segundo um esquema técnico meio-fim.

A questão da adequação do tratamento tem, pois, uma dimensão técnica, porque se a tecnologia não puder, de modo algum, servir o propósito, não deve ser utilizada. A componente técnica também deve ser tida em conta, aquando da avaliação da necessidade do tratamento., devendo ser tido em conta o artigo 25.º do RGPD. Isto significa, entre outras coisas, que as tecnologias de ponta devem ser levadas em conta e que o princípio da minimização dos dados deve ser observado.

O tratamento só é adequado para alcançar um objetivo se o equilíbrio específico de interesses for a favor do responsável de tratamento no contexto de uma ponderação de objetivos e meios. Os interesses das pessoas em causa devem, portanto, ser ponderados em relação aos interesses no tratamento dos responsáveis pelo tratamento. Esta ponderação deve também ter em conta os efeitos e "efeitos colaterais" na sociedade como um todo. Estes podem ser questões médicas, mas também sociais, económicas ou psicológicas, que se encontram interligados.

A aplicação reveste um caráter temporário, atuando complementarmente a um outro conjunto de medidas que se encontram a ser implementadas, como a lavagem das mãos ou o distanciamento social. A aplicação, proporcionando o alcance espacial previsto, cruzando os dados dos vários utilizadores, permitirá detetar redes de transmissão, auxiliando na sua quebra, ao emitir alertas que poderão conduzir a alterações de comportamentos, evitando aglomerados de pessoas ou preferindo rotas de circulação menos populosas, por exemplo. Poderia argumentar-se, é certo, que o objetivo poderia, porventura, ser alcançado através da adoção ou reforço das campanhas de sensibilização relativas aos cuidados de higiene individual, cruciais para o combate à epidemia. Todavia, os dados partilhados diariamente, que dão conta da evolução do número de mortes e do número de infetados, demonstram que Portugal, apesar de não ter atingido o pico de contágio, se mantém numa curva de planalto da qual dificilmente está a sair.

Neste sentido, uma medida como a implementação da aplicação poderá ter o efeito mais célere na contenção de comportamentos, pelo impacto que terá, ao ativar em tempo real “lembretes” aos seus utilizadores sobre as potencialidades de contágio. Mais, poderá, inclusive, contribuir para o reforço da adoção das demais medidas, ao conseguir transmitir em tempo real, que a epidemia ainda não se encontra extinta, pelo facto de, a qualquer momento, qualquer cidadão se poder tornar num agente de contágio.

A aplicação ao fornecer orientações aos cidadãos e facilitar a organização do acompanhamento médico dos doentes, pode desempenhar um papel importante na identificação de contactos, na limitação da propagação de doenças e na interrupção das cadeias de transmissão.

Ao nível de direitos fundamentais, estamos, naturalmente diante de condicionalismos quanto ao seu âmbito e amplitude, contudo, não nos esqueçamos que tanto a CRP, como a CDFUE o permitem em casos de emergência de saúde pública como aquele que vivemos, bem como que a aplicação será de utilização estritamente voluntária, podendo ser desinstalada a qualquer momento pelo utilizador. Acresce, que a intrusão em matéria de privacidade se encontra mitigada pela aplicação em análise assentar em prazos de conservação claramente definidos, tendo em conta o seu caráter excecional, limitando-se ao estritamente necessário para produzir o seu efeito de contenção. Mais importa referir, que a aplicação apenas se restringirá aos tempos de exceção em que nos encontramos, não se prolongando além disso, atuando nesta

funcional ou aptidão instrumental e a racionalidade eficiência ou eficácia – é o discurso funcional ou instrumental e de uma racionalidade funcional técnico-finalística”.

medida de acordo com as diretrizes que serão transmitidas pelo responsável pelo tratamento de dados, seguindo aquelas que são as indicações das autoridades de saúde mundiais, europeias e nacionais, devidamente concertadas.

Os direitos fundamentais não são absolutos ou ilimitados. Primeiramente, pelo facto de as normas constitucionais não outorgarem a determinação da extensão da proteção do respetivo direito fundamental ao próprio titular, além do facto de ser inevitável que interesses constitucionalmente garantidos, porém de naturezas opostas, entrem em conflito com determinados direitos. No plano valorativo-constitucional, as Constituições tendem a relacionar os direitos fundamentais a uma noção de responsabilidade social, associando-os ao conjunto de valores comunitários, como, por exemplo, a segurança pública, a autoridade do Estado, etc. Assim, percebe-se que, além dos limites internos (aqueles que resultam das situações de choque entre os diferentes direitos fundamentais) também podem existir limites externos, que buscam harmonizar os interesses individuais com as imposições próprias da convivência em comunidade. As restrições aos direitos fundamentais são uma redução da extensão de determinado direito fundamental, para que assim se possa conviver harmoniosamente com outras garantias constitucionais, sejam individuais ou referentes aos valores da vida em sociedade, como emergências de saúde pública.

A utilização adequada de dados pseudonimizados a fim de melhor e mais rapidamente responder à forma como o vírus se propagará e a mitigação dos efeitos económicos da crise; a aplicação de salvaguardas para evitar a reidentificação de pessoas, incluindo garantias quanto ao nível suficiente de segurança dos dados e da infraestrutura informática, e avaliação dos riscos de reidentificação no caso de os dados serem correlacionados com outros dados; a eliminação imediata e irreversível de todos os dados acidentalmente tratados que possam conduzir à identificação de pessoas e a comunicação aos fornecedores dos dados, bem como às autoridades competentes, do tratamento e da eliminação acidentais; a eliminação dos dados o mais tardar quando a pandemia for declarada sob controlo, e a restrição do tratamento dos dados exclusivamente para as finalidades descritas contribuem para a mitigação das limitações no exercício de direitos à vida privada e intimidade.

5.10.3. Análise custo-benefício[43]

Neste campo, o jogo do princípio da proporcionalidade já não se fará, por isso, entre meios e fins, mas sim entre bens, interesses e valores. Antes se fazendo uma análise comparativa entre os custos (por exemplo, oneração de direitos, eventuais inconvenientes de ordem social, afetação de outros interesses públicos) e os benefícios (vantagens) para os interesses públicos e privados em causa resultantes da medida. Se o custo (leia-se o sacrifício de certos bens, interesses ou valores) estiver numa proporção aceitável com o benefício (leia-se a satisfação de certos bens, interesses ou valores), então a medida é proporcional em sentido estrito. O instrumento francês do *bilan coût-avantages* traduz também essa ideia.

As principais ameaças à privacidade deste tipo de solução advêm do mapeamento das relações entre as pessoas, da reidentificação por localização implícita, das fragilidades dos protocolos na construção de tokens pseudoanónimos e da dispersão dos sinais de infeção para que a identidade das pessoas infetadas nunca seja identificada. O tratamento da informação poderá não afetar apenas o utilizador, mas também os terceiros com quem aquele tenha estado em

[43] KAI MÖLLER, «Proportionality: Challenging the critics», *in International Journal of Constitutional Law*, vol. 10, n.º 3 (2012), pp. 709-731.

contacto. Efetivamente existem estudos[44] que demonstram que a robustez da criptografia e protocolos de anonimização pode sempre ser quebrada mediante a aplicação do tempo e esforços necessários nesse sentido, ainda que ultrapassem largamente o limite da razoabilidade em muitos casos. Não existem, por certo, soluções cem por cento seguras.

Mais uma vez, há que salientar que as soluções técnicas não podem ser consideradas isoladamente, antes se alicerçando o seu sucesso em muitos outros fatores. Desde logo, a necessidade de ser encarada como uma medida complementar às demais veiculadas pela OMS, pela DGS, como a lavagem das mãos, por exemplo. Ademais, alguns estudos[45] falam da importância da adesão da população, que segundo alguns, deveria mesmo rondar uma fasquia de 60%, difícil de atingir, já que representaria a quase totalidade de utilizadores de telemóveis. Este argumento vem, no entanto, sendo infirmado por outros estudos, de sentido contrário apontando os assinaláveis méritos da solução ainda que com taxas de adesão muito mais modestas, retirando da sua utilização sempre um efeito positivo, muito embora reconheçam a relevância de garantir concomitantemente um maior acesso à realização de testes, por se revelarem essenciais do ponto de vista individual, evitando que determinado utilizador se torne numa fonte de contágio[46]. Do ponto de vista societal, permitirá a atualização da informação periódica sobre a evolução da epidemia num determinado lapso temporal. A aplicação só poderá gravar contacto mediante prévia instalação e ativação de Bluetooth, centrando-se a utilização da aplicação na disponibilidade das partes, enquanto manifestação do seu caráter voluntário.

A aplicação, sendo de alerta e rastreio, revela-se útil para o país para efeitos de identificação de contactos e pode desempenhar um papel importante de contenção durante os cenários de inversão da escalada do confinamento. As aplicações de rastreio de contactos de proximidade não substituem a intervenção das demais medidas promovidas pela autoridade de saúde pública. Uma aplicação baseada na proximidade da localização de contactos com COVID-19 não pode ajudar substancialmente, se utilizada isoladamente das demais medidas, sobretudo, numa altura como a atual, em que a transmissão é feita comunitariamente, procurando as pessoas, apesar do desconfinamento gradual, o refúgio de sua casa, sempre que possível. Num universo de tantas pessoas infetadas, grande parte das quais assintomáticas, uma aplicação de proximidade não será capaz de, isoladamente, alertar para a maioria dos riscos de infeção, revelando-se nesta sede, crucial, a disponibilização e realização rápida de testes.

A utilização da aplicação pode também constituir um instrumento valioso para os cidadãos exercerem um distanciamento social efetivo e orientado. O seu impacto pode ser multiplicado por uma estratégia de apoio baseada na realização mais generalizada de testes.

A utilização de dados de proximidade e a desnecessidade do tratamento de dados sobre a localização ou os movimentos de pessoas, bem como a utilização de dados pseudonimizados e agregados, além da utilização de tecnologias adequadas, como é o caso do recurso ao Bluetooth de baixo consumo para estabelecer a proximidade dos dispositivos, a encriptação, a segurança dos dados, o armazenamento dos dados sobre o dispositivo móvel permitem mitigar os efeitos nocivos no que à matéria de privacidade e confidencialidade concerne.

---

[44] https://github.com/DP3T/documents/blob/master/DP3T%20-%20Upload%20Authorisation%20Analysis%20and%20Guidelines.pdf.

45 FERRETI, Luca; WYMANT, Chris Wymant; KENDALL, Michelle; ZHAO, Lele; NURTAY Anel; ABELER-DORNER, Lucie; PARKER, Michael; BONSALL, David; FRASER, Christophe, «Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing», in Science, Vol. 368, n.º 6491, American Association for the Advancement of Science, 2020.

[46] Cfr. https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown.

Qualquer aplicação de proximidade cria novos riscos para os utilizadores da tecnologia. Um registo da proximidade de um utilizador com outros utilizadores poderia ser utilizado para demonstrar com quem poderia estar a estabelecer contacto, podendo o receio da divulgação de tal informação de proximidade, demover os utilizadores de a utilizarem em espaços públicos ou com grande afluência. Todavia, algumas tecnologias comummente utilizadas criam riscos semelhantes ou superiores, mantendo um registo de todos os locais frequentados. Convém reforçar que o simples transporte de um telemóvel acarreta o risco de rastreio através da triangulação da torre do telemóvel.

A proposta da presente aplicação de proximidade não acarreta riscos novos, não sendo o risco tão elevado como muitas das aplicações utilizadas diariamente, assentes em geolocalização e não em tecnologia Bluetooth. O contexto é, naturalmente, importante. Estamos perante uma epidemia sem precedentes. A existência de salvaguardas suficientes ajuda a mitigar este risco. A transparência sobre a finalidade e as funcionalidades da aplicação, assim como a publicação do código fonte auxiliam na mitigação dos riscos por informarem os utilizadores, de modo claro e direto.

Avaliação EPD

A ponderação acima tratada afigura-se forçosamente complexa, especialmente perante contextos de reconhecida excecionalidade como aquele que atravessamos, em que frequentemente se recorre a novas utilizações de meios tecnológicos existentes em busca de benefícios difíceis de garantir, à partida, com absoluta certeza. É porém, inquestionável, a relevância social dos benefícios em causa, especialmente quando integrados, adequadamente, numa estratégia global de natureza sanitária cuja eficiência se pretende maximizar. Naturalmente, tal objetivo não deve resultar num relaxamento da exigência na avaliação e mitigação dos riscos envolvidos, pelo contrário solicitando um maior e continuado esforço de monitorização e acompanhamento da implementação das medidas adotadas, impedindo a adesão imponderada a um solucionismo tecnológico que sempre será de evitar.

A este propósito realce-se a planeada funcionalidade de *Remote Switch* referente à possibilidade de suspensão provisória e posterior reativação do funcionamento do sistema (em particular da recolha e disseminação de códigos) segundo determinação do Governo, autoridades de saúde ou de controlo em matéria de proteção de dados. Esta funcionalidade permitiria a avaliação regular e contextualizada da necessidade, adequação e justa medida da manutenção do sistema ativo, por parte das autoridades competentes, em função da evolução da epidemia, acrescendo à prevista descontinuação, aquando do fim da pandemia.

Ao nível do subprincípio da necessidade salienta-se a patente preocupação com a minimização dos dados refletida não apenas na opção por um sistema de pendor semidescentralizado ou distribuído, cujos principais méritos, reconhecidamente, se relacionam, precisamente, com aquela dimensão, mas também na informação recolhida e conservada pelo sistema conforme descrito na secção 2. Com efeito, no que concerne ao cálculo do risco de contágio, são seguidas as diretrizes atuais da Organização Mundial de Saúde, sendo unicamente avaliada e automaticamente extraída a informação atinente à existência de contactos a menos de 2 metros e por mais de 15 minutos. Por outro lado, conforme acima assinalado, as Chaves de Identificadores TEK e os Identificadores Aleatórios RPI são automaticamente apagados do DMP 14 dias após terem sido armazenados.

Acresce a ausência de recolha de meta-dados com informação epidemiológica complementar como, por exemplo, a referente a região de domicílio ou ao número de contactos, ou quaisquer

dados adicionais sobre a exposição a contágio que poderiam ser relevantes para fins de análise estatística. Num cotejo simples com sistemas de natureza similar propostos ou a operar no espaço europeu, diremos que, neste particular, a solução STAYAWAY COVID privilegiou o princípio da minimização de dados em detrimento de outros objetivos, ainda que louváveis, como seriam o do aperfeiçoamento dos algoritmos ou um conhecimento mais profundo dos fenómenos associados à propagação da doença.

No que concerne ao princípio da voluntariedade que preside à utilização do sistema, idealmente, será possível ao utilizador não apenas desinstalar a aplicação mas também controlar o desempenho da funcionalidade Bluetooth podendo, designadamente, desativar temporariamente o Bluetooth no seu dispositivo após ter descarregado a aplicação que nele assenta. Esta possibilidade permitirá, do mesmo passo, contrabalançar algumas das vulnerabilidades inerentes a um sistema deste tipo, nomeadamente, o desafio colocado pelo contexto das relações de vizinhança de grande proximidade, permitindo aos utilizadores instruídos alguma defesa perante o risco potencial de deteção de casos positivos em vizinhos. A mesma lógica se aplicará, *mutatis mutandis*, ao caso dos falsos positivos em profissionais de saúde ou outros, cuja exposição real ao risco seja menor (fruto da adoção de especiais medidas) do que aquela sugerida pelo algoritmo subjacente à funcionalidade de notificação.

Aceitável	☐	Aceitável com recomendações	☒	Inaceitável	☐

6. Análise de riscos e vulnerabilidades

Na presente secção é feita uma análise de risco, cruzando diferentes metodologias e linhas de abordagem, por forma a melhor abarcar o leque de cenários de risco possíveis. Parte-se de uma análise geral das principais vulnerabilidades identificadas e das possíveis medidas mitigadoras de riscos, para, seguidamente, ser feita uma análise crítica das medidas já implementadas, terminando com uma avaliação à luz das clássicas noções da tríade CIA.

6.1 Identificação e análise de riscos e medidas de mitigação

Os inegáveis méritos do modelo de gestão descentralizada de dados em que se baseia o STAYAWAY COVID são acompanhados por certas vulnerabilidades que lhe são intrínsecas e que importa considerar a fim de adotar as adequadas medidas de mitigação de riscos relacionadas, essencialmente, com a possível reidentificação dos utilizadores que hajam sido diagnosticados com COVID-19.

Os Identificadores Aleatórios RPI (*Rolling Proximity Identifier*) são obtidos com recurso a técnicas criptográficas que utilizam a capacidade interna de cálculo do dispositivo móvel pessoal. Tratam-se de pseudónimos temporários de curta duração, que não contêm qualquer informação diretamente referenciável, seja ao utilizador, seja ao dispositivo que os gera. Tão-pouco será possível associá-los a outros identificadores técnicos do DMP, como os endereços MAC das interfaces de rede WiFi e Bluetooth, os códigos IMEI das interfaces GSM ou os números de telefone.

Os Identificadores Aleatórios RPI são gerados aproximadamente a cada quinze minutos a partir de uma chave de 128 bits de médio prazo - Chave de Identificadores TEK (*Temporary Exposure Key*). Esta última é gerada aquando da primeira utilização da aplicação, sendo, a partir de então, regenerada diariamente utilizando um gerador criptográfico pseudoaleatório. A partir de cada Chave de Identificadores TEK é possível, matematicamente, obter até 144 Identificadores Aleatórios RPI. A função utilizada não permite calcular as Chave de Identificadores TEK a partir dos Identificadores Aleatórios RPI. Quando um utilizador é diagnosticado com COVID-19, submete voluntariamente as suas Chaves de Identificadores TEK ao SPD (Chaves de Identificadores TEK até aos 14 dias anteriores).

Para minimizar o risco de rastreio e reidentificação, o sistema GAEN recorre à utilização do Bluetooth LE Privacy, disponível desde a versão 4.2[47] do BlueTooth. O Bluetooth LE Privacy permite a utilização de endereços MAC aleatórios temporários (com duração de cerca de 15 minutos), o que limita eventuais cenários de reidentificação recorrendo a outras fontes de informação à duração do endereço MAC temporário. A difusão de dados Bluetooth em iOS ou Android é sempre efetuada através do sistema operativo, seja utilizada a API GAEN ou outra qualquer interface mais elementar, pelo que não será, portanto, impossível à Google e Apple, na implementação dos sistemas operativos, seguir as cadeias de RPI. Ao nível da aplicação não é possível, no entanto, detetar ou evitar que tal aconteça.

Acresce a ausência de recolha de meta-dados com informação epidemiológica complementar como, por exemplo, a referente à região de domicílio ou ao número de contactos, ou quaisquer dados adicionais sobre a exposição a contágio que poderiam ser relevantes para fins de análise

[47] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13702.

estatística. Num cotejo simples com sistemas de natureza similar propostos ou a operar no espaço europeu, diremos que, neste particular, a solução STAYAWAY COVID privilegiou o princípio da minimização de dados em detrimento de outros objetivos, ainda que louváveis, como seriam o do aperfeiçoamento dos algoritmos ou um conhecimento mais profundo dos fenómenos associados à propagação da doença.

6.1.1. Sistema de Notificação de Exposição Google-Apple (GAEN API)

A conceção do sistema STAYAWAY COVID foi iniciada antes da disponibilização da interface de Notificação de Exposição Google-Apple (GAEN API), tendo, entretanto, sido adaptado para a utilização das novas funcionalidades que esta permite.

O protocolo implementado pela GAEN API é muito próximo do protocolo DP^3T. Contudo, ao contrário deste último, o protocolo de geração de chaves, a divulgação de pseudónimos entre dispositivos móveis e a gestão das chaves/identificadores no dispositivo móvel deixaram de ser implementadas pela aplicação e passaram a ocorrer ao nível do sistema operativo (Android e iOS). A Google e a Apple disponibilizam a especificação do protocolo, algoritmos e respetiva API, contudo, ao contrário do DP^3T, o código da GAEN API não é aberto.

De acordo com a GAEN, apenas uma aplicação por país e endossada oficialmente está autorizada a aceder à API. Esta limitação visa impedir o acesso aos dados locais nos dispositivos por outras aplicações, que poderiam explorar esse acesso para fins ilegítimos, tais como alimentar uma base de dados central com as chaves e identificadores dos utilizadores.

Poderemos sempre colocar um cenário em que, na hipótese de ser tecnicamente possível aos fabricantes usar os dados guardados para outras finalidades, estes tentassem cruzar os RPI trocados pelos dispositivos e, em conjunto com outras base de dados existentes, procurar estimar percursos/contactos. É importante, porém, salientar que, perante este cenário, mesmo que fosse seguida outra abordagem em que o código que implementa as funcionalidades da GAEN fosse aberto, os fabricantes continuariam a ter acesso a esses dados. Além do mais, em bom rigor, do ponto de vista do incentivo, os fabricantes não careceriam daqueles dados para um propósito de reidentificação por se tratarem de dados a que já teriam acesso por outras vias. Do ponto de vista técnico, os fabricantes poderiam ter acesso ilegítimo a outras fontes de dados que lhes poderiam, igualmente, dar acesso a trajetos/relações dos utilizadores. Estes factos não devem, nem podem, contudo, ser vistos como legitimação da exploração dessas fontes de dados pelos fabricantes.

É expectável, de resto, uma atenção redobrada pela comunidade à forma como a GAEN API trata os dados. Por exemplo, apesar do código ser fechado, há padrões de tráfego que podem ser monitorizados nos seus próprios dispositivos (ver com quem comunicam, quando e quais as características do tráfego) pela comunidade das áreas académicas e de segurança. De notar que, sendo os sistemas operativos fechados, este tipo de escrutínio já tem vindo a ser feito pela comunidade.

Nota de atualização - versão 2 da AIPD:

As considerações proferidas no anterior AIPD ao sistema STAYAWAY sobre os riscos de utilização do GAEN mantêm-se, uma vez que não foram divulgadas novas informações ou revelações sobre implementações no protocolo que minimizem ou elevem o nível de risco de reidentificação dos titulares de dados por parte da Google ou da Apple.

No entanto regista-se como muito positivo o facto de ter sido, entretanto, publicada parte do código fonte anteriormente desconhecida (disponível no github na hiperligação https://github.com/google/exposure-notifications-internals), por conta da Google. Este facto favorece, certamente, o escrutínio publico do sistema e representa um ganho acrescido de transparência. Ainda assim, volta-se a frisar, a importância de as comunidades das áreas académicas e de segurança para o escrutínio da forma como a GAEN API trata os dados, além da análise técnica conduzida pelo CNCS no caso específico da STAYAWAY COVID.

6.1.2. Reidentificação recorrendo a sistemas externos

A garantia de confidencialidade dos dados respeitantes aos utilizadores diagnosticados com COVID-19 é confiada à tecnologia e à capacidade de minimizar as ocasiões em que os Identificadores Aleatórios RPI, de curto prazo, divulgados através da tecnologia sem fios Bluetooth Low Energy (BLE), possam ser captados por elementos estranhos ao sistema STAYAWAY COVID, e explorados em combinação com a aquisição de outros identificadores por via do recurso a sistemas externos. Neste cenário, os RPI captados poderiam comparar-se com os RPI calculados a partir das Chave de Identificadores TEK, dos utilizadores diagnosticados com COVID-19, disponibilizados pelo SPD. Poderá colocar-se o cenário de haver dispositivos físicos especializados com a capacidade para captar, através de software de *scanning* de rede (*sniffers*), a difusão dos pseudónimos RPI a uma distância superior, permitindo captar pseudónimos RPI transmitidos numa área superior recorrendo a um menor número de "pontos de escuta" ocultos.

Noutra vertente, poder-se-á, ainda, afirmar que os sistemas descentralizados, quando implicam a difusão de pseudónimos de indivíduos diagnosticados com COVID-19, poderão em certas condições colocá-los à mercê de um tipo de ataque conhecido por ataque *Paparazzi*[48]. Este consiste em captar os Identificadores Anónimos RPI dos dispositivos móveis de sujeitos cuja identidade é conhecida ou possa ser facilmente conhecida, nomeadamente, através da captação dos Identificadores Anónimos RPI perto do local de residência ou de trabalho da pessoa que é alvo de uma atenção específica. O mesmo se aplica, naturalmente, e de forma genérica, a qualquer localização espacial onde uma identificação pessoal possa ser associada à emissão do Identificador Anónimo RPI. Podemos conjeturar que estes casos possam mais facilmente ter lugar em estabelecimentos comerciais no contexto do pagamento através da utilização de cartão de crédito, servindo igualmente de exemplo, a passagem por portões de embarque controlados nos aeroportos, ou os locais de trabalho onde existem sistemas de deteção de presença ou sistemas de monitorização do tráfego rodoviário com recurso a sistemas de gravação vídeo. Através desta recolha de dados e do subsequente *labelling*, pretender-se-ia gerar, assim, uma base de dados de Identificadores Aleatórios RPI relativos a uma ou várias pessoas singulares cujo estado de saúde seja uma informação com um especial interesse ou relevo (um ativo com valor financeiro ou de outro tipo) para, então, nela buscar possíveis correspondências com os pseudónimos tornados públicos pelo sistema de notificação de exposição.

Relativamente a sistemas descentralizados como o STAYAWAY COVID, poderá ser dito que a divulgação das Chaves de Identificador TEK dos titulares diagnosticados com COVID-19, aliada à publicação do código fonte da aplicação e dos algoritmos criptográficos utilizados, permite a derivação dos RPIs associados às TEK dos utilizadores diagnosticados com COVID-19 por

[48] VAUDENA, Serge Vaudenay, Analysis of DP3T - Between Scylla and Charybdis, IACR-EPRINT, 2020. Disponível em https://eprint.iacr.org/2020/399.pdf.

sistemas externos. O que, associado a bases de dados externas ilegítimas, referidas supra, poderiam intentar a reidentificação desses utilizadores. Contudo, é importante ressalvar que a disponibilização de código aberto e dos algoritmos permite o escrutínio pela comunidade e uma maior aposta na qualidade das abordagens, algoritmos e código. Por esta razão, o consenso na comunidade científica é de que os méritos da transparência compensam largamente, a este título, os inconvenientes aliados à opção pela disponibilização dos programas em código aberto. Por outro lado, como se discute em 6.1.1, a disponibilização do código fonte não é integral, no caso da GAEN API.

A limitação do acesso à API GAEN a uma aplicação por país, endossada oficialmente, juntamente com o isolamento da aplicação no sistema operativo (*sandboxing*), permite reduzir consideravelmente o risco de ação de software ilegítimo ou qualquer outra aplicação aparentemente inofensiva que possa ter um comportamento malicioso (com ou sem o conhecimento do utilizador), que de outra forma poderia adquirir, por exemplo, os mesmos dados utilizados pela aplicação STAYAWAY COVID e transmitindo-os depois para o exterior, alimentando assim coleções em grande escala de pseudónimos RPI que permitiriam a procura de combinações úteis para reconstruir, por exemplo, movimentos de pessoas ou para identificar os pseudónimos de sujeitos diagnosticados com COVID-19. Ainda assim, os utilizadores devem ser aconselhados a seguir boas práticas de Higiene e Segurança informática para evitar a instalação de software ilegítimo ou com comportamento malicioso.

Como fatores mitigadores deste risco específico, considera-se ainda, e em geral[49], a pouca utilidade do ataque e a falta de motivação, sem prejuízo da possibilidade de tais ataques, mesmo sem interesse utilitário, poderem ocorrer com o mero objetivo de criar perturbação, protestar ou adquirir informações sobre o estado de saúde de indivíduos relativamente aos quais o conhecimento de tais informações assume um valor de per se, pelas seus eventuais implicações ou benefícios (financeiros ou de outra ordem) para quem os promove.

Considere-se, ainda, e sempre que qualquer aquisição oculta e utilização subsequente de dados nos cenários aqui referidos, prefigurando ataques externos e maliciosos ao sistema STAYAWAY COVID, constituiriam uma conduta ilícita e seguramente merecedora de perseguição pelo sistema de justiça.

6.1.3. Reidentificação por inferência

Em boa verdade, o risco de reidentificação por inferência de utilizadores diagnosticados com COVID-19, e que submetem as suas Chaves de Identificadores TEK ao SPD, não está inerentemente ligado à utilização do sistema, verificando-se independentemente do uso deste. Ou seja, cada utilizador que receba um alerta de exposição ao risco, da mesma forma que todos aqueles que - fora do contexto da utilização da tecnologia - receberem um diagnóstico positivo, procurarão, naturalmente, levar a cabo uma reconstrução dos contactos passados com outras pessoas, a fim de, eventualmente, relacionarem alguma ou algumas destas pessoas singulares à exposição ao risco de infeção ou ao estado da doença através de uma análise retrospetiva, dos

[49] Sobre os riscos e méritos inerentes à arquitetura dos sistemas distribuídos valem, genericamente as observações feitas a este título noutras avaliações de impacto (ou em pareceres e deliberações de autoridades de controlo) conduzidas recentemente noutros Estados Membros da UE com base em sistemas de natureza similar, sem prejuízo das idiossincrasias que também apresentam. Com particular pertinência citem-se os casos da Corona-Warn-App (https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf), Immuni (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9357972) e STOPP CORONA (https://www.roteskreuz.at/fileadmin/user_upload/Bericht_Datenschutzfolgeabschaetzung_StoppCorona_App.pdf)

contactos mais prolongados que tenham tido na janela temporal configurada pela aplicação (que é de 14 dias).

Reconheça-se que em certos casos será relativamente fácil ou mesmo muito provável estabelecer uma tal relação. Para tanto há-de contribuir, por sinal, o especial interesse que será de esperar, da parte dos utilizadores (pelo menos de alguns destes), naquele exercício de memória visando uma tentativa de reidentificação, mas dependendo, igualmente, do perfeito conhecimento dos seus movimentos mais recentes e do contexto em que o contacto ocorreu. Este exercício não depende, efetivamente, da existência de ferramentas tecnológicas sofisticadas destinadas a permitir a reidentificação de contactos. Por outro lado, impõe-se referir que as possibilidades de reidentificação (por inferência) verificar-se-iam em qualquer sistema, seja este centralizado ou distribuído, constituindo, portanto, numa vulnerabilidade que poderá ser considerada intrínseca à própria finalidade da notificação de exposição que é assignada ao sistema.

Nesta ótica, e em suma, verifica-se que qualquer solução de notificação de exposição é potencialmente vulnerável, em casos específicos significativamente vulnerável, a ataques de reidentificação por inferência. Por outro lado, as soluções de cariz descentralizado serão potencialmente mais expostas ao risco de ataques baseados na correspondência.

6.1.4. Falsos alertas por reencaminhamento de RPIs ilegítimos

Um risco que também tem sido discutido na comunidade académica, tem sido a possibilidade de serem reencaminhados Identificadores Aleatórios RPI de utilizadores diagnosticados com COVID-19 com o objetivo de criar falsos alarmes[50]. De momento não há uma solução que impeça ou mitigue esta vulnerabilidade sem, simultaneamente, comprometer a segurança ou privacidade dos utilizadores por outras vias.

O risco apresenta-se, no entanto, como pouco provável, ainda que o impacto de alguns ataques que explorassem esta vulnerabilidade pudessem, eventualmente, ser relevantes.

Visto que a troca e validação dos Identificadores Aleatórios RPI é feito ao nível da GAEN, eventuais contramedidas para mitigar este risco terão de ser implementadas pelos fabricantes (Google e Apple). Contudo, recomenda-se que sejam sistematicamente estudadas outras formas de mitigação que possam ser implementadas ao nível do sistema, mais concretamente ao nível da aplicação e do SPD, por forma a mitigar o impacto de eventuais ataques, ainda que remotos.

6.1.5. Armazenamento de dados de tráfego IP

O armazenamento dos endereços IP dos clientes pode levar a identificação por associação dos dispositivos móveis que se ligam aos servidores. Ainda que os endereços IP não possam ser associados às Chave de Identificadores TEK ou aos Identificadores Aleatórios RPI, é fundamental que os tempos de retenção dos endereços IP, ou outro identificador diretamente associado ao dispositivo móvel, devam ser limitados ao estritamente necessário para a deteção de anomalias

[50] BAUMGARTNER, Lars, et al., «Mind the GAP: Security & Privacy Risks of Contact Tracing Apps». Disponível em https://arxiv.org/abs/2006.05914.

e ciberataques, limitados ao curto prazo, e que só possam ser acedidos pelos administradores de sistema no estrito âmbito das suas tarefas.

No caso do SPD, não está previsto o armazenamento de endereços IP ou outro identificador diretamente associado ao dispositivo móvel. No caso do SLD, o endereço IP é armazenado durante um curto período pela infraestrutura de perímetro com o único objetivo de garantir a segurança informática, nomeadamente contra ataques DDoS (*Distributed Denial of Service*).

6.2. Medidas adicionais de mitigação de riscos

Algumas medidas mitigadoras e melhorias técnicas adicionais planeadas:

- O utilizador deve ser adequadamente avisado dos cuidados especiais a ter com a segurança do seu dispositivo móvel.
- Deve ser feito o acompanhamento dos acessos efetuados aos sistemas e bases de dados pelos administradores dos sistemas, com um período adequado de retenção dos registos.
- Devem ser utilizados sistemas de segurança perimetrais para mitigar ataques destinados a explorar vulnerabilidades conhecidas, associadas tanto ao software de base como ao código desenvolvido para o Sistema STAYAWAY COVID.

Controlo de acesso aos dados

- Os controlos previstos em relação aos dados armazenados na componente central da infraestrutura parecem inspirar-se na disposição geral do fiador relativa aos administradores de sistemas. Por conseguinte, as medidas de auditoria e de recolha de registos devem ser alargadas às operações efetuadas sobre os dados por todos os operadores que irão intervir no seu tratamento no *backend*, e não apenas nos acessos (eventos de autenticação informática), a partir da fase delicada de recolha de informações sobre casos positivos.

Duração da conservação dos dados

- Com base no sistema previsto para a deteção de anomalias e ciberataques, os logs que contenham endereços IP ou outro identificador diretamente associado ao dispositivo móvel, não deverão ser guardados por um período superior a uma hora.
- Os backups do SPD, que inclui as Chaves de Identificadores TEK submetidas pelos utilizadores, não deverão ser guardados por um período superior a três dias. Sendo o eventual acesso aos backups feito por administradores de sistemas autorizados e com a única finalidade de reposição do servidor SPD em caso de problemas.

Funcionalidade de *Remote Switch*

- A planeada funcionalidade de *Remote Switch* refere-se à possibilidade de suspensão provisória e posterior reativação do funcionamento do sistema (em particular da recolha e disseminação de códigos) segundo determinação do Governo, autoridades de saúde ou de controlo em matéria de proteção de dados. Esta funcionalidade permitiria a avaliação regular e contextualizada da necessidade, adequação e justa medida da

manutenção do sistema ativo, por parte das autoridades competentes, em função da evolução da epidemia, acrescendo à possibilidade existente de descontinuação definitiva, supra mencionada, coincidente com o anúncio do fim da pandemia. De acordo com o plano, esta funcionalidade, consentânea com o cumprimento das obrigações de assegurar a proteção de dados desde a conceção e por omissão, seria preferencialmente implementada conforme se descreve seguidamente:

- A aplicação obtém diariamente do SPD informação de configuração que usa para garantir o cumprimento dos seus objetivos (i.e., os pesos usados na tradução dos sinais recebidos para o critério de proximidade).
- Esta configuração é datada e assinada, de forma a evitar a repetição de configurações passadas.
- Como parte de informação de configuração e, opcionalmente com base na versão da aplicação que faz o pedido, pode ser recebida pela aplicação a indicação que a aplicação precisa de ser atualizada.
- Neste caso, a aplicação desliga a recolha e disseminação de RPIs, com uma indicação que deve ser feita uma atualização através do sistema através da Play Store ou Apple Store.
    - Esta medida serve, em primeiro lugar, para mitigar problemas que sejam descobertos em produção, permitindo retirar rapidamente de circulação versões especificas da aplicação onde sejam reveladas eventuais vulnerabilidades.
    - Em segundo lugar, serve para a descontinuação definitiva, em que a atualização forçada substitui a aplicação por uma versão desativada, que se limita a informar o cidadão desse facto.
- No caso de não conseguir obter a informação de configuração depois de algumas tentativas, a aplicação desliga também a recolha e disseminação de códigos, com uma indicação que deve ser feita uma ligação à Internet.
- No caso de não conseguir realizar essa operação durante um determinado número de dias seguidos, a aplicação desliga a recolha e disseminação de RPIs, com uma indicação que deve ser feita uma ligação à Internet.
- A disseminação e recolha de RPIs é reposta automaticamente logo que nova configuração seja obtida com sucesso.
- No caso de uma aplicação recém instalada ou reiniciada, só se dá inicio à disseminação e recolha de RPIs depois de obtenção com sucesso de uma nova configuração.
- Em obediência ao princípio da transparência e lealdade do tratamento, os utilizadores são informados da existência desta funcionalidade através das políticas de privacidade (website, App) e informação fornecida aquando da instalação da aplicação, bem como das campanhas de informação sobre o uso do sistema, e deverão ser, igualmente, informados sempre que as autoridades competentes decidirem recorrer a este recurso.

Conclusões

Em última análise, a solução STAYAWAY COVID é uma implementação de um sistema de notificação da exposição baseado num modelo de dados distribuídos, e numa arquitetura semidescentralizada em que as funcionalidades centrais estão relacionadas com a submissão das Chaves de Identificadores TEK dos utilizadores diagnosticados com COVID-19 e com a disseminação dos respetivos pseudónimos.

As questões críticas analisadas podem ser abordadas com medidas técnicas e organizacionais adequadas, cuja adoção e eficácia terão de ser verificadas durante o funcionamento do sistema, havendo ainda alguns aspetos de risco potencial decorrentes das características intrínsecas do modelo de dados distribuídos e da arquitetura descentralizada, e não da especificidade do sistema tecnológico existente (reidentificação de utilizadores diagnosticados com COVID-19 através da procura de pseudónimos, na sequência de ataques *paparazzi*), comuns a todas as experiências de rastreio de contactos para combater a pandemia com base no mesmo modelo descentralizado que está a ser realizado em diferentes países.

6.3. Medidas de cibersegurança implementadas no sistema STAYAWAY COVID

Análise de ameaças tendo como base as orientações da ENISA para as aplicações móveis COVID-19[51].

Alvo	**Ameaças**	**Medidas (mitigação da ameaça)**
Utilizador	O utilizador é falsificado por um atacante	Autenticação do utilizador do DMP
	Ação do utilizador é repudiada	Autenticação do utilizador do DMP
Dados da aplicação	Adulteração de dados locais	Proteção dos dados locais do acesso externo à aplicação.
	Exfiltração de dados locais	Proteção dos dados locais do acesso externo à aplicação.
	Recusa de acesso aos dados locais pela aplicação	N/A
Aplicação no DMP	A aplicação é falsificada	Apenas aplicações endossadas pelo Governo têm acesso à API GAEN indispensável ao funcionamento do sistema
	A aplicação é adulterada pelo atacante	Apenas aplicações endossadas pelo Governo têm acesso à API GAEN indispensável ao funcionamento do sistema
	A ação da aplicação é repudiada	Autenticação o utilizador do DMP
	Exfiltração de dados da aplicação	Minimização de dados expostos pela API GAEN. Limitação da comunicação externa aos dois servidores oficiais (SLD e SPD) e via sistema operativo.
	A aplicação saturada por acessos externos (DoS)	N/A
	A aplicação é explorada para obter maiores privilégios de acesso	Utilização de ambientes de execução isolados (*sandboxes*)
Comunicação entre DMP e servidores *backend* (SLD e SPD)	O tráfego é adulterado	Uso de protocolos de comunicação seguros (sobre TLS)
	O tráfego é intercetado	Uso de protocolos de comunicação seguros (sobre TLS)
	A ligação é saturada	Uso de interfaces resistentes a tentativas de negação de serviço (DoS)
Aplicações nos servidores *backend* (SLD e SPD)	A aplicação é falsificada	Uso de TLS e certificados de autenticidade
	A aplicação é comprometida	Minimização dos dados no servidor, minimização do valor dos dados, salvaguarda de dados
	A ação do servidor é repudiada	Uso de registos de ações críticas
	Exfiltração de dados da aplicação	Minimização dos dados no servidor, minimização do valor dos dados, controlo de acessos
	A aplicação é saturada	Separação de servidor de escrita e leitura. Replicação dos servidores.

[51] EUROPEAN UNION AGENCY FOR CYBERSECURITY, "COVID-19 apps - cybersecurity requirements and testing", página 19-21.

	A aplicação é explorada para obter maiores privilégios de acesso	Minimização da interface externa, controlo de acessos.
Dados nos servidores *backend* (SLD e SPD)	Adulteração dos dados do servidor	Minimização dos dados no servidor, minimização do valor dos dados, salvaguarda de dados.
	Exfiltração de dados do servidor	Minimização dos dados no servidor, controlo de acessos.
	Recusa de acesso aos dados	N/A
Comunicação de gestão aos servidores *backend* (SLD e SPD)	Ligação adulterada	Uso de protocolos de comunicação seguros (sobre TLS)
	Ligação permite exfiltração de dados	Uso de protocolos de comunicação seguros (sobre TLS)
	Saturação da API de gestão	N/A
Processo de desenvolvimento e implantação do sistema	Falsificação da equipa da aplicação	Todos os desenvolvedores têm autenticação própria para submissão das aplicações nas lojas Google e Apple. As aplicações estão associadas a contas da FCT devidamente autenticadas.
	Violação da aplicação dev/mgmt	O ambiente de desenvolvimento é seguro e regido pelos standards de proteção de repositórios de código e de conhecimento. A aplicação é assinada com certificados da equipa FCT e validados pelas lojas de aplicações Apple e Google. Uma aplicação alterada não conseguirá ser instalada nos dispositivos finais dos utilizadores nem conseguirá acesso à GAEN.
	Rejeição da ação dev/sysadmin	Automação e documentação em repositórios seguros.
	Fugas de dados da aplicação dev/mgmt	Código fonte da aplicação será aberto e auditável. Não será possível desviar dados da aplicação.
	Dev/sysadmin sobrecarregados/inundados	Equipa experiente e automação dos processos de gestão e *release* das aplicações.
	Explorar dev/sysadmin para obter privilégios	Autenticação e ambiente de desenvolvimento seguro e com verificação de código.
O repositório do código contém o código fonte da aplicação e dos servidores *backend*	Adulteração do repositório do código	Assinatura do código
	Exfiltração e dados do repositório do código	N/A
	Recusa do serviço no repositório do código	N/A
Administração e gestão	Falsificação dos administradores do sistema	Autenticação forte
	Repúdio de ação do administrador de sistema	Registos de ação seguros
Desenvolvedores	Falsificação de um desenvolvedor	Autenticação forte
	Rejeição ação do desenvolvedor	Registos de ação seguros
A ligação entre a aplicação do DMP e a loja de aplicações para carregamento e atualização da aplicação	A aplicação é adulterada durante o upload	Uso de TLS, assegurado pelas lojas de aplicações
	Upload da aplicação origina exfiltração de dados	Uso de TLS, assegurado pelas lojas de aplicações
	Loja de aplicações está saturada	Assegurado pelas lojas de aplicações
A loja de aplicações responsável	Falsificação da loja de aplicações	Informação aos utilizadores, assegurado pelas lojas de aplicações
	Adulteração da loja de aplicações	Assegurado pelas lojas de aplicações

pela distribuição da aplicação e das suas atualizações	Repúdio de ação pela loja de aplicações	N/A
	Exfiltração de dados da loja de aplicações	Assegurado pelas lojas de aplicações
	A loja de aplicações está saturada	Assegurado pelas lojas de aplicações
	Explorar a loja de aplicações para obter privilégios superiores	Assegurado pelas lojas de aplicações
A ligação entre o DMP e a loja de aplicações para descarregar e instalar a aplicação	Violação do tráfego entre DMP e loja de aplicações	Assegurado pelas lojas de aplicações
	Exfiltração de dados no tráfego entre DMP e loja de aplicações	Assegurado pelas lojas de aplicações
	A ligação entre DMP e loja de aplicações está saturada	Assegurado pelas lojas de aplicações

6.4. Análise dos riscos do sistema com base na tríade CIA[52]

6.4.1. Acesso ilegítimo aos dados pessoais (confidencialidade)

A aplicação não recorre a dados pessoais como o nome ou outro identificador que identifique diretamente o utilizador. Os principais riscos que são avaliados nesta secção, são a possibilidade do utilizador poder ser reidentificado, ou de poderem ser encontradas ou deduzidas informações como, por exemplo, movimentos de pessoas.

Principais impactos nos titulares dos dados se ocorrer o risco

O SPD contém Chaves de Identificadores TEK tornadas públicas pelos seus utilizadores, pelo que não há risco de acesso indevido a estes dados.

O SLD não guarda dados pessoais dos utilizadores, chaves TEK ou Identificadores Aleatórios RPI.

O DMP contém Chaves de Identificadores TEK do próprio e Identificadores Aleatórios RPI dos DMPs remotos com os quais esteve próximo. A limitação do acesso à API GAEN a uma aplicação por país, endossada oficialmente, juntamente com o isolamento da aplicação no sistema operativo (*sandboxing*), permite reduzir consideravelmente o risco de ação de software ilegítimo ou qualquer outra aplicação aparentemente inofensiva que possa ter um comportamento malicioso. Apesar da dificuldade e baixa probabilidade, se os dados protegidos pelo GAEN forem acedidos ilegitimamente, poderiam ser transmitidos para o exterior, podendo alimentar coleções em larga escala de Identificadores Aleatórios RPI que permitiriam a procura de combinações úteis para reconstruir, por exemplo, movimentos de pessoas ou para identificar os pseudónimos de sujeitos diagnosticados com COVID-19.

Para além dos ataques por intrusão nos equipamentos, é necessário avaliar o risco de ataques por recurso a sistemas externos de monitorização (ver 6.1.2). O facto dos RPIs serem alterados, em média, a cada 15 minutos, impossibilita alguém que capte um RPI de conseguir rastrear os movimentos de um dado DMP durante longos períodos. No cenário de captação de RPIs em larga escala, através de muitos dispositivos externos espalhados por uma região, poder-se-ia tentar estimar certos movimentos.

[52] Sigla inglesa para “confidentiality”, “integrity” e “availability”.

No tipo particular de ataque, chamado ataque *Paparazzi* [48], seria possível associar certos RPIs a determinadas pessoas. O potencial impacto neste último cenário de risco é, em princípio, mais limitado por não ser generalizado e circunscrever-se, antes, à esfera daquelas pessoas que, concretamente, são alvo do ataque. Dependendo da pessoa, ou pessoas, e do contexto em questão, poderão, naturalmente, equacionar-se eventuais efeitos indiretos, gerais ou sobre outras pessoas, em particular, para além do diretamente visado pelo ataque.

A divulgação das Chaves de Identificadores TEK dos utilizadores infetados, permite associar diferentes Identificadores RPIs do mesmo DMP, mas não reidentificar diretamente os respetivos utilizadores. Para tal, seria necessário tentar a reidentificação por inferência (ver 6.1.3) ou já ter identificado os utilizadores, entretanto infetados, através de ataques do tipo *Paparazzi*.

A complexidade deste tipo de ataque, bem como a motivação e capacidade para construir e manter uma base de dados em larga escala sem ser detetado durante um período de tempo razoável, apresenta-se como pouco provável. Por exemplo, atualmente, já é possível captar endereços MAC Wi-Fi, que são estáticos, de muitos dispositivos móveis e intentar ataques semelhantes, mas não são conhecidos ataques desta natureza.

O princípio da segregação entre o SLD e o Trace COVID-19, minimizando os fluxos informação entre sistemas ao mínimo imprescindível para a finalidade do SLD, minimiza os riscos de correlação e acesso ilegítimo a dados pessoais. Com efeito, o facto de o médico não se autenticar nem aceder diretamente ao SLD (conforme já foi especificado na secção 2.8), mas através do Trace COVID-19, a cargo da SPMS, permite separar os subsistemas de autenticação e autorização do serviço de geração de códigos CL e CA prestado pelo SLD, fazendo com que o SLD não mantenha nem registe dados dos médicos que requerem os CLs para fornecer aos utilizadores diagnosticados com Covid-19. Assim, ainda que o SLD ficasse comprometido, não haveria dados que permitissem identificar médicos ou os seus pacientes, nem que permitissem usar as contas de sistema no Trace COVID-19 dos médicos para fins ilícitos.

Por outro lado, se o sistema Trace COVID-19 ou uma conta de um médico autorizado neste sistema ficassem comprometidos, o risco seria essencialmente o de obter CLs que poderiam ser usados ilegitimamente por utilizadores que não tivessem sido diagnosticados com COVID-19, espelotando falsos alertas. Pese a criticidade do impacto de um hipotético ataque desta natureza, e o facto de no STAYAWAY COVID ele dever ser evitado, ressalve-se, em todo o caso, que o respetivo impacto seria provavelmente muito superior no seio do Trace COVID-19 do que no sistema STAYAWAY COVID, pelo que é expectável que estejam associadas robustas medidas de segurança adequadas ao Trace COVID-19 mitigadoras deste tipo de ataque.

Finalmente, refira-se que a previsão da utilização de um canal externo, para a comunicação do CL ao utilizador diagnosticado com COVID-19, que não carece de autenticação do utilizador no sistema Trace COVID-19, representa uma relevante garantia para a separação dos dados de *contact tracing*,mantidos no sistema distribuído STAYAWAY COVID, dos dados dos pacientes que são mantidos no sistema Trace COVID-19.Caso seja conhecido um ataque desta natureza e escala, resultará:

- Num sentimento de ansiedade e de receio para os utilizadores, que, desconhecendo o ataque, escala e as tecnologias envolvidas, poderão recear a sua reidentificação ou a divulgação da sua localização nos últimos dias.
- Perda de confiança na aplicação/sistema.
- Num período de inatividade do sistema que vai reduzir a confiança dos titulares de dados na eficácia e utilidade da aplicação.
- Potencial sujeição a estigmatização e decisões discriminatórias no caso remoto de reidentificação.

- Potencial sujeição a sentimentos de ansiedade e receio resultante de uma falsa notificação, para além do incómodo resultante da eventual sujeição a certos cuidados e recomendações destinados a casos reais de risco potencial, designadamente no acima indicado cenário de falsas notificações recebidas na sequência de um ataque e ao sistema Trace COVID-19.

Principais ameaças que podem levar ao risco

- Instalação de software ilegítimo.
- Utilização de dispositivos móveis que não verifiquem a origem das aplicações que são instaladas.
- Utilização de dispositivos móveis que não tenham as atualizações de segurança.
- Vulnerabilidades não corrigidas no sistema operativo do dispositivo móvel, incluindo GAEN.
- Vulnerabilidades não corrigidas na aplicação, tanto ao nível do front end como do back end, incluindo quanto à integração do sistema com o Trace Covid-19.
- Instalação de dispositivos de monitorização/vigilância ilegais numa região.

Fontes de risco

- Hackers ou utilizadores dos dispositivos móveis.
- Elementos que constituem as equipas que fazem o desenvolvimento, gestão, teste e manutenção dos sistemas operativos, implementação GAEN, e da aplicação.
- Erro humano na introdução de datas aquando da geração de CLs ou errónea atribuição/ comunicação dos CLs aos doentes.

Controlos para minimizar os riscos

- Os utilizadores devem ser aconselhados a seguir boas práticas de Higiene e Segurança informática para evitar a instalação de software ilegítimo ou com comportamento malicioso.
- Testes contínuos de segurança à aplicação e respetiva integração com sistemas geridos pelos SPSM. Colaboração do CNCS. Os testes contínuos de segurança às implementações GAEN para Android e IOS são da responsabilidade da Google e Apple.
- Publicação do código fonte permitindo o escrutínio público e a identificação e correção de vulnerabilidades.
- Seguimento nos fóruns próprios acerca de ataques suspeitos (relacionados) ao nível dos dispositivos móveis.
- Legislação que sanciona e pelo seu efeito dissuasor desincentiva a utilização de sistemas de monitorização/vigilância ilícitos.
- Instruções claras aos profissionais de saúde sobre a forma como deverão atuar, designadamente no contexto da interação necessária para o efeito da geração dos códigos de legitimação.
- Separação do SPD e SLD.
- Segregação entre o SLD e o Trace COVID-19, minimizando a troca de informação entre sistemas ao mínimo necessário para a finalidade do SLD.
- Autenticação por médico no portal PRVR.
- Canal externo de comunicação dos códigos CL.

Gravidade do risco, de acordo com impactos potenciais e os controlos implementados/planeados

Indefinido	Insignificante	Limitado	Significativo	Máximo
☐	☐	☒	☐	☐

Considerando o atual contexto de pandemia agravado pela consequente crise económica é inegável a existência de uma pressão sobre a sociedade, o que eleva a gravidade do risco quando são efetuados tratamentos de dados que permitem o rastreio desta nova doença com novas tecnologias ou novas utilizações de tecnologias conhecidas para esta nova finalidade. Porém, o sistema descentralizado e a pseudonimização forte adotados são essenciais para minimizar o risco de re-identificação do utilizador da aplicação, o qual acarretaria um impacto potencialmente significativo.

É notório, nomeadamente nas discussões sobre as questões éticas e de proteção de dados colocadas a propósito das aplicações de rastreio do COVID-19, a existência de alguma resistência às soluções adotadas e dúvidas sobre o real propósito de tais aplicações. A transmissão de informação pouco rigorosa ou fiável em certos meios de comunicação pode adensar receios infundados de vigilância por parte das entidades envolvidas, nomeadamente na utilização da aplicação para localização das pessoas. Assim, é crucial para combater a desinformação uma política de privacidade transparente e clara, em conformidade com o artigo 13.º do RGPD, e que assegure que não são recolhidos identificadores nem dados de geolocalização, mitigando os receios da população nestas matérias.

Probabilidade do risco, em relação a ameaças, fontes de risco e controlos implementados/planeados

Indefinido	Insignificante	Limitado	Significativo	Máximo
☐	☐	☒	☐	☐

As medidas de segurança implementadas para garantir que dados guardados no DMP não são acessíveis para além das pessoas autorizadas são robustas e são especialmente relevantes no que diz respeito à segurança física e lógica da plataforma informática. Porém, é preciso ter em conta o fator humano. Assim, os utilizadores devem ser informados das boas práticas de higiene e segurança informática, bem como sensibilizados sobre todos os elementos que constituam as equipas de desenvolvimento, gestão e manutenção do sistema para a urgência de adoção de práticas de segurança de informação que limitem comportamentos negligentes.

É inegável que existe um grande mediatismo à volta destas aplicações por toda a Europa e um grande interesse por parte de profissionais e aficionados das áreas das novas tecnologias de informação e comunicação, o que pode resultar numa maior probabilidade do sistema ser alvo de ataques informáticos que originam, numa ótica de segurança da informação, uma perda de confidencialidade dos dados.

Em sentido contrário, conforme já destacado, a publicação do código fonte, tanto por parte dos desenvolvedores da aplicação como, na medida existente, pelos responsáveis pelas implementações GAEN, promove a precoce identificação e correção de vulnerabilidades, o que, por sua vez, contribui para uma maior resiliência do sistema perante ataques externos.

Por sua vez o princípio da segregação entre o SLD e o Trace COVID-19, minimizando os fluxos informação entre sistemas ao mínimo imprescindível para a finalidade do SLD, minimiza os riscos de correlação e acesso ilegítimo a dados pessoais. Finalmente, também a previsão de um canal externo para a comunicação do CL representa uma relevante garantia para a separação dos

dados de *contact tracing*, mantidos no sistema distribuído STAYAWAY COVID, dos dados dos pacientes que são mantidos no sistema Trace COVID-19.

6.4.2. Modificação indesejada dos dados pessoais (integridade)

A aplicação não recorre a dados pessoais como o nome ou outro identificador que identifique diretamente o utilizador. Os principais riscos avaliados nesta secção, são a possibilidade de serem usadas Chaves de Identificadores TEK ou Identificadores Aleatórios RPI ilegítimos, para criar falsos positivos, mais concretamente, a apresentação de falsos alertas de exposição ao risco de contágio pela aplicação.

Principais impactos nos titulares dos dados se ocorrer o risco

Um alerta de risco de exposição, não é uma indicação de que utilizador está infetado. Por outro lado, é sabido que tão-pouco serão atribuídos quaisquer efeitos jurídicos a estas notificações de risco de contágio. Contudo, para alguns utilizadores, todo o processo que envolve a realização de um teste de COVID-19, o isolamento profilático, ou outras indicações que sejam dadas pelas autoridades de saúde competentes, causa transtorno e ansiedade e, em caso de residentes em zonas mais isoladas e sem meios para fazer o teste, pode acatar um custo financeiro que pode ser significativo em certos escalões da sociedade no atual contexto de dificuldade económica resultante da crise epidemiológica.

Refira-se, ainda, que a perda de credibilidade da aplicação que acompanharia inevitavelmente a eventual proliferação de casos de falsos positivos (falsos alertas) devido a submissões ilegítimas de Chaves de Identificadores TEK submetidas ao SPD, ou devido ao reencaminhamento de Identificadores Aleatórios RPI ilegítimos, através de outros dispositivos, de utilizadores diagnosticados com COVID-19 para utilizadores remotos, que não estiverem expostos, geraria, igualmente um sentimento de frustração, transtorno e ansiedade nos utilizadores, com impacto na eficácia do sistema.

Principais ameaças que podem levar ao risco

- Ataque informático ao SPD que o comprometa, permitindo que possam ser adicionadas Chaves de Identificadores TEK, passando como sendo de DMPs de utilizadores infetados.
- Submissão ilegítima de Chaves de Identificadores TEK por DMPs recorrendo a códigos CL legítimos.
- Reencaminhamento de Identificadores Aleatórios RPI ilegítimos, através de outros dispositivos, de utilizadores diagnosticados com COVID-19 para utilizadores remotos, que não estiverem expostos (ver 6.1.4).

Fontes de risco

- Hackers ou utilizadores da aplicação.
- Elementos que constituem as equipas que fazem o desenvolvimento, gestão e manutenção do sistema.
- Erro humano na introdução de datas aquando da geração de CLs ou errónea atribuição/ comunicação dos CLs aos doentes.

Controlos para minimizar os riscos

- Testes contínuos de segurança ao código do SPD.
- Monitorização de ataques ao nível do SPD.
- Capacidade de remoção rápida de Chaves de Identificadores TEK ilegítimos.
- Backups frequentes (vários durante o dia) para reposição rápida em caso de SPD comprometido.
- Separação do SPD e SLD.
- Segregação entre o SLD e o Trace COVID-19 nos termos supra apontados.
- Utilização de CL com curto período de validade, que obrigue à sua eventual utilização num curto período e apenas possa ser usada uma vez. Na hipótese de ser alterado o CL deixaria de funcionar.
- Autenticação por médico no portal PRVR.
- Sigilo médico.
- Instruções / procedimentos claros - DGS.
- Comunicação do CL por canal externo.

Gravidade do risco, de acordo com impactos potenciais e os controlos implementados/planeados

Indefinido	Insignificante	Limitado	Significativo	Máximo
☐	☐	☒	☐	☐

A submissão ilegítima de Chaves de Identificadores TEK por DMPs recorrendo a códigos CL por transmissão de um utilizador que recebeu um CL é indetetável pelo sistema mas tende a ser de impacto reduzido por se limitar a um DMP.

O risco de serem reencaminhados Identificadores Aleatórios RPI de utilizadores diagnosticados com COVID-19 apresenta-se como pouco provável, ainda que o impacto de alguns ataques que explorassem esta vulnerabilidade pudessem, eventualmente, ser relevantes.

A aplicação alerta de que o utilizador esteve em contacto com alguém a quem foi diagnosticada COVID-19, durante pelo menos 15 minutos a 2 metros de distância, mas não da probabilidade de este poder ter ficado infetado.

Caso ocorra, resulta num transtorno para o titular de dados que vai, caso opte por seguir a recomendação do alerta, fazer um teste ao COVID-19 desnecessariamente e, possivelmente, com custos financeiros diretos e indiretos.

Pode-se afirmar que gravidade do risco é limitada, já que não aumenta os riscos de reidentificação, sendo a maior preocupação a perda da integridade dos dados, resultando numa exposição do titular de dados pessoais às modificações não autorizadas que podem contribuir para danos morais e patrimoniais em casos de falsos positivos.

Probabilidade do risco, em relação a ameaças, fontes de risco e controlos implementados/planeados

Indefinido	Insignificante	Limitado	Significativo	Máximo
☐	☒	☐	☐	☐

A probabilidade de uma modificação do conjunto de Chaves de Identificadores TEK que estão alojadas no SPD que resulte em falsos positivos (falsos alertas) é muito reduzida. A probabilidade do SPD ficar comprometido é reduzida. As contramedidas permitem reduzir a probabilidade de o ataque passar despercebido durante um longo período de tempo. Além disso, para ser eficaz, teriam de ser muitas Chaves de Identificadores TEK válidas, que teriam de ser obtidas de DMPs, os quais teriam de ter estado próximos de muitos utilizadores.

O risco de serem reencaminhados Identificadores Aleatórios RPI de utilizadores diagnosticados com COVID-19 com impacto relevante, apresenta-se como pouco provável.

6.4.3. Desaparecimento de dados pessoais (disponibilidade)

Principais impactos nos titulares dos dados se ocorrer o risco

Em termos de privacidade, não existem riscos derivados do apagamento de dados pessoais, chaves ou identificadores nos DMPs, SPD e SLD. O impacto, a existir, é essencialmente de eficácia do serviço fornecido; o utilizador perde a possibilidade de poder ser alertado acerca de eventuais contactos com utilizadores diagnosticados com COVID-19.

Principais ameaças que podem levar ao risco

- Apagamento ilegítimo das chaves ou identificadores.
- Falhas no software, hardware ou rede de comunicação que podem originar o apagamento das chaves ou identificadores.

Fontes de risco

- Hackers ou utilizadores da aplicação.
- Elementos que constituem as equipas que fazem o desenvolvimento, gestão e manutenção do sistema.
- Desastres naturais (incêndios, inundações, sismos).
- Problemas com a infraestrutura (corte de energia, erro técnico, dano no equipamento).

Controlos para minimizar os riscos

- Partição dos dados através do modelo descentralizado.
- Backups do SPD.
- Controlo de acessos físicos e lógicos ao SPD e SLD.
- Monitorização de atividade suspeita no SPD ao nível do sistema operativo.
- Medidas de segurança contra ameaças humanas e naturais dos edifícios que alojam o SPD e SLD, designadamente, a existência de serviços de gestão de infraestruturas dedicados, planos de contingência e resposta a eventos de origem humana ou não humana, como incêndios, contratualização de serviços de segurança profissionais e implementação de sistemas de CCTV e de controlo físico de acessos.

Gravidade do risco, de acordo com impactos potenciais e os controlos implementados/planeados

Indefinido	Insignificante	Limitado	Significativo	Máximo
☐	☒	☐	☐	☐

Em termos de privacidade, não existem riscos derivados do apagamento de dados pessoais, chaves ou identificadores nos DMPs, SPD e SLD. O impacto, a existir, é essencialmente de eficácia do serviço fornecido; o utilizador perde a possibilidade de poder ser alertado acerca de eventuais contactos com utilizadores diagnosticados com COVID-19.

No caso de um apagamento no SPD, a maioria dos dados deverá poder ser reposta a partir de um backup recente. No caso do SLD, não são guardados dados pessoais para além dos códigos referidos e existiria sempre a possibilidade de serem gerados novos CL e respetivos CA, já que cada CL é sempre de utilização única. No caso do DMP, o utilizador perde a possibilidade de poder ser alertado acerca de eventuais contactos com utilizadores diagnosticados com COVID-19 nos passados dias (até 14 dias anteriores).

Probabilidade do risco, em relação a ameaças, fontes de risco e controlos implementados/planeados

Indefinido	Insignificante	Limitado	Significativo	Máximo
☐	☐	☒	☐	☐

As medidas implementadas ao nível do SPD, bem como o controlo no acesso à aplicação nos dispositivos móveis e a limitação do acesso ao subsistema GAEN à aplicação STAYAWAY COVID, fazem com que a probabilidade de acidentes ou ataques com impacto relevante seja muito reduzida.

6.5. Avaliação adicional dos riscos: análise do código fonte

Durante a avaliação do impacto da proteção de dados, foi efetuada uma análise do código fonte para a versão 1.1 da aplicação pelas organizações INESCTEC e Keyruptive.

Subsequentes e regulares avaliações serão conduzidas até ao momento da disponibilização pública da solução para utilização.

Além desta avaliação, será realizada uma análise independente pelo Centro Nacional de Cibersegurança, que efetuará um conjunto de testes de caráter técnico, para aconselhamento na mitigação de eventuais vulnerabilidades de segurança, numa perspetiva de colaboração com a comunidade científica nacional ao nível da cibersegurança.

Antes da disponibilização da solução serão conduzidos vários testes piloto, com vista a identificar eventuais falhas ou potenciais riscos ainda não detetados.

Nota de Atualização - Versão 2.0. da AIPD

Na sequência da versão anterior da AIPD e da subsequente deliberação da CNPD foi realizado um teste piloto externo e restrito a um universo significativo de utilizadores, participantes do estudo Diários de uma Pandemia, no decurso do qual foram testados os principais componentes do sistema e corrigidas vulnerabilidades identificadas.

A Publicação do código fonte, pela equipa do INESC TEC e Keyruptive, através do github[53], contribui para este desiderato permitindo a ativa participação da comunidade dos especialistas na área da segurança informática e proteção de dados.

Acresce como fator positivo digno de menção a disponibilização pública por parte da Google de código fonte da respetiva API, através do github[54], contribuindo para a transparência e escrutínio da integralidade do sistema, iniciativa que posteriormente foi igualmente acompanhada pela empresa Apple.

Avaliação EPD

Verifica-se que os riscos mais críticos e sobressalientes analisados (associados à disseminação de pseudónimos e a cenários de reidentificação por ataque externo) pendem-se, fundamentalmente, com características intrínsecas do modelo de dados e da arquitetura descentralizada, e não das especificidades do sistema tecnológico em desenvolvimento. Por outro lado, numa comparação com modelos de arquitetura mais centralizada, vemos que estes últimos apresentam, igualmente, as suas vulnerabilidades. Ambos apresentam as suas vantagens e desvantagens. No que concerne aos riscos identificados, as medidas técnicas e organizacionais apontadas dir-se-ão, genericamente, e no seu conjunto, adequadas à sua mitigação e proporcionadas.

Relativamente à utilização da API da Google e a Apple, convém sublinhar que, ao contrário do DP^3T, o código da GAEN API não é aberto, sendo expectável e recomendável uma atenção redobrada pela comunidade à forma como a GAEN API trata os dados. De acordo com a GAEN API, apenas uma aplicação por país e endossada oficialmente está autorizada a aceder à API.

Muito embora os riscos assinalados possam considerar-se, na sua generalidade, como satisfatoriamente mitigados, por contrabalançados com medias organizativas e técnicas proporcionadas ao impacto e probabilidade de ocorrência dos riscos identificados, nunca será de mais reforçar a inevitável permanência de riscos potenciais, na sua maioria inerentes às características dos modelos que vêm sendo analisados e comparados no contexto atual, e que dada a escala da sua potencial utilização - antecipando-se e almejando-se, até, uma utilização massiva da solução de rastreio, os mesmos hão de considerar-se, não negligenciáveis, e em contextos que possam não ter sido identificados, como potencialmente elevados.

Por este motivo justificar-se-ia, salvo melhor opinião, a submissão de um pedido de consulta prévia à autoridade de controlo por parte do responsável pelo tratamento de dados, nos termos e para os efeitos do artigo 36.º n.º 1 do RGPD, sem prejuízo da possibilidade de um pedido de parecer no âmbito de uma eventual iniciativa legislativa de enquadramento da sua implementação e utilização. De resto, saliente-se que, não por acaso, o próprio RGPD no n.º 5 do mesmo artigo confere aos Estados Membros margem para consagrar nos respetivos ordenamentos jurídicos nacionais, um requisito de autorização prévia em casos de tratamentos de dados por responsável no exercício de missão de interesse público, incluindo por motivos de saúde pública. No mesmo sentido apontaria um princípio de precaução, atenta a novidade do contexto e da escala da utilização da tecnologia (BLE) empregue.

A realização de um teste piloto, em condições reais, circunscrito a um grupo específico de utilizadores antes da disponibilização mais alargada e irrestrita, recomendada na prévia versão

[53] Disponível em: https://github.com/stayawayinesctec.

[54] Disponível em: https://github.com/google/exposure-notifications-internals.

desta avaliação e na deliberação da CNPD, foi, sem dúvida, um passo importante no sentido de assegurar uma atempada correção de falhas e vulnerabilidades e de providenciar maiores garantias de segurança e robustez do sistema.

Acresce a prévia aprovação por Comissão de Ética independente.

Na fase de acompanhamento subsequente à disponibilização alargada da solução, será adequado constituir um comité independente de acompanhamento e aconselhamento, inclusivo e desejavelmente com a participação de representantes da comunidade de utilizadores.

Finalmente, a regular revisão da presente avaliação de impacto revela-se imprescindível como medida de controlo e monitorização, salvaguardando a necessidade de implementar medidas adicionais para fazer face a riscos entretanto detetados durante a fase de utilização, seja no decurso de testes ou já de adoção alargada pela população.

Uma parte dos riscos potenciais é mitigável através de uma utilização informada dos recursos disponíveis por parte dos usuários. Por este motivo é relevante fazer acompanhar a disponibilização da aplicação da divulgação regular de informação clara e transparente sobre o uso e funcionalidades da solução, bem como, de conselhos práticos ao nível da utilização e da configuração dos próprios dispositivos móveis em que corre esta e outras aplicações, porventura com um grau de intrusão superiores à ora avaliada. Com efeito, para além dos cuidados a ter com a segurança dos dispositivos móveis, para evitar, por exemplo, a ação nefasta de malware, importa não descurar, igualmente, a existência de eventuais externalidades negativas decorrentes da utilização intensiva de um novo sistema, (cuja eficácia depende, de resto, da sua utilização mais ou menos alargada e continuada) em concomitância com outras aplicações já instaladas, muitas das quais com permissões de acesso a dados pessoais particularmente intrusivas.

Eventuais efeitos colaterais da adoção da tecnologia poderão, assim, ser compensados, através de campanhas de sensibilização para uma boa e responsável utilização de recursos informáticos, em particular, de dispositivos móveis, acompanhando as expectáveis campanhas de incentivo à utilização alargada e regular da aplicação de rastreio de contactos pela população. Uma entidade como o CNCS, que para além da sua missão, soma a uma capacidade de avaliação técnica de soluções tecnológicas complexas, uma larga experiência pedagógica e de disseminação de boas práticas em temas de cibersegurança, perfilar-se-ia, a este propósito, como especialmente adequada para a transmissão daquela mensagem de sensibilização geral, muito embora vários outros organismos ou entidades disponham de valências e competências para cumprir com tal desiderato.[55]

Enfatiza-se a necessidade de serem dadas instruções precisas aos profissionais de saúde (médicos), para tanto devendo contribuir o próprio processo de normação legal conduzido, e cumpridos procedimentos estabelecidos ao nível dos SPMS para garantir a confidencialidade dos dados tratados.

Os riscos assinalados podem considerar-se, na sua generalidade, como satisfatoriamente mitigados, por contrabalançados com medias organizativas e técnicas proporcionadas ao impacto e probabilidade de ocorrência dos riscos identificados.

[55] O mapeamento e análise de risco do sistema com base na tríade CIA estão representados graficamente no apêndice C.

No entanto, no que concerne especificamente à componente do sistema a cargo dos SPMS, referente, concretamente, à interface entre o sistema STAYAWAY COVID e os sistemas próprios do Ministério da Saúde e ao sistema da autenticação / autorização de acesso por parte de médicos, a respeito da validação dos casos positivos de COVID-19, cujos detalhes de implementação foram testados de forma controlada durante o teste Piloto realizado, será útil e adequado o seu acompanhamento regular pelo parceiro CNCS, designadamente auditando aos aspetos de segurança informática das soluções implementadas, tendo em vista, em particular o desiderato de assegurar a proteção dos dados tratados e a não introdução de dados identificáveis dos doentes diagnosticados com COVID-19 ao nível do SLD.

A este propósito realce-se a importância do papel já desempenhado pelo CNSC, tanto ao nó nível da execução da análise estática do código fonte como da performance de outros testes e avaliações contextuais de cibersegurança da solução implementada, esforço este complementado pelos contributos da comunidade académica, na área das ciências da computação e, genericamente, dos especialistas e interessados em informática, tornados possíveis pela publicação do código fonte.

No mesmo sentido, como reforço dos adequados mecanismos de segregação já implementados, recomenda-se que o SLD e Trace Covid-19 sejam mantidos por equipas diferentes, atendendo a que são operados por uma mesma entidade.

Tal preocupação não deve descurar, no entanto, a integração com os processos e procedimentos existentes e a importante vertente de usabilidade que recomenda a audição de partes interessadas como a Ordem dos Médicos, por forma a melhor garantir a adoção e contínuo aperfeiçoamento das soluções implementadas, essencial para a garantia da eficiência deste recurso complementar da estratégia de saúde pública gizada.

Outra preocupação que (justificadamente) tem sido levantada e aflorada recentemente, tanto em Portugal como um pouco por toda a Europa, refere-se à questão das permissões solicitadas pela Google no contexto do sistema operativo Android, aquando da instalação da aplicação, ao nível dos serviços de localização, em aparente contradição com as permissões que são referenciadas nesta avaliação como necessárias à utilização do sistema e que prescindem de georreferenciação.

Registam-se como positivos os esclarecimentos entretanto prestados no sentido de que o sistema de notificação de exposição não utiliza a localização do dispositivo Android e não partilha nenhuma informação do utilizador com a Google. Ou seja, a utilização da API não requer de facto, e não utiliza a interface de GPS, ainda que seja solicitada ao utilizador a ativação dos serviços de localização.

Reconheça-se, no entanto, que não deixa de constituir uma limitação relevante que o serviço BLE [tecnologia Bluetooth utilizada] esteja, no sistema operativo Android, ligado aos "Serviços de localização", permanecendo estes ligados como condição para a utilização da aplicação, ainda que não sejam recolhidos quaisquer dados sem a permissão dos utilizadores, por via de outras aplicações instaladas nos dispositivos móveis. Neste sentido os esforços que vêm sendo levados a cabo por vários governos junto da empresa Google, propondo a implementação de uma solução, designadamente, ao nível do sistema operativo Android, que permita que este tipo de aplicações de notificação de exposição seja usado sem que se torne necessário manter

ativos os serviços de localização, afiguram-se como muito importantes e os seus resultados devem ser acompanhados com atenção. Do mesmo passo, impõe-se um especial dever de cuidado ao nível da prestação de informação atualizada aos utilizadores, dissipando dúvidas existentes a propósito deste tema. Sublinhe-se, novamente, que a transparência é uma condição da confiança imprescindível para o sucesso do sistema na prossecução dos seus objetivos.

Finalmente, e em coerência com o supra exposto, só podemos saudar e reputar como muito relevantes as iniciativas recentes, tanto da Google como da Apple, quanto à publicação de código fonte, constituindo mais um contributo para o aumento das condições de transparência e, bem assim, de segurança e robustez do sistema. Trata-se de uma medida que deve ser analisada na sua extensão e significado e acompanhada atentamente, devendo resultar num maior escrutínio quanto à Interface de Programação de Aplicações GAEN.

Aceitável	☐	Aceitável com recomendações	☒	Inaceitável	☐

7. Conclusão e recomendações

A solução STAYAWAY COVID é uma implementação de um sistema de notificação da exposição baseado num modelo de dados distribuídos e numa arquitetura semidescentralizada. A conceção do sistema STAYAWAY COVID foi iniciada antes da disponibilização da interface de Notificação de Exposição Google-Apple (GAEN API), tendo, entretanto, sido adaptado para a utilização das novas funcionalidades que esta permite. O protocolo implementado pela GAEN API é muito próximo do protocolo DP^3T. A Google e a Apple disponibilizam a especificação do protocolo, algoritmos e respetiva API, contudo, ao contrário do DP^3T, à data da presente avalaição nem todo o código da GAEN API é inteiramente aberto. Regista-se porém, como positivo que, conforme havia sido previamente anunciado e pudemos já ressaltar noutras passagens, parte do código do sistema GAEN implementado pela Google foi já entretanto disponibilizado.

A aplicação pretende dar um contributo significativo para a rápida interrupção das cadeias de infeção no decurso da epidemia provocada por COVID-19, procurando detetar, apoiada pela automatização, os chamados contactos intensivos. Em causa estão os contactos entre pessoas singulares que duram mais de 15 minutos e em que a distância física entre os utilizadores da aplicação é inferior a 2 metros.

O sistema STAYAWAY COVID não deverá ser visto, nem deverá funcionar, como uma medida autónoma, mas antes enquanto medida complementar de outras tantas medidas como a mobilização do pessoal de saúde e dos investigadores sanitários, a disponibilidade de máscaras e testes ou a sensibilização para higienização, todas elas cruciais para colher os benefícios positivos da utilização da aplicação. Esta mobilização de recursos faz, portanto, parte de um plano global, que a aplicação integrará.

Neste sentido, a aplicação não se destina a controlar o cumprimento das medidas de confinamento ou outras obrigações sanitárias, nem tão-pouco a identificar as zonas para onde essas pessoas se deslocaram. Por esta ordem de motivos, não deverão ser extraídos quaisquer efeitos jurídicos (ou outros de importância equivalente na esfera dos utilizadores) a partir dos resultados atingidos através da utilização da aplicação. Esta conclusão deve ser vista como um corolário natural do cariz voluntário e não discriminatório, erigido em requisito essencial da aplicação e respetiva disponibilização pública.

O caráter voluntário não se deve manifestar apenas no momento em que o utilizador descarrega a aplicação, ou seja, na sua instalação, mas também na verificação da habilitação do Bluetooth ou ainda na capacidade de a desinstalar.

O carácter voluntário não se confunde com o consentimento, enquanto fundamento de licitude. A base jurídica mais pertinente para o tratamento de dados em questão, atenta a finalidade declarada, é a necessidade de exercer funções de interesse publico no domínio da saúde pública, nos termos articulados do artigo 6.º, n.º 1, alínea e), e do artigo 9.º n.º 2, alínea i) ambos do RGPD. Como já se assinalou, tal conclusão pressupõe a designação de um responsável pelo tratamento que, atenta a finalidade da aplicação de rastreio em análise, tenha por mandato o exercício de funções de interesse público ou de autoridade pública relacionados. A este propósito, a Deliberação 2020/277 da CNPD, de 20 de junho, relembra que o consentimento do titular, enquanto manifestação de vontade inequívoca à instalação da aplicação no seu dispositivo móvel, será fundamento de licitude desde que cumpridos os quatro requisitos que tornam o seu consentimento válido (previstos na alínea 11 do artigo 4º do RGPD). Acrescenta, ainda, a Deliberação que "(...) 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 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."

A solução STAYAWAY COVID visa cumprir com todos os princípios fundamentais da proteção de dados, incorporando características que acautelam a proteção de dados desde a conceção e por omissão. A ponderação exigida pelo princípio da proporcionalidade afigura-se forçosamente complexa, especialmente perante contextos de reconhecida excecionalidade como aquele que atravessamos, atreitos a tentações de solucionismo tecnológico. É porém, inquestionável, no caso presente, a relevância social dos benefícios em causa, especialmente quando integrados, adequadamente, numa estratégia global de natureza sanitária cuja eficiência se pretende maximizar.

Os diferentes e inquestionáveis méritos do modelo de gestão descentralizada de dados em que se baseia o STAYAWAY COVID, especialmente ao nível do princípio da minimização de dados, são acompanhados por algumas fragilidades intrínsecas das quais é necessário estar consciente também para adotar as medidas adequadas de mitigação de riscos relacionadas com a possível reidentificação dos utilizadores que alteraram o seu estado de saúde, tornando-se diagnosticados com COVID-19.

No que concerne aos riscos identificados, as medidas técnicas e organizacionais apontadas dir-se-ão, genericamente, e no seu conjunto, adequadas à sua mitigação e proporcionadas.

Relativamente à utilização da API da Google e a Apple, convém sublinhar que, ao contrário do DP^3T, o código da GAEN API não é ainda inteiramente público, sendo por isso expectável e recomendável uma atenção redobrada pela comunidade à forma como a GAEN API trata os dados. De acordo com a GAEN API, apenas uma aplicação por país e endossada oficialmente está autorizada a aceder à API. Regista-se, no entanto, como muito positiva a iniciativa recente da publicação de código fonte por parte daquelas empresas, com inegáveis ganho para tanto para segurança como para a imprescindível transparência na utilização do sistema.

Conforme referido pelo EPD, muito embora os riscos assinalados possam considerar-se, na sua generalidade, como satisfatoriamente mitigados, por contrabalançados com medias organizativas e técnicas proporcionadas ao impacto e probabilidade de ocorrência dos riscos identificados, nunca será de mais reforçar a inevitável permanência de riscos potenciais, na sua maioria inerentes às características dos modelos considerados, e ainda que, dada a escala da sua potencial utilização - antecipando-se e almejando-se, até, uma utilização massiva da solução de rastreio, os mesmos riscos hão de sempre considerar-se não negligenciáveis, e em contextos específicos que possam não ter sido ainda identificados ou acautelados, qualificados como potencialmente elevados.

Por esse motivo é justificada a submissão de um pedido de consulta prévia à autoridade de controlo, nos termos e para os efeitos do artigo 36º nº 1 do RGPD. No mesmo sentido apontaria sempre um princípio de precaução, atenta a novidade do contexto e da escala da utilização da tecnologia (BLE) empregue.

7.1. Decisão sobre procedimento a seguir

Implementação das medidas mitigadoras de riscos planeadas e previstas na secção 6.

Consideração de outras medidas eventualmente sugeridas pelo CNCS e das recomendadas pela CNPD.

Realização de um teste piloto, em condições reais, circunscrito a um número significativo de pessoas no território nacional antes da disponibilização mais alargada e irrestrita, em linha com o sugerido pelo EPD e recomendado pela CNPD.

Continuação dos testes regulares e avaliação contínua durante a fase de produção e pré-produção.

Consideração de eventuais recomendações de parecer da Comissão de Ética independente - do ISPUP.

Regular revisão da presente avaliação de impacto.

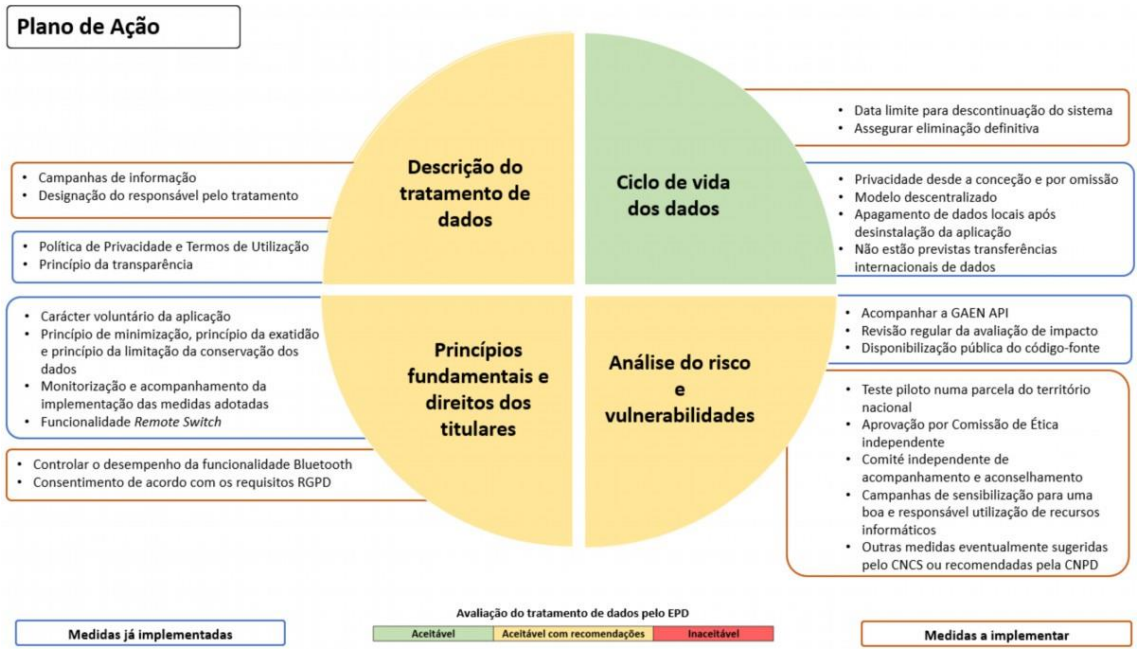


Figura 12 - Plano de ação

7.2. Futuras revisões

Conforme acima referido, a regular revisão da presente avaliação de impacto revela-se imprescindível como medida de controlo e monitorização, salvaguardando a necessidade de implementação de medidas adicionais para fazer face a riscos entretanto detetados durante a fase de utilização, seja no decurso de testes ou já de adoção alargada pela população.

É de esperar uma próxima revisão considerando uma eventual interoperabilidade com sistemas similares de outros Estados. A receção de contributos da parte do CNCS ou de eventuais recomendações adicionais da parte da CNPD deverão, igualmente, ser endereçados em nova avaliação.

Referências bibliográficas

CALVÃO, FILIPA URBANO, «Garantia de direitos: a proteção de dados pessoais perante os desafios tecnológicos», *in Garantia de Direitos e Regulação: Perspetivas de Direito Administrativo*, AAFDL Editora, 2020.

CANOTILHO, J. J. GOMES, Direito Constitucional e Teoria da Constituição, Almedina, 7.ª Edição.

_____O problema da responsabilidade do Estado por actos lícitos, Almedina, 1974.

FERRETI, Luca; WYMANT, Chris Wymant; KENDALL, Michelle; ZHAO, Lele; NURTAY Anel; ABELER-DORNER, Lucie; PARKER, Michael; BONSALL, David; FRASER, Christophe, «Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing», in Science, Vol. 368, n.º 6491, American Association for the Advancement of Science, 2020.

HILDEBRANDT, Mireille "The New Imbroglio – Living with Machine Algorithms", in The Art of Ethics in the Information Society, 2016. Disponível em https://works.bepress.com/mireille_hildebrandt/75/.

NEVES, António Castanheira, Metodologia Jurídica: Problemas fundamentais, Coimbra Editora, 2013.

MÖLLER, KAI - «Proportionality: Challenging the critics», in International Journal of Constitutional Law, vol. 10, n.º 3 (2012), pp. 709-731.

MONGE, Cláudia, «Proteção de dados de saúde nos hospitais públicos», in Revista de Direito Administrativo, n.º 8, 2020.

MORAIS, Pedro Jacob, «O internamento compulsivo do portador de doença infecto-contagiosa notas de andar e ver», *in Lex Medicinae*, Ano 10, n.º 20, 2013.

PINHEIRO, Alexandre Sousa, *Privacy e Proteção de Dados Pessoais - a construção dogmática do direito à identidade informacional*, Lisboa, AAFDL, 2015, página 826.

VICENTE, Laura Nunes, O Princípio da Proporcionalidade - Uma Nova Abordagem em Tempos de Pluralismo, Faculdade de Direito da Universidade de Coimbra - Instituto Jurídico, 2014, páginas 28-29.

VAUDENA, Serge Vaudenay, *Analysis of DP3T - Between Scylla and Charybdis*, IACR-EPRINT, 2020. Disponível em https://eprint.iacr.org/2020/399.pdf.

BAUMGARTNER, Lars, et al., «Mind the GAP: Security & Privacy Risks of Contact Tracing Apps», 2020. Disponível em https://arxiv.org/abs/2006.05914.

Documentos Oficiais União Europeia

Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter,Data Protection Commissioner of the Council of Europe, março 2020.

Wojciech Wiewiórowsk, EU Digital Solidarity: a call for a pan-European approach againstthe pandemicWojciech Wiewiórowsk, de 6 de abril de 2020.

Grupo de Trabalho do Artigo 29.ºOrientações relativas ao consentimentona aceção do Regulamento (UE)2016/679, adotadas em 28 de novembro de 2017Última redação revista e adotada em 10 de abril de 2018.

Comunicação da Comissão Europeia — Orientações respeitantes a aplicações móveis de apoio à luta contra a pandemia de COVID-19 na perspetiva da proteção de dados, C(2020) 2523 final, de 16 de abril de 2020.

Comunicação da Comissão Europeia, Orientações respeitantes a aplicações móveis de apoio à luta contra a pandemia de COVID-19 na perspetiva da proteção de dados (2020/C 124 I/01), de 17 de abril de 2020.

Diretrizes 4/2020 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19 do Comité Europeu para a Proteção de Dados, de 21 de abril de 2020.

EUROPEAN UNION AGENCY FOR CYBERSECURITY, “COVID-19 apps - cybersecurity requirements and testing”.

Documentos de Autoridades de Proteção de Dados Externas

CNIL, Deliberation N°. 2020-046 of April 24, 2020 delivering an opinion on a proposed mobile application called "StopCovid".

«Tracing App des Bundes»Wissen, Einstellungen, ErklärungsfaktorenStudienbericht zur Bevölkerungsbefragung, maio de 2020. Disponível em https://sotomo.ch/site/wp-content/uploads/2020/05/sotomo_BAG_TracingApp.pdf.

The Health Foundation COVID-19 SurveyA report of survey findings on public attitudes towards a potential smartphone app to ‘track and trace’ Coronavirus outbreaks, maio 2020. Disponível em https://www.health.org.uk/sites/default/files/2020-06/Health-Foundation-polling-contact-tracing-app-May-2020.pdf.

Projeto de Investigação, Diários de Pandemia, Disponível em https://diariosdeumapandemia.inesctec.pt/.

TECHNOLOGIES IN THE FIGHT AGAINST COVID19. A COST-BENEFIT ANALYSIS. Agencia Española de Protección de Dados, maio 2020. Disponível em https://www.aepd.es/sites/default/files/2020-05/analisis-tecnologias-COVID19.pdf.

Ac. Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, The Attorney General, Proc. n.º C-293/12 e C-594/12, de 8 de abril de 2014.

Ac. proferido no contexto de um reenvio prejudicial, referente à responsabilidade pelo tratamento de dados pessoais implicado nas comunicações porta-a-porta realizados por testemunhas de jeová, e à possibilidade de responsabilidade conjunta com a respetiva comunidade religiosa, Proc. n.º C-25/17, de 10 de julho de 2018.

Ac. proferido no contexto de um reenvio prejudicial, referente ao caso de uma página de fãs na rede social Facebook e ao estatuto de responsável pelos tratamentos de dados efetuados através daquela página, Proc. n.º C-40/17, de 29 de julho de 2019.

Ac. Volker und Markus Schecke e Eifert, Proc. n.º C-92/09 e de 9 de novembro de 2010;

Acórda GC e o. c. Commission nationale de l'informatique et des libertés (CNIL), Proc. n.º C-136/17, de 24 de setembro de 2019.

Apêndices

Apêndice A - Requisitos comuns definidos por organizações internacionais / europeias e respetiva implementação no sistema STAYAWAY

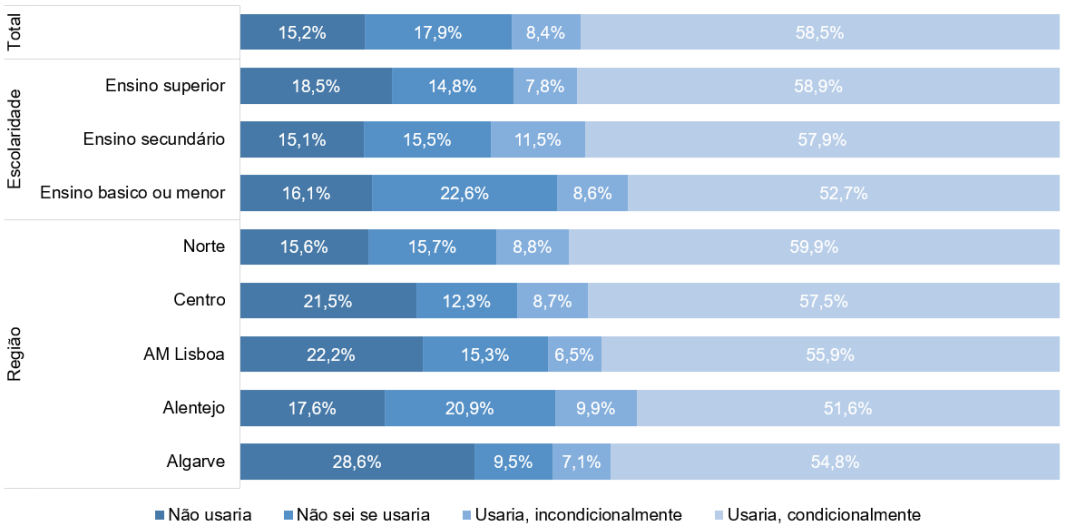
Os documentos em que se baseia a tabela apresentada permitem identificar um conjunto de recomendações comuns emitidas pela Comissão Europeia, o Comité Europeu para a Proteção de Dados e o Conselho da Europa, relativamente ao tratamento de dados pessoais no contexto da pandemia de COVID-19, especificamente, através da utilização de aplicações móveis para rastreio de contactos. Deste modo, pretende-se verificar e controlar o grau de cumprimento pelo sistema STAYAWAY dos requisitos nas mesmas mencionados como salvaguarda do respeito pelos direitos fundamentais e as liberdades dos titulares dos dados.

	EC - eHealth Network Toolbox	EC - Guidance	EDPB - Guidelines	Council of Europe - Joint Statement	**Sistema STAYAWAY**	
					Implementação	**Justificação**
Eficácia comprovada antes do desenvolvimento	✔	✔		✔	✔	Execução de testes piloto
Voluntária	✔	✔	✔	✔	✔	A adesão à aplicação é voluntária, bem como a difusão dos códigos no servidor quando é diagnosticada a doença.
Avaliação prévia	✔	✔	✔	✔	✔	Antes da disponibilização pública da aplicação foi realizada uma avaliação prévia do impacto da app nos titulares de dados pessoais.
Privacidade desde a conceção	✔	✔	✔	✔	✔	Cariz voluntário ao longo do tratamento de dados. Modelo distribuído dos dados. Pesudonimização forte.
Finalidade específica e base jurídica	✔	✔	✔	✔	✔	A app visa contribuir para um rastreio mais rápido, amplo e eficaz da COVID-19 em Portugal. Os fundamentos de licitude para tratamento de dados na aplicação móvel é o interesse público no domínio da saúde pública com base na lei nacional portuguesa e nos artigos 6º nº 1 e) e 9º nº2 i) do RGPD.
Código aberto (transparência)	✔	✔	✔	✔	✔	O código da aplicação vai estar disponível ao público.
Minimização e exatidão dos dados	✔	✔	✔	✔	✔	Sistema distribuído com cruzamento de códigos aleatórios ao nível dos próprios dispositivos móveis; finalidade restrita à notificação de risco de contágio, recolha de dados

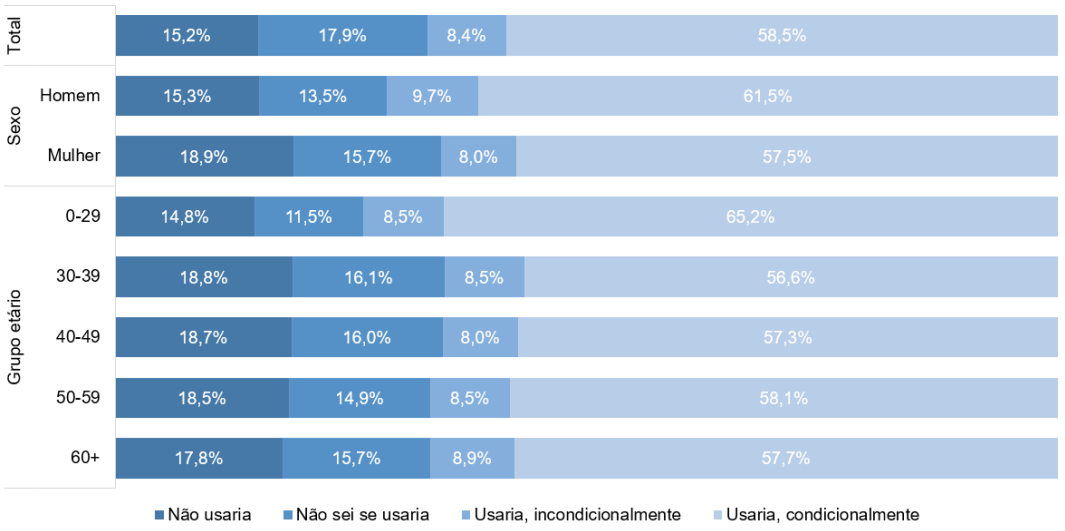
						epidemiológicos adicionais
Exatidão tecnológica das deteções de contactos	✔	✔	✔		✔	A avaliação da distância entre dispositivos deduzida da intensidade do sinal Bluetooth comporta margem de erro, Porém, noutra vertente, é crucial ter sido implementada a validação por médico através de subsistema de autenticação, limitando enormemente o risco de ocorrência de falsos positivos em grande escala.
Dados anonimizados ou dados pseudonimizados	✔	✔	✔	✔	✔	São usados identificadores alfanuméricos efémeros e gerados aleatoriamente, que legalmente são considerados dados pseudoanonimizados.
Segurança contra ciberataques	✔	✔	✔	✔	✔	Medidas previstas na secção 6 da presente AIPD, sem prejuízo de medidas adicionais que sejam adotadas no âmbito da sua revisão regular.
Sem dados de geolocalização	✔	✔	✔	✔	✔	Não são recolhidos dados de geolocalização.
Supervisão independente contínua	✔	✔	✔	✔	✔	Acompanhamento e avaliação por CNSC e Comissão de Ética ISPUP; planeamento de criação de comité independente de acompanhamento
Interoperabilidade	✔	✔	✔	✔	✔	Sim, ainda em fase de desenvolvimento.
Desativação e eliminação após a pandemia	✔	✔	✔	✔	✔	Todo o sistema será descontinuado quando o fim da pandemia for declarado em Portugal.
Responsabilização e responsabilidade dos intervenientes	✔	✔	✔		✔	Designação obrigatória de responsável pelo tratamento como condição da disponibilização da tecnologia; Revisão regular da AIPD.

Apêndice B - Resultados da questão sobre a aplicação móvel de rastreio de COVID-19 efetuada aos participantes do projeto de investigação Diários de uma Pandemia

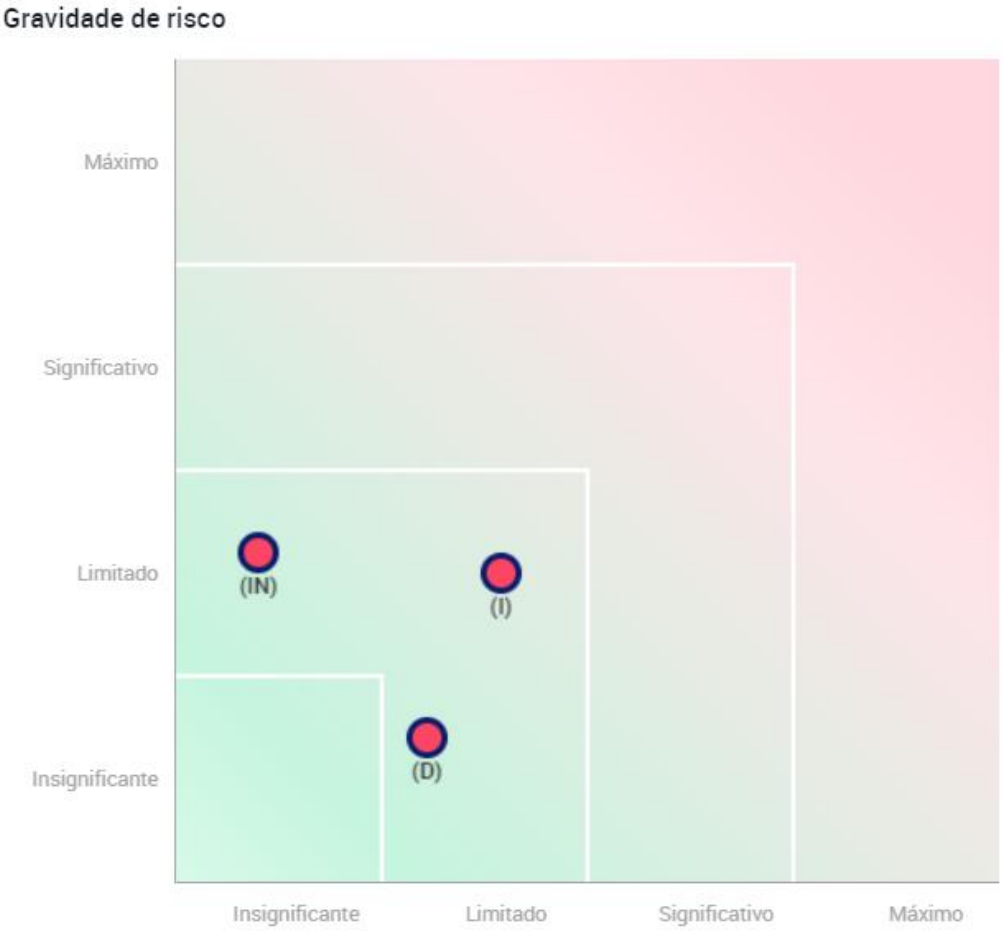
Se houvesse uma aplicação para telemóvel (app), voluntária e gratuita, capaz de informar sobre a possibilidade de ter estado em contacto com alguém infetado:



Se houvesse uma aplicação para telemóvel (app), voluntária e gratuita, capaz de informar sobre a possibilidade de ter estado em contacto com alguém infetado:

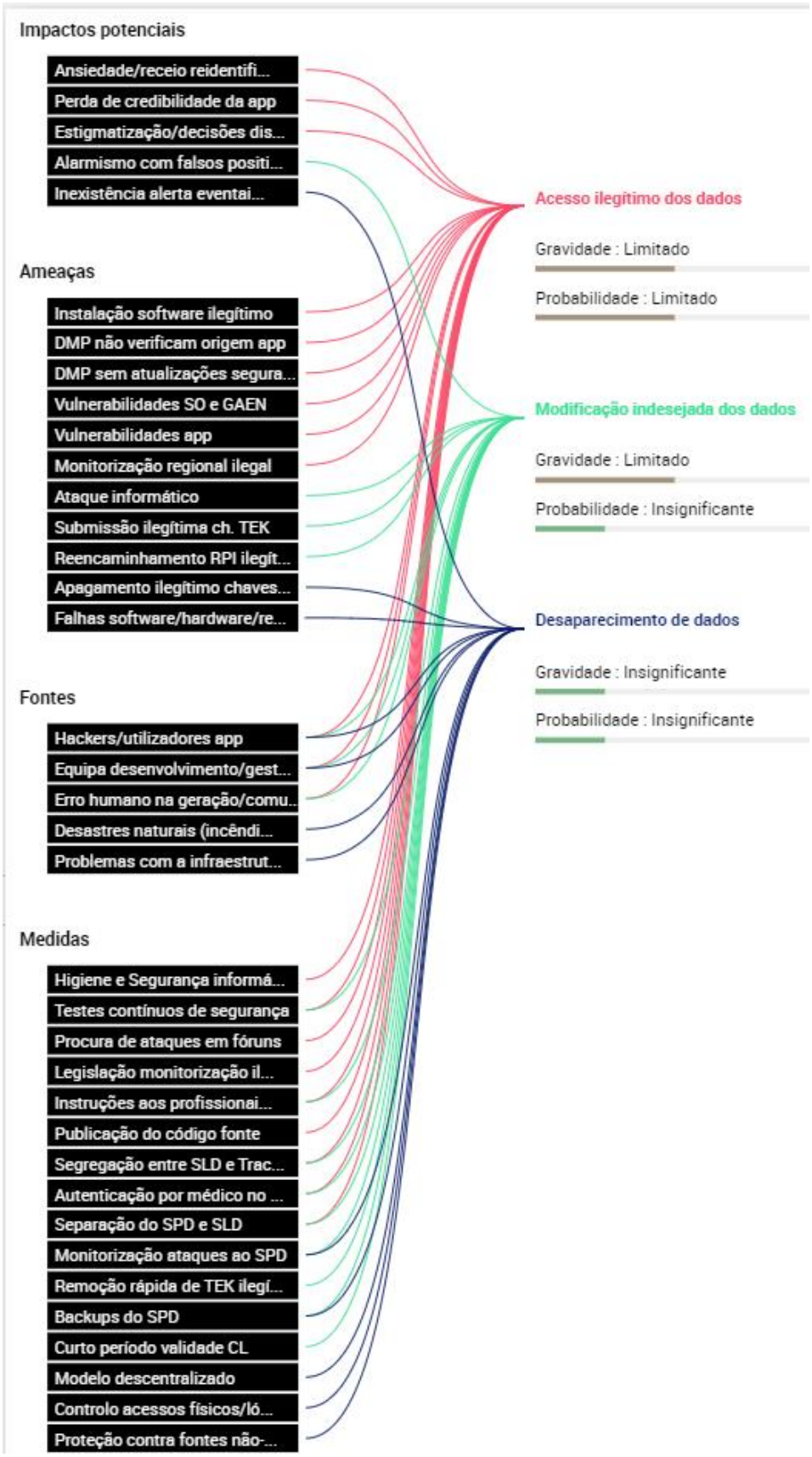


Apêndice C.1 – Mapeamento e Análise dos Riscos do sistema



- Medidas existentes ou planeadas
- Com as medidas corretivas implementadas
- Acesso (i)legítimo aos dados
- Modificação (in)desejada dos dados
- Desaparecimento dos dados

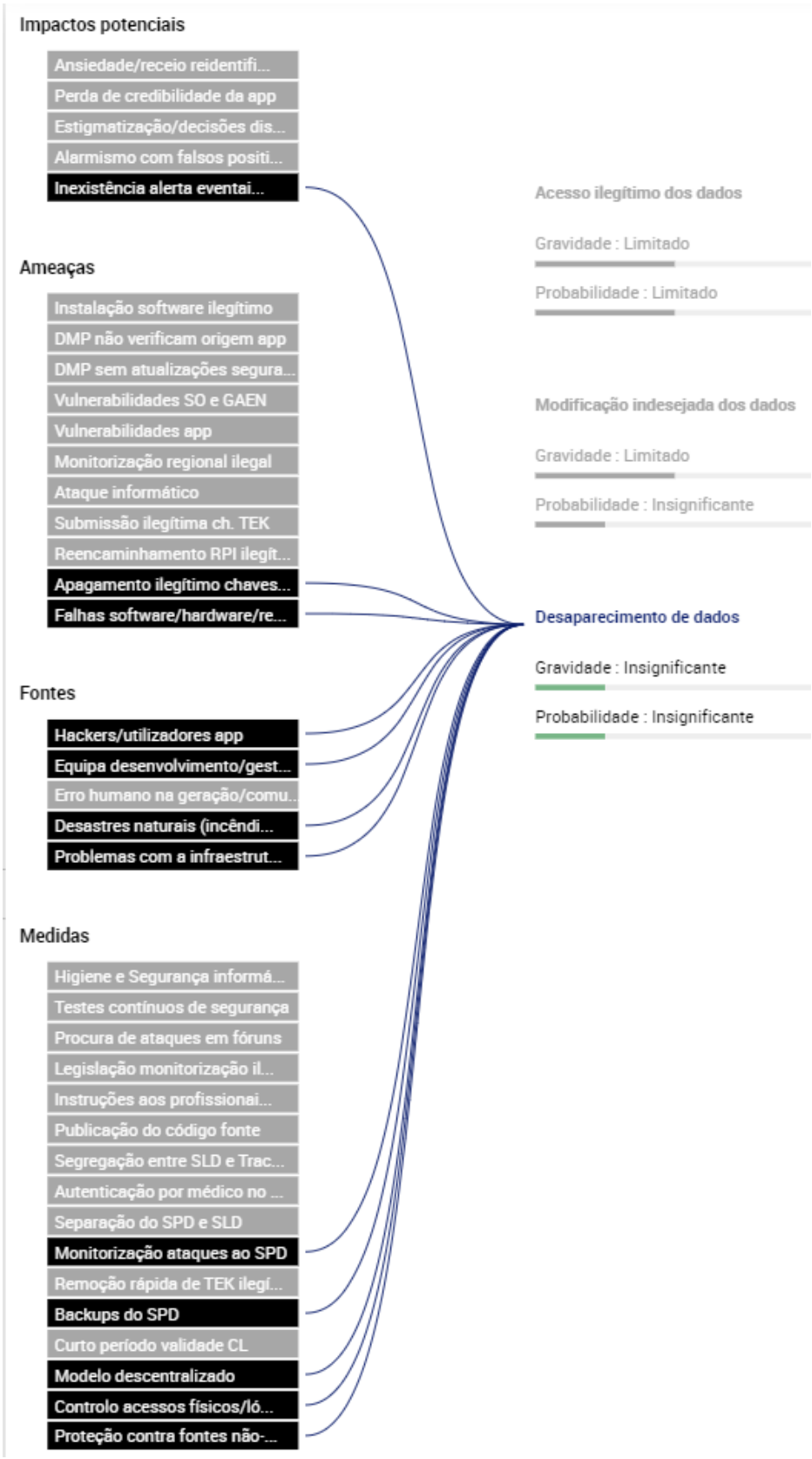
Apêndice C.2 - Mapeamento e Análise dos Riscos do sistema - Vista geral



Apêndice C.3 - Mapeamento e Análise dos Riscos do sistema - Acesso ilegítimo aos dados pessoais (confidencialidade)

Apêndice C.4 - Mapeamento e Análise dos Riscos do sistema - Modificação indesejada dos dados pessoais (integridade)

Apêndice C.5 - Mapeamento e Análise dos Riscos do sistema - Desaparecimento de dados pessoais (disponibilidade)



Deliberação CNPD 2020/277				
Ponto	**Tópico**	**Pág. AIPD**	**Justificação**	**Medidas a implementar**
28	Realização de teste piloto circunscrito a um círculo de pessoas	74-75; 77	Eventual deteção e correção de falhas, como frisa a CNPD.	Para além dos vários testes em curso está prevista a realização de um teste piloto, circunscrito a um número de pessoas mais alargado, que permitirá a eventual correção de falhas.
38-39	Riscos de localização utilizador através de BLE	17; 58	Ainda que o estado ativo da interface Bluetooth torne o dispositivo "visível", o endereço MAC não permite identificar diretamente o utilizador na medida em que o recetor apenas "vê" identificadores pseudoaleatórios. Para associar estes identificadores ao utilizador e com isso, posteriormente, conseguir uma reidentificação a partir deles, o recetor necessitará de criar uma ocasião de suficiente isolamento do utilizador, eventualmente com recurso a fontes de informação secundárias. Além disso, a aplicação STAYAWAY COVID usa a API GAEN, a qual recorre ao Bluetooth LE Privacy, disponível desde a versão 4.2 do Bluetooth. O Bluetooth LE Privacy permite a utilização de endereços MAC aleatórios temporários (com duração de cerca de 15 minutos), o que limita eventuais cenários de rastreio e reidentificação à duração do endereço MAC temporário. A utilidade da aplicação STAYAWAY COVID exige a interface Bluetooth ativa nas ocasiões em que a proximidade, em linha de vista, do utilizador com outra pessoa é de aproximadamente 2 metros. Este requisito é explicita e frontalmente apresentado ao utilizador e solicitado, também explicita e previamente, o seu consentimento para a utilização da interface Bluetooth. Posteriormente, e em qualquer momento, é dada ao utilizador, de forma simples, a opção de suspender a utilização da	N/A

			interface Bluetooth por parte da aplicação e com isso cessar a emissão de quaisquer dados.	
40; 91-92	Transmissão de sinais ativos contém identificadores únicos	58	A aplicação STAYAWAY COVID usa a API GAEN, a qual recorre ao Bluetooth LE Privacy sempre que os dispositivos a suportem, sendo que a versão 4.2 do Bluetooth já tem mais de 4 anos. O Bluetooth LE Privacy permite a utilização de endereços MAC temporários (com duração de cerca de 15 minutos), o que limita eventuais cenários de rastreio e reidentificação à duração do endereço MAC temporário.	N/A
41; 91-92	Endereço MAC da interface Bluetooth	58	Tanto o GAEN bem como os módulos de comunicação, onde é implementado o Bluetooth LE Privacy e feita a respetiva gestão de endereços MAC temporários aleatórios, são ambos parte integrante do sistema operativo. A difusão de dados Bluetooth em iOS ou Android é sempre efetuada através do sistema operativo, seja utilizada a API GAEN ou implementado um protocolo ao nível da aplicação, pelo que não será, portanto, impossível à Google e Apple, na implementação dos sistemas operativos, seguir as cadeias de RPI, mesmo que não seja usada a API GAEN. Ao nível da aplicação não é possível, no entanto, detetar ou evitar que tal aconteça.	N/A
47-50; 89	Sistema GAEN pode ser alterado	N/A	N/A	Qualquer alteração realizada na API GAEN será imediatamente notificada aos utilizadores, de modo que compreendam claramente as consequências das modificações.
53	Descarregar aplicação necessita de conta Google ou Apple	N/A	A Google e Apple, na sua respetiva loja de aplicações, recolhem informações sobre as aplicações descarregadas pelos utilizadores, tais dados são utilizados para a elaboração de históricos de download dos utilizadores, históricos e sugestões de pesquisa e estatísticas de utilização dessas plataformas. Contudo, considera-se mais seguro disponibilizar a app só em lojas oficiais, evitando a disponibilização da app pela web, o	Nas campanhas de informação sobre o sistema, desejavelmente associadas a campanhas de sensibilização para uma boa e responsável utilização de recursos informáticos, deve ser dada visibilidade suficiente à forma como deve ser descarregada a app, a fim de minimizar o risco de ataques de versões falsificadas, cuja difusão já é dificultada pelo facto de apenas poder ser descarregada em lojas oficiais.

			que poderia facilitar a difusão de versões falsificadas.	
54; 91-92	RPI têm associada a data	21-22	Os RPIs são gerados com base nas respetivas Chaves de Identificadores TEK e no intervalo durante os quais são válidos. Os RPIs e os referidos intervalos são difundidos pelos DMPs. A utilização e divulgação dos intervalos temporais juntamente com os RPIs tem como principal objetivo mitigar ataques de repetição: evita que um atacante possa gravar e enviar mais tarde RPIs de utilizadores diagnosticados com COVID-19 com o objetivo de criar falsos positivos (falsos alertas). Os intervalos temporais recebidos são também usados para calcular o período de armazenamento dos RPI, que são apagados ao fim de 14 dias.	N/A
55	Exatidão dos dados após teste com resultado negativo	N/A	No protocolo atual das autoridades de saúde, o teste negativo não é definitivo e implica o acompanhamento da pessoa testada com a marcação de um novo exame. Neste sentido, um teste negativo não deverá, por si, justificar a transição para o estado de "sem risco". Não havendo confirmação do estado de infetado, a aplicação transita para o estado "sem risco" ao fim de 14 dias.	N/A
56; 91-92	Dados tratados no SLD: data dos primeiros sintomas ou a data do teste no caso de indivíduos assintomáticos - a finalidade desta informação.	27-30	A obtenção da data dos primeiros sintomas ou de teste para assintomáticos, destina-se a limitar os contactos que poderão receber avisos de exposição aos que ocorreram após a data de 2 dias antes da referida data, que corresponde ao consenso atual sobre o período pré-sintomático em que há a possibilidade de contágio. O critério das 48 horas está em consonância com a Norma de Rastreio de Contactos da DGS. Quando se trata de um caso assintomático, é da responsabilidade do médico usar a data do teste ou determinar a data mais adequada. A data é inserida pelo profissional de saúde no SLD para emissão do CL. Após ter sido inserida, esta data só pode ser obtida com o conhecimento do CL,	N/A

			que é apenas do conhecimento do doente e do médico. Por exemplo, imagine-se que um cidadão tem os primeiros sintomas no dia 19, faz o teste no dia 20 e recebe os resultados no dia 21. A aplicação tem a possibilidade de enviar Chaves de Identificadores TEK para o SPD desde o dia 7, ou seja, 14 dias antes. No entanto, o profissional de saúde irá emitir um CL com a data de 19, pelo que a aplicação estará autorizada apenas a publicar chaves desde o dia 17. Desta forma não são publicadas chaves de dias cuja infeção não é confirmada pelo profissional, correspondentes aos contactos entre os dias 7 e 17, minimizando-se significativamente a partilha de pseudónimos e bem assim de potenciais falsos positivos (falso alertas) em obediência ao princípio da privacidade por omissão. Os registos de dados para o CL e do CA, guardados no SLD, tem uma validade de 24 horas. Após terem expirado a validade, são apagados pela tarefa diária de manutenção. Acrescente-se o seguinte detalhe de implementação: o dispositivo móvel (DMP) do utilizador autentica-se no SPD através do CA e envia as Chaves de Identificadores TEK geradas desde a data designada "*onset*", a qual é a data introduzida pelo médico no SLD subtraída de dois dias (de acordo com a Norma de rastreio da DGS). A data *onset* fica guardada no SLD antes mesmo de o utilizador receber o CL. O DMP recebe esta data como parte do CA e envia para o SPD as chaves TEK relevantes, isto é, entre "*onset date*" e a data atual, inclusivamente. Estas são as chaves TEK publicadas pelo SPD para o utilizador em causa.	
57	Autenticação dos profissionais de saúde para obter CL	23-24	O sistema utilizado para o acesso ao SLD será o Trace COVID-19, atestando-se a categoria profissional com recurso ao Portal de Requisição de Vinhetas e Receitas (PRVR). Este sistema de autenticação dos médicos é gerido pela SPMS.	N/A

58-59; 91-92	Dados processados no SLD e no SPD	27-30	O identificador único universal (uuid) é produzido pelo SLD como parte do CA. É armazenado no SPD quando o CA é usado para publicar dados e usado depois para garantir que cada CA não é usado mais do que uma vez dentro do seu período de validade. Para o efeito, é eliminado pela tarefa diária de manutenção da base de dados após o fim da sua validade, que é no máximo de 24 horas.	N/A
60-62; 92	Armazenamento dos dados IP	30	N/A	Está previsto ser implementado o mecanismo reverse proxy e a segregação de funções
64	Inteligibilidade da informação prestada ao utilizador	47-48	A informação disponibilizada procurará ser o mais concisa e inteligível quanto possível, seguindo as melhores práticas na matéria, por forma a assegurar de modo eficaz a compreensão das funcionalidades da aplicação e dos limites à sua utilização, tendo em consideração o universo alargado e diversificado de possíveis utilizadores, que poderão incluir crianças.	N/A
71; 74	Designação de responsável pelo tratamento	N/A		O Decreto-Lei 52/2020 de 11 de agosto designa a DGS como entidade responsável pelo tratamento de dados.
71; 93	Intervenção do profissional de saúde no sistema	23-24	A título processual, o circuito previsto ao nível da intervenção dos médicos contempla os seguintes passos descritos, melhor descritos no ponto 2.8 da AIPD: • Os médicos responsáveis pela legitimação acedem ao Trace COVID-19; • Mediante verificação de caso confirmado, o médico (validado pelo PRVR) seleciona a opção disponível para geração de CL. • O médico insere a data dos primeiros sintomas ou data do teste (em caso de utente assintomático). • O Trace COVID-19 autentica-se no SLD recorrendo a um token e pede um Código de Legitimação (CL), indicando a data identificada no ponto anterior.	N/A

			• O SLD valida o token, gera o CL e respetivo Código de Acesso (CA) e envia o CL ao TC-19. • O CL (código com 12 algarismos) é apresentado ao médico numa caixa específica da interface gráfica do TC-19. • O médico transmite o CL ao utilizador da aplicação STAYAWAY COVID, através de um canal externo, para que este o possa inserir no seu telemóvel. • O utilizador insere o CL no DMP, o qual usa o CL para se autenticar no SLD e obter o respetivo CA. • O dispositivo móvel (DMP) do utilizador autentica-se no SPD através do CA e envia as Chaves de Identificadores TEK relevantes que são as geradas desde a data "*onset*". • A data *onset* é a data introduzida pelo médico subtraída de dois dias (de acordo com a Norma de rastreio da DGS) no SLD • O DMP recebe esta data como parte do CA e envia para o SPD as chaves TEK relevantes, isto é, entre "*onset date*" e a data atual, inclusivamente. Estas são as chaves TEK publicadas pelo SPD para o utilizador em causa.	
71; 82-84; 95	Interoperabilidade da aplicação na UE	N/A	Ainda por definir. Será abordado numa futura revisão do AIPD.	N/A
76-78; 93	Enquadramento legal da utilização e designação do responsável pelo tratamento	N/A		O Decreto-Lei 52/2020 de 11 de agosto dá enquadramento legal à utilização do STAYAWAY COVID, estabelecendo a DGS como o responsável pelo tratamento de dados e regulando a intervenção do médico no sistema.
80; 81; 94	Dupla condição de licitude	42-45	A STAYAWYAY seguirá de perto as orientações veiculadas pelas autoridades europeias quanto ao fundamento de licitude de tratamento de dados no âmbito de aplicações com a mesma finalidade, bem como a deliberação da CNPD quanto à pertinência em assegurar um duplo fundamento de licitude, como reforço da legitimidade e proporcionalidade das operações	Está previsto implementar um mecanismo para a prestação de consentimento prévio à instalação da aplicação, cumprindo com os requisitos de validade previstos no RGPD.

			de tratamento de dados levadas a cabo.	

Rastreio de proximidade pan-europeu com preservação de privacidade

O sistema STAYAWAY COVID resultou de uma iniciativa, levada a cabo no âmbito do programa INCoDe.2030, com o objetivo de desenvolver uma solução de rastreio digital de contactos para prevenir e mitigar a propagação da COVID-19. Este sistema, baseado na utilização estritamente voluntária de uma aplicação para dispositivos móveis pessoais, destina-se a ser mais uma ferramenta ao serviço de uma estratégia global de resposta à pandemia causada pelo vírus SARS-CoV-2. A principal funcionalidade da aplicação é alertar o seu utilizador de exposições, consideradas de elevado risco (Organização Mundial de Saúde), a outros utilizadores da aplicação a quem foi entretanto diagnosticada a COVID-19. Em rigor, mais do que de uma solução de rastreio, trata-se de um sistema de notificação da exposição individual a fatores de risco de contágio. Nessa medida servirá de complemento aos esforços já levados a cabo pelas autoridades de saúde para rastrear e interromper as cadeias de transmissão da doença.

O sistema foi concebido com a constante preocupação de conciliar a sua utilidade e eficácia com a segurança intrínseca e a preservação da privacidade dos utilizadores. Este equilíbrio, norteou, desde o início, as opções de arquitetura que determinam a transmissão, armazenamento e processamento dos dados em todo o sistema.

A solução proposta decorre do trabalho de investigação desenvolvido no projeto DP^3T (https://arxiv.org/abs/2005.12273), do qual resultou um kit de desenvolvimento (SDK (https://https://github.com/DP-3T) que implementa todo o protocolo de geração de chaves aleatórias, difusão e receção de identificadores aleatórios, avaliação de risco de contactos, etc. e que é o núcleo da aplicação móvel e dos servidores auxiliares necessários. Muitas destas funcionalidades necessárias às aplicações móveis foram posteriormente integradas pela Google e pela Apple nos seus sistemas operativos, através do que chamamos hoje a GAENAPI, ou seja, a Google-Apple Exposure Notification API. O projeto DP^3T produziu então uma versão "despida" do SDK, na qual tudo que passou a ser oferecido pelos sistemas operativos Android e IOS é neles delegado. Como outras aplicações móveis desenvolvidas e em desenvolvimento em diversos países da Europa, aSTAYAWAY COVID faz uso do SDK DP^3T para acesso à GAEN API e para garantir a interoperabilidade com estas outras aplicações europeias.

Rastreio digital de contactos

No quadro de uma doença infeto-contagiosa, o rastreio de contactos, normalmente efetuado de forma física e presencial, visa identificar as pessoas com quem alguém diagnosticado com a doença teve contacto próximo e recente e, portanto, a quem poderá ter sido criado um elevado risco de infeção.

Um sistema digital de rastreio de contactos, tem como objetivo complementar o protocolo habitual dos serviços de saúde, acrescentando ao levantamento dos contactos recentes baseado na memória e no conhecimento da pessoa doente,um conjunto de contactos relevantes mas omissos, seja por esquecimento ou por desconhecimento.

Os desafios colocados a um sistema digital de rastreio de contactos são muitos e diversos. Os principais, e que mais diretamente relevam para os cidadãos, são a sua confiabilidade, o respeito pela privacidade individual e a comodidade de utilização.

De uma forma sucinta e muito simplificada, o sistema STAYAWAY COVID depende de uma aplicação móvel instalada nos telemóveis que, simultaneamente, emite identificadores únicos e, como um radar, recolhe os identificadores únicos emitidos pelos telemóveis próximos. Na posse dos identificadores recebidos, é simples para a aplicação verificar se o telemóvel no qual está instalada esteve próximo de um determinado telemóvel se lhe for fornecido um dos identificadores por ele emitido. Desta forma, permite-se à aplicação de cada utilizador, se lhe for fornecido um identificador gerado pelo telemóvel de alguém doente, avaliar se terá estado em contacto com esse telemóvel e se este contacto representa ou não risco de contágio.

Para que esta abordagem simples possa configurar uma solução eficaz e segura, é necessário: que os riscos de identificação de alguém sejam minimizados; que a associação de identificadores a diagnósticos positivos da doença seja legitimada por uma autoridade de saúde; que a avaliação sobre um contacto de risco seja o mais precisa possível, de acordo com a diretrizes da Organização Mundial de Saúde; que todos os dados manipulados respeitem as leis europeias e nacionais sobre proteção de dados; e que a utilização do sistema seja o menos intrusiva e mais cómoda possível para as pessoas.

Neste documento, é apresentada uma explicação detalhada do funcionamento dos três componentes de software que constituem o sistema STAYAWAY COVID. Para cada um, apresentamos o modo como a implementação procura responder aos desafios colocados. Para uma análise completa sobre a forma como são satisfeitos os requisitos e respeitadas as leis europeias e nacionais sobre proteção de dados, deverá ser consultada a Análise de Impacto sobre a Proteção de Dados do sistema STAYAWAY COVID.

A aplicação móvel

A aplicação móvel foi inicialmente desenvolvida adotando o algoritmo “Low-cost decentralized proximity tracing”, descrito em (https://arxiv.org/abs/2005.12273) sobre o SDK DP^3T. Posteriormente, com a disponibilização da funcionalidade “Exposure Notification” pelos sistemas operativos iOS e Android, a aplicação deixou de ter a sua própria implementação passando a usar a disponibilizada pelo sistema operativo que segue a versão “Hybrid decentralized proximity tracing”. O acesso à GAEN API é feito através do SDK DP^3T, mantendo-se a arquitetura e funcionalidade de todo o sistema uniforme a todas as aplicações baseadas no projeto DP^3T.

No que se refere ao rastreio de contactos, e do ponto de vista algorítmico, a aplicação gera identificadores aleatórios a que chamamos RPI (Rolling Proximity Identifier) e difunde-os usando o protocolo de comunicação Bluetooth Low Energy (BLE - https://dl.acm.org/doi/book/10.5555/3181282) implementado e acessível apenas através do sistema operativo. Simetricamente, escuta, usando a mesma interface de comunicação, e guarda identificadores recebidos de outros dispositivos a executar a aplicação STAYAWAY COVID.

Para a geração dos RPI é seguido o método a seguir exposto. Diariamente, é gerada uma chave aleatória de 360 bit a que chamamos TEK (Temporary Exposure Key). Cada dia t, com base na chave TEKt, é gerado um número aleatório de 144 x 16 bytes usando um gerador pseudo-aleatório do tipo Advanced Encryption Standard, que recebe como argumento uma função pseudo-aleatória do tipo HMAC-SHA256 que, por sua vez, recebe a chave TEKt como argumento (para uma descrição pormenorizada, ver a especificação criptográfica da Google e Apple) . Este número aleatório de 144 x 16 bytes fornece, de facto, 144 RPI de 16 bytes que o telemóvel

difunde e troca cada 10 minutos. Ao trocar de RPI cada 10 minutos a aplicação dificulta o seguimento ou reconhecimento dos dispositivos durante o dia. Cada dispositivo mantém armazenadas localmente as TEK dos últimos 14 dias, eliminando automaticamente as mais antigas.

Do lado da escuta, os RPI recebidos são armazenados juntamente com a data da receção e parâmetros que permitem avaliar a relevância do contacto, tais como a atenuação estimada do sinal recebido e a duração do estabelecimento da ligação entre dispositivos. Esta informação é armazenada apenas localmente e por um período máximo de 14 dias.

No caso do utilizador ser diagnosticado com COVID-19, a aplicação, por ação explícita do utilizador, envia para o servidor a que chamamos Servidor de Publicação de Diagnóstico (SPD) as chaves TEK geradas nos últimos 14 dias. Para que a aplicação possa fazer este envio, o seu utilizador terá primeiro que obter um código especial, a que chamamos Código de Legitimação, e de que falaremos adiante. Uma vez publicadas a TEK a aplicação cessa permanentemente a partilha de RPI e, consequentemente, a sua funcionalidade principal.

Em todos os outros casos, a aplicação, até duas vezes por dia, sem hora certa, acede ao SPD e descarrega as chaves TEK aí disponíveis até ao limite de 14 dias anteriores. Uma vez obtidas as chaves TEK, para cada uma gera os respetivos 144 RPI. Para cada RPI, efetua uma comparação com os RPI entretanto armazenados (RPI com, no máximo, 14 dias). Havendo coincidências, avalia, usando uma função parametrizável quanto à atenuação do sinal e ao tempo de estabelecimento de ligação, se o contacto deve ou não ser considerado de elevado risco. Se o for, alerta de imediato o utilizador. O alerta refere apenas que houve um contacto de proximidade suscetível de elevado risco de contágio. Nenhuma outra informação é diretamente revelada, sendo ainda assim viável determinar o dia a que se refere o alerta produzido. A aplicação permanece no estado de alerta durante 14 dias voltando ao estado normal se, entretanto, não for introduzido o código CL e submetidas ao SPD as chaves TEK.

Se a versão inicial da aplicação, versão DP^3T, incluía todos estes procedimentos, com a disponibilização e adoção da GAEN API vários procedimentos passaram a ser invocados ao sistema operativo. A saber, a geração das chaves TEK, a geração e difusão dos identificadores RPI, a receção e armazenamento dos identificadores RPI e, a verificação e avaliação de contactos, passaram a ser implementadas pelo sistema operativo e, como tal, inacessíveis às aplicações.

Dos protocolos DP^3T, a aplicação STAYAWAY COVID limita-se agora a invocar a inicialização das funcionalidades de “Exposure Notification”, obter as TEK para, em caso de necessidade, as enviar para o SPD, descarregar as TEK do SPD e submetê-las ao sistema operativo, e reagir à eventual notificação de contacto de risco. A função de avaliação de existência de contacto de risco é parametrizável pela aplicação usando limites máximos e mínimos para a atenuação do sinal e os tempos de exposição. A partir dos contactos detetados, a aplicação faz uma análise de risco e determina se esses contactos representam risco elevado de contágio avisando, em caso afirmativo, o utilizador. Esta análise de risco de contágio, em contínua revisão, segue resultados de estudos que podem ser encontrados aqui.

Perante as condições de utilização dos seus sistemas operativos, a Apple e a Google não deixam alternativa ao uso da GAEN API às aplicações de rastreio de contactos da COVID-19. Não utilizando a GAEN API a aplicação, para difundir e receber beacons BLE, os RPI, terá que estar a executar em primeiro plano (em foreground). Esta limitação, insuportável por qualquer

aplicação instalada num dispositivo móvel, foi e ainda é a principal causa de não utilização de algumas das soluções de rastreio de contactos em vários países.

Pela positiva, a uniformização de um protocolo de difusão BLE comum aos dois sistemas operativos que dominam o mercado dos telemóveis, a capacidade de teste das duas empresas (com maior relevância no caso da Google) na miríade de modelos de telemóveis existentes e a criação de modelos de calibração dos sinais no envio e receção de BLE entre eles, é algo que não estaria ao alcance de iniciativas individuais nacionais.

Do ponto de vista puramente técnico, a implementação da aplicação STAYAWAY COVID sobre a GAEN API, para além de inevitável, foi manifestamente vantajosa.

O Servidor de Legitimação de Diagnóstico

A cada utilizador diagnosticado com COVID-19, é solicitado que partilhe as suas chaves TEK dos últimos 14 dias com os restantes utilizadores do sistema. Com o acesso a estas chaves TEK, a aplicação de cada um dos outros utilizadores poderá gerar os correspondentes RPI e avaliar se tiveram lugar contactos considerados de elevado risco.

O sistema tem de assegurar que apenas utilizadores com diagnóstico positivo à COVID-19 partilham as suas chaves TEK. Desta garantia depende a confiabilidade do sistema enquanto auxiliar de rastreio de contactos com COVID-19.

Para que tal seja assegurado, a partilha das chaves TEK de um utilizador tem que ser acompanhada de uma "legitimação" efetuada pelo médico responsável pelo diagnóstico. O sistema STAYAWAY COVID implementa esta garantia através de um código, a que chamamos Código de Legitimação (CL) que é fornecido ao utilizador, pelo médico, junto com o diagnóstico. Este código é um número de 12 algarismos que o utilizador pode receber verbalmente ou por qualquer forma de mensagem eletrónica (SMS, email, etc.) e que permite à aplicação aceder de forma legitimada e segura ao servidor que publica as chaves TEK de pessoas diagnosticadas com COVID-19.

O servidor de legitimação de diagnóstico (SLD) atende dois tipos de pedidos: por parte do médico para obtenção de um CL, e por parte da aplicação de um utilizador para obtenção de um certificado de acesso (CA) para aceder ao servidor de publicação de diagnóstico (SPD, descrito a seguir).

Quando acedido por um médico, o SLD requer que o pedido seja previamente autenticado de forma a garantir que tem origem num profissional de saúde autorizado a obter códigos CL. Esta autenticação é, em Portugal, efetuada através do cartão de cidadão ou da cédula profissional do médico. Além da autenticação, é solicitada ao médico data estimada dos primeiros sintomas do doente. O SLD gera um CL e um CA, e devolve o CL ao médico que, por sua vez, o transmite ao doente.

O utilizador introduz o CL na aplicação STAYAWAY COVID que, por sua vez, obtém o CA junto do SLD e com esse certificado acede ao servidor de publicação de diagnóstico (SPD). O CA (um certificado standard JWT) contém codificada a data estimada dos primeiros sintomas do doente subtraída de 3 dias (valor configurável pelas autoridades de saúde), que corresponde ao início do período em que há um maior risco de contágio. Munida do CA, a aplicação STAYAWAY COVID coloca no SPD as chaves TEK armazenadas no dispositivo (no máximo até 14 dias).

O SLD permite assim que apenas chaves TEK de utilizadores diagnosticados com COVID-19 pelas entidades de saúde possam partilhar as suas chaves TEK. A identidade do médico não chega ao SPD e não é, portanto, nunca conhecida por este. Analogamente, a aplicação apresenta-se ao SLD com o CL e nada mais. O CL e correspondente CA são válidos durante 24 horas. Passado este período ou logo que reclamado o CA, o par é eliminado do servidor.

De forma a garantir que a aplicação entrega o CL apenas ao verdadeiro SLD e que não é suscetível a ataques to tipo man-in-the-middle, o certificado do SLD é conhecido previamente e usado para validar todas as interações com o SLD (certificate pinning). As aplicações simulam também, aleatoriamente, a troca de CL por CA no SLD, de forma a dificultar eventuais tentativas de identificação dos utilizadores através da análise do tráfego na rede.

Como o acesso ao SLD por parte dos utilizadores não é autenticado, este servidor é sensível a acessos abusivos para obtenção de um CA existente por força-bruta ou para saturação e consequente quebra de serviço. A mitigação de ambos os ataques é efetuada recorrendo a técnicas simples mas comprovadas, que seguem as melhores práticas de segurança.

O Servidor de Publicação de Diagnóstico

Por fim, descrevemos o servidor de publicação de diagnóstico (SPD) no qual são partilhadas as chaves TEK dos utilizadores diagnosticados com COVID-19. Este servidor é acedido por estes utilizadores, na posse de um certificado de acesso (CA) obtido previamente no SLD. Ao receber as TEK do utilizador junto com o CA, o SPD guarda apenas as chaves TEK do dia indicado na data codificada no CA (data estimada dos primeiros sintomas do doente subtraída de 2 dias) e posteriores. Apenas estas chaves TEK serão partilhadas, pois, segundo as autoridades de saúde, as anteriores não relevam para a avaliação dos contactos de risco. Qualquer chave TEK é preservada no SPD por um período de 14 dias, no máximo. Neste passo, a aplicação valida o certificado do SPD (certificate pinning) de forma a garantir que as chaves TEK não são intercetadas por qualquer intermediário. As aplicações simulam também, aleatoriamente, a entrega de chaves TEK ao SPD de forma a dificultar eventuais tentativas de identificação dos utilizadores através da análise do tráfego na rede.

As aplicações de todos os outros utilizadores acedem ao SPD duas vezes por dia, para obter novas chaves TEK que tenham sido publicadas. Com essas novas chaves procedem à avaliação de contactos de risco. A informação publicada contendo as chaves TEK é assinada pelo SPD, de forma a que a sua origem possa ser validada. Com a GAEN esta validação e avaliação é da responsabilidade do sistema operativo. Além disso, como precaução adicional, a aplicação valida também o certificado do SPD.

A escrita de chaves TEK no servidor é autenticada através do CA. O acesso a estas chaves é público e proporcional ao número de utilizadores ativos. Para assegurar a resposta atempada, os acessos ao SPD por parte das aplicações são distribuídos no tempo e o SPD está equipado com mecanismos de replicação e caching.

Riscos e eficácia

Para minimizar os riscos de identificação dos utilizadores do sistema, em momento algum são utilizados dados pessoais. Aos RPI (Rolling Proximity Identifier), chamamos identificadores porque, apesar de serem gerados aleatória e independentemente de dados pessoais, em última análise servem para identificar alguém de quem foi recebido um RPI com alguém de quem foi recebida uma chave TEK do SPD. Ainda que, dentro do sistema, não seja possível associar o RPI

a uma pessoa concreta, nem sequer ao seu dispositivo móvel, essa relação anónima existe e por isso no AIPD do STAYAWAY COVID são tratados os TEK e os RPI como dados pessoais.

No sistema STAYAWAY COVID os TEK e o RIP não podem ser associados, por nenhuma das entidades envolvidas, a pessoas concretas. São, no entanto, conhecidas técnicas ilegítimas que o permitiram fazer. Um dos tipos destas técnicas baseia-se na criação de cenários onde, sem o conhecimento ou autorização do utilizador, são recolhidos dados de identificação, como imagens ou impressões digitais, enquanto são recolhidos e associados a estes dados RPI do seu dispositivo móvel. O outro, baseia-se na capacidade de implantar um sistema massivo de sensores BLE geolocalizados que constantemente recolhem e armazenam todos os RPI que recebem. Por si, esta informação não é relevante devido à natureza dinâmica dos RPI. No entanto, uma vez publicadas as chaves TEK de uma pessoa, seria possível traçar os seus percursos dos últimos dias e, eventualmente, identificá-la.

Para lá do interesse teórico destes "ataques" ao sistema não existem, até ao momento, evidências de riscos significativos da sua ocorrência.

O rastreio digital de contactos, como auxiliar ao rastreio epidemiológico habitual, foi algo despoletado pela pandemia de COVID-19 no início deste ano, a nível mundial. Independentemente das tecnologias existentes, o ainda incompleto conhecimento das formas de propagação do vírus, apenas nos permitem simular a eficácia da abordagem com simulações simplificadas e pressupostos mais ou menos conservadores mas, ainda assim, passíveis de serem desadequados.

A utilização de Bluetooth Low Energy como medida indireta para avaliação de distância (para implementar a avaliação de risco sugerida inicialmente pela Organização Mundial de Saúde e depois conserva doramente alargada por vários países) foi e é um recurso, na falta de quaisquer outras alternativas. O BLE não foi desenvolvido para medir distância nem nunca terá sido usado com esse propósito antes da COVID-19. Apesar disso, e não sendo ainda conhecidas alternativas concretas, apesar da investigação na matéria, para o problema em mãos (medição de distância aproximadas de 2 metros) e depois do enorme trabalho efetuado na análise dos muitos dispositivos móveis existentes e na calibração de resultados, a tecnologia em si não parece ser o maior obstáculo.

No entanto, uma vez que não existe ainda uma experiência consolidada com este tipo de aplicações, a sua eficácia está por determinar. As potenciais vantagens e desvantagens foram avaliadas por painéis científicos a nível internacional que informaram os decisores políticos de vários países dentro e fora da União Europeia. As decisões políticas tomadas na grande maioria dos países Europeus, incluindo Portugal, vai no sentido de lançar este tipo de aplicações, tendo em conta os potenciais benefícios no controlo da pandemia.

Salvaguardados os receios de respeito pela privacidade e havendo uma compreensão por parte dos utilizadores do significado dos eventuais alertas da aplicação, a abordagem só poderá ser benéfica, ainda que possa nunca atingir a eficácia esperada ou desejada.

Anexos

Anexo A – Acesso ao SLD para geração de CL por médico

Os profissionais de saúde acedem ao Trace COVID-19 e efetuam a sua autenticação com recurso à autenticação Office 365, atestando-se a sua categoria profissional através do Portal de Requisição de Vinhetas e Receitas (PRVR). O PRVR contém informação de todos os médicos registados na Ordem, independentemente de exercerem funções no setor público ou no setor privado. A confirmação da categoria profissional provém da relação direta entre o médico que está com a sessão aberta no Trace COVID-19 e o PRVR, sendo atestada através do seu número de ordem profissional.

O utilizador seleciona a opção disponível para geração de CL e, mediante verificação de que é um médico habilitado, abre-se uma janela própria para a introdução da data dos primeiros sintomas ou data do teste (em caso de utente assintomático). O Trace COVID-19 autentica-se no SLD através de um *token* e pede um CL, indicando a data introduzida anteriormente. O SLD valida o *token* recebido, gera o CL e o respetivo CA e envia o CL para o Trace COVID-19. Garante-se, assim, o princípio da separação entre o SLD e o sistema Trace COVID-19, em benefício da privacidade dos utilizadores.

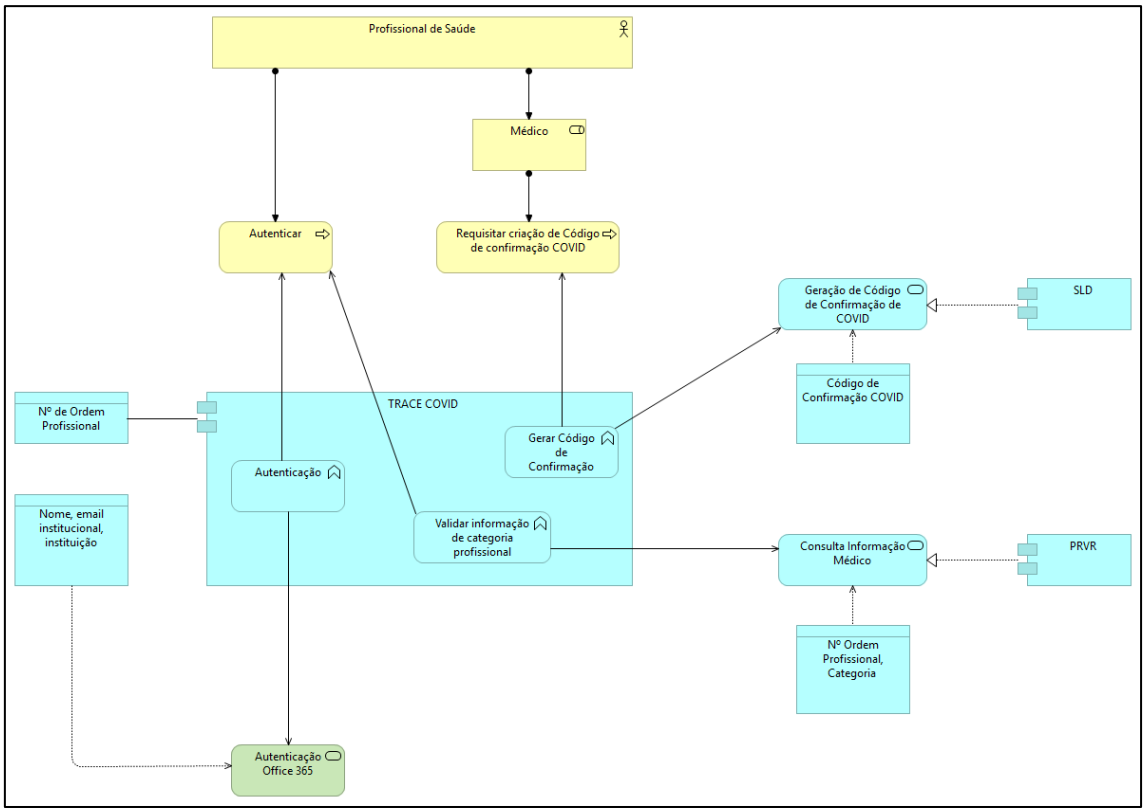


Figura 13 - Validação do médico no PRVR

O médico observa o CL numa caixa específica da interface gráfica do Trace COVID-19, enviando este código de 12 algarismos para o utilizador da aplicação STAYAWAY COVID através de um canal externo.

Após o utilizador inserir o CL na aplicação STAYAWAY COVID, o dispositivo móvel pessoal (DMP) usa o CL para autenticar-se no SLD e para obter o respetivo CA. Através do CA, o DMP autentica-se no SPD e envia as Chaves de Identificadores TEK geradas desde a data designada "*onset*", a qual é a data introduzida pelo médico subtraída de dois dias (de acordo com a Norma de Rastreio de Contactos da DGS). Esta data *onset* fica guardada no SLD antes de o utilizador receber o CL.

O dispositivo do utilizador recebe esta data no CA e envia para o SPD as chaves TEK relevantes, isto é, entre *"onset date"* e a data atual, inclusivamente. Estas são as chaves TEK publicadas pelo SPD para o utilizador em causa.