Sábado, 20 de junho de 2020

I Série
Número 73

BOLETIM OFICIAL

ÍNDICE

CONSELHO DE MINISTROS

Resolução nº 86/2020

de 20 de junho

A calamidade pública de natureza sanitária vivida por Cabo Verde, provocada pela COVID-19, justificou por parte dos órgãos de soberania nacionais a unanimidade de entendimento de que se tratava de um quadro excecional, que exigia medidas apenas admissíveis num contexto de estado de emergência, declarado nos termos constitucionais.

A 28 de março de 2020, através de um aturado processo de ponderação e auscultação de todos os atores constitucionalmente relevantes, o Presidente da República decidiu decretar o estado de emergência, por se ter considerado necessário reforçar a cobertura constitucional a medidas mais abrangentes e efetivamente mais restritivas, que se revelavam importantes adotar para combater uma situação cada vez mais emergencial.

No quadro do estado de emergência, decidira-se pela restrição à liberdade de circulação, ao direito ao trabalho efetivo e aos direitos dos trabalhadores, à propriedade e à iniciativa privada, ao direito de reunião e de manifestação e à liberdade de culto, no seu âmbito coletivo, sempre balizados pelos princípios da proporcionalidade e adequação.

Essas medidas, entretanto, foram excecionais e temporárias, em virtude dos seus efeitos nefastos em quase todas as esferas da vida pessoal e coletiva, dos interesses públicos e privados.

Tendo o Estado o dever de garantir o direito à saúde individual e de defender a saúde pública face à capacidade exponencial de propagação do vírus;

Observando sempre o núcleo irredutível do direito à reserva da vida pessoal e familiar e do direito à proteção de dados, consagrados no n.º 2 do artigo 41° e artigo 45º da Constituição;

Estando o país, ainda a lutar para conter o avanço da doença;

Enquadrado numa estratégia ampla integrada de implementação de medidas, condições e procedimentos que visam mitigar a disseminação do SARS-CoV-2 em virtude da retoma da normalidade, após o fim do estado de emergência no país;

Estando concomitantemente a decorrer a campanha de massificação de testes de despiste da COVID-19, nos diferentes bairros e nas comunidades;

Reconhecendo a existência de interesse público importante, no caso, a prestação de cuidados de saúde pública, conforme consagrado na Constituição da República; e

De modo a complementar a capacidade de atuação das autoridades sanitárias, na esteira daquilo que tem sido a experiência noutras paragens, o Governo entende por bem acolher a proposta de um grupo de cidadãos nacionais para o desenvolvimento de uma aplicação de rastreamento de contactos de proximidade, sustentada no protocolo aberto DP-3T (*Decentralized Privacy - Preserving Proximity Tracing*), para a sua utilização em Cabo verde no âmbito da gestão da pandemia, como parte da resposta à COVID-19 nesta fase de desconfinamento, em que o risco de relaxamento das medidas de autoproteção é maior, ciente de que soluções tecnológicas levantam, naturalmente, preocupações com a privacidade.

A proposta do grupo de cidadãos é pública e de forma expressa é manifestada como uma oferta da cidadania, como expressão da vontade de dotar o país, para exploração pelas autoridades sanitárias nacionais, de uma ferramenta tecnológica moderna, devidamente customizada e adaptada à nossa realidade.

Por outro lado, e não obstante o rastreamento de contactos ser ainda uma tecnologia em fase de desenvolvimento e amadurecimento, o quadro jurídico de proteção de dados em vigor em Cabo Verde é forte e garante uma resposta eficaz na proteção dos direitos humanos e das liberdades fundamentais, sendo indispensável a proteção de dados para construir a confiança, criar as condições de aceitação social de qualquer solução e, assim, promover a sucesso desta medida.

A tecnologia quando usada para a combater a COVID-19 tem por objetivo capacitar, em vez de controlar, estigmatizar ou reprimir indivíduos. A este respeito, a utilização da aplicação de rastreamento de contactos deve ser opcional, voluntária e não deve depender do rastreamento de movimentos individuais, mas sim de informações de proximidade sobre os utilizadores.

Os princípios gerais de eficácia, necessidade e proporcionalidade devem orientar a opção pelo tratamento automatizado de dados pessoais para combater a doença e nesse sentido, as soluções tecnológicas têm limitações que lhes são intrínsecas e apenas podem alavancar outras medidas de saúde pública, seguindo uma estratégia global e integrada.

Pretende-se, pois, aprovar um conjunto de orientações que clarificam as condições e princípios para a utilização proporcionada da tecnologia para fins específicos de rastreamento de contactos, de notificação de indivíduos que estiveram próximos de alguém que foi confirmado como portador do vírus, a fim de, rapidamente, quebrar a cadeia de contaminação.

A eficiência da contribuição das aplicações de rastreio de contactos para a gestão da pandemia depende, contudo, de muitos fatores, desde logo da percentagem de pessoas que a irão instalar, da definição de «contacto» em termos de proximidade e duração, e da capacidade de interoperabilidade do aplicativo.

A sua implementação deve ser acompanhada de medidas de apoio para garantir que as informações fornecidas aos utilizadores sejam contextualizadas e que os alertas possam ser úteis ao sistema público de saúde.

Foram solicitados os pareceres prévios da Comissão Nacional de Proteção de Dados sobre o aplicativo de rastreamento de proximidade, o qual se pretende que venha a chamar-se "*NaNosMon*", bem relativo à presente Resolução.

Assim,

Nos termos do n.º 2 do artigo 265º da Constituição, o Governo aprova a seguinte Resolução:

Artigo 1º

Aprovação e adoção

1. É aprovado o rastreamento de contactos de proximidade, que tem por objetivo determinar quem esteve próximo a uma pessoa infetada e, assim, permitir o rastreamento do percurso do SARS-CoV-2 e a contenção da propagação.

2. É adotada a solução tecnológica "*NaNosMon*", enquanto aplicativo nacional para o rastreamento de contactos de proximidade.

3. É, ainda, aprovado o regulamento de implementação, utilização e gestão do aplicativo nacional de rastreamento de contactos de proximidade, em anexo à presente Resolução, da qual faz parte integrante.

Artigo 2º

Entrada em vigor

A presente Resolução entra em vigor no dia seguinte ao da sua publicação.

Aprovada em Conselho de Ministros, aos 18 de junho de 2020. — O Primeiro-Ministro, *José Ulisses de Pina Correia e Silva.*

ANEXO

(A que se refere o nº 3 do artigo 1º)

REGULAMENTO DE IMPLEMENTAÇÃO, UTILIZAÇÃO E GESTÃO DO APLICATIVO NACIONAL DE RASTREAMENTO DE CONTACTOS DE PROXIMIDADE.

Artigo 1º

Âmbito

O presente regulamento estabelece as condições e princípios para a realização proporcionada do rastreamento de contactos de indivíduos que estiveram próximos de alguém confirmado como portador do vírus, os procedimentos de obtenção, transmissão e proteção de dados, as medidas adicionais de segurança, os mecanismos de implementação, comunicação e de acompanhamento e, designa a equipa técnica de execução.

Artigo 2º

Definições

Para efeitos do presente regulamento, entende-se por:

a) "Contacto" - um utilizador que teve uma interação com um utilizador confirmado como portador do vírus, e cuja duração e distância permitem deduzir um risco de exposição significativa à infeção.

b) "Computação em nuvem" – é a tecnologia que permite guardar dados na internet através de um servidor *online* sempre disponível, em que o usuário pode armazenar arquivos, documentos e outras informações, sem precisar de um disco rígido no seu computador, podendo a nuvem pode ser:

i. Pública - quando compartilha recursos e oferece serviços ao público em geral através da internet;

ii. Privada - quando não é compartilhada e oferece serviços numa rede interna privada, geralmente hospedada localmente;

iii. Híbrida - quando compartilha serviços entre nuvens públicas e privadas, de acordo com o seu propósito.

c) "Dados de localização" - todos os dados tratados numa rede de comunicações eletrónicas ou por um serviço de comunicações eletrónicas que indique a posição geográfica do dispositivo móvel de um utilizador de um serviço de comunicações eletrónicas publicamente disponível, bem como dados de outras potenciais fontes, relativos à latitude, longitude ou altitude do equipamento terminal, à direção da viagem do utilizador, ou ao momento em que as informações de localização foram registadas.

d) "Dados pessoais de saúde" - dados pessoais relacionados com o estado de saúde de uma pessoa singular, incluindo informações recolhidas durante a inscrição para a prestação de serviços de saúde ou durante a prestação do serviço de saúde, que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro.

e) "Interação" - troca de informações entre dois dispositivos localizados na proximidade um do outro (no espaço e no tempo), dentro da gama da tecnologia de comunicação utilizada (p. ex., *bluetooth*). Esta definição exclui dados de localização.

f) "Localização do contacto" - é uma metodologia de controlo da doença que lista todas as pessoas que estiveram na proximidade de um portador do vírus, a fim de verificar se estão em risco de infeção e tomar as medidas sanitárias adequadas.

g) "Portador do vírus" - os utilizadores que foram testados positivos para o vírus, mediante teste laboratorial e que receberam um diagnóstico oficial de médico ou estabelecimento de saúde.

h) "Pseudonimização" - o tratamento de dados pessoais de forma a que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

i) "Anonimização" - utilização de medidas para impossibilitar a associação direta ou indireta dos dados ao indivíduo, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa, sendo que os dados anonimizados, por regra, não são considerados dados pessoais na medida em que o potencial de reidentificação é residual.

j) "Upload" - corresponde à ação de enviar dados a partir de um computador ou outro equipamento local, para um computador ou servidor remoto, geralmente através da internet.

Artigo 3º

Finalidade

1 - O aplicativo nacional de rastreamento tem como única e exclusiva finalidade o rastreamento de contactos de pessoas potencialmente expostas ao vírus SARS-CoV-2 para que possam ser alertadas, testadas e cuidadas.

2 - A finalidade do tratamento de dados referida no número anterior é específica e exclui o tratamento para outros fins, nomeadamente para efeitos de controlo do cumprimento das medidas de quarentena, de confinamento e de distanciamento social, de localização e identificação dos seus utilizadores ou de construção de mapas de proximidade globais.

Artigo 4º

Infraestrutura

1 - A infraestrutura de suporte ao aplicativo assenta na existência de um dispositivo móvel de comunicação, um servidor de *backend* e um portal de gestão de permissões.

2 - O dispositivo de comunicação é um aparelho *smartphone* equipado com *bluetooth* e que executa o aplicativo de rastreamento de contactos.

3 - O servidor de *backend* atua como arquivo do histórico das interações das pessoas infetadas, onde essa informação é disponibilizada para consulta dos demais subscritores do aplicativo.

4 - O processo de *upload* dos dados é voluntário e é despoletado pela pessoa infetada, ao introduzir o código disponibilizado para esse efeito.

5 - O portal de gestão de permissões atua como interface da autoridade da saúde, a partir da qual é gerado o código único, pseudonimizado, atribuído à pessoa infetada e que lhe permite o *upload* dos identificadores anónimos e efémeros decorrentes dessas interações, no servidor de *backend,* fazendo com que todos os utilizadores que estiveram em contacto com o portador do vírus recebam um alerta, sem nunca se saber quem é o contacto dessa cadeia ou a sua localização.

Artigo 5º

Consentimento do titular de dados

1 - Entende-se por «consentimento do titular dos dados», qualquer manifestação de vontade, livre, específica, informada e inequívoca, nos termos da qual aceita que os seus dados pessoais sejam objeto de tratamento, nos termos da alínea *h*) do n.º 1 do artigo 5° do regime jurídico geral de proteção de dados pessoais, aprovado pela Lei nº 133/V/2001, de 22 de janeiro, alterada pela Lei n.º 41/VIII/2013 de 17 de setembro

2 - O consentimento só é livre se o titular dos dados o puder recusar ou revogar sem ficar prejudicado.

3 - O consentimento informado pressupõe um ato positivo inequívoco e impõe que o responsável pelo tratamento dos dados atue com transparência quanto a todas as vicissitudes do tratamento, podendo, assim, garantir maior confiança ao funcionamento do aplicativo e a adesão da população.

4 - Quando o utilizador do aplicativo tiver menos de dezasseis anos, o consentimento apenas é fundamento para o tratamento de dados se for autorizado pelo seu representante legal.

Artigo 6º

Participação voluntária

1 - A instalação e a utilização do aplicativo de rastreamento é um ato voluntário e implica o consentimento do titular dos dados.

2 - Nos termos do número anterior, a utilização ou não utilização do aplicativo não implica consequências negativas e é garantido o cumprimento do princípio de igualdade de tratamento.

3 - O utilizador do aplicativo tem total controlo sobre os seus dados pessoais, em todos os momentos e é capaz de decidir livremente sobre a sua instalação, utilização ou desinstalação, cessando de imediato o rastreio.

Artigo 7º

Princípio da proporcionalidade

1- Os dados tratados devem ser adequados, pertinentes e não excessivos para efeitos de rastreamento de contactos, sendo absolutamente vedado o tratamento de dados não relacionados ou não necessários à prossecução da finalidade, designadamente sobre o estado civil, sexo, identificadores de comunicação, itens de diretório de equipamentos, dados de localização, identificadores do dispositivo ou outros.

2- Os dados de registo no dispositivo e no servidor de *backend* devem ser minimizados e cumprir com os requisitos da proteção de dados.

Artigo 8º

Princípio da limitação da conservação dos dados

Os dados devem ser conservados pelo tempo estritamente necessário à gestão da crise, finda a qual devem ser destruídos.

Artigo 9º

Obtenção de dados

1 - O aplicativo deve utilizar exclusivamente o *Bluetooth Low Power* como tecnologia de comunicação de proximidade para o registo das interações.

2 - Os parâmetros de duração da exposição e distância entre pessoas e que determinam quando uma interação deve ser registada na lista de rastreamento de contactos são fixados pelas autoridades de saúde e devem ser definidos no aplicativo.

3 - O aplicativo deve manter o histórico das interações de um utilizador no seu respetivo equipamento, por um período de tempo limitado, predefinido, nunca superior a vinte e um dias.

4 - Por iniciativa dos utilizadores notificados como infetados e após confirmação do seu estado pelas autoridades de saúde, o seu histórico de contactos ou seus próprios identificadores são transmitidos ao servidor de *backend*.

Artigo 10º

Transmissão de dados

1 - Os dados a transmitir entre os dispositivos dos utilizadores ou entre esses dispositivos e o servidor de *backend* são dados únicos, pseudonimizados, gerados pelo próprio aplicativo e em nenhum caso incluem dados de identificação dos dispositivos.

2 - Os certificados digitais para a transmissão dos dados referidos no número anterior devem ser renovados regularmente de forma a restringir os riscos de identificação dos utilizadores a que dizem respeito, de rastreamento dos seus movimentos ou da sua ligação a outros utilizadores.

Artigo 11º

Validade dos dados e duração do aplicativo

1 - O aplicativo é uma ferramenta complementar às técnicas tradicionais de rastreamento de contactos, nomeadamente entrevistas com pessoas infetadas e como tal deve ser usada apenas até que as técnicas de rastreamento de contactos por intervenção humana possam gerir a quantidade de novas infeções.

2 - Sem prejuízo do estabelecido no número anterior, a conservação dos dados nos dispositivos móveis ou no servidor de *backend*, deve ser limitada em função da verdadeira necessidade e da relevância médica.

3 - O Ministério da Saúde e da Segurança Social, enquanto entidade responsável pelo tratamento dos dados, deve instituir um procedimento para interromper a troca de identificadores e eliminar os dados recolhidos dos telefones e no servidor de *backend*, o mais tardar até ao fim da situação excecional de pandemia.

4 - O procedimento referido no número anterior, deve incluir a possibilidade de desativação global do aplicativo, a desinstalação automática e ainda instruções para os utilizadores a desinstalarem.

Artigo 12º

Proteção dos dados pessoais e privacidade

1 - O intercâmbio de dados deve respeitar a privacidade dos utilizadores e em especial, respeitar o princípio da minimização dos dados.

2 - O aplicativo deve garantir que os dados de identificação dos utilizadores e os seus movimentos não são rastreados.

3 - O aplicativo deve garantir a segurança dos dados de outros utilizadores, especialmente dos portadores do vírus.

4 - A gestão do servidor de *backend* e do portal de gestão de permissões deve seguir regras de gestão claramente definidas e incluir todas as medidas necessárias para garantir a segurança dos equipamentos.

5 - O servidor de *backend* e o portal de gestão de permissões devem ficar alojados na infraestrutura tecnológica da rede privativa do Estado, ainda que em nuvem, de forma a permitir uma supervisão eficaz por parte das autoridades de controlo competentes.

6 - O aplicativo revela ao utilizador se foi exposto ao vírus, sem revelar outras informações, nomeadamente sobre data, hora, lugares ou identificadores de utilizadores.

7 - Os *linkage attacks* não devem ser possíveis.

8 - A desinstalação do aplicativo deve resultar na eliminação de todos os dados recolhidos localmente.

9 - O aplicativo só deve recolher dados transmitidos por instâncias do aplicativo ou aplicações equivalentes interoperáveis, sendo vedada a recolha de dados de outras aplicações ou de outros dispositivos de comunicação de proximidade.

10 - Para evitar a reidentificação pelo servidor de *backend*, devem ser implementadas medidas acrescidas de segurança que possibilitem, nomeadamente, a mistura dos identificadores dos vários utilizadores, antes de partilhá-los.

11 - Quer o aplicativo, quer o servidor de *backend* devem ser cuidadosamente desenvolvidos e configurados para só recolherem os dados necessários à finalidade pretendida.

12 - Nenhum identificador deve ser incluído nos *logs* de acesso ao servidor de *backend*.

Artigo 13º

Entidade responsável pelo tratamento de dados

1 - Nos termos da alínea *d*) do n.º 1 do artigo 5° do regime jurídico geral de proteção de dados pessoais das pessoas singulares, o responsável pelo tratamento de dados é a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais.

2 - O responsável pelo tratamento de dados é quem assegura a conformidade da implementação e utilização do aplicativo, com as exigências legais e regulamentares aplicáveis, nomeadamente, a obrigação de notificação prevista no artigo 23º do referido regime, e demais obrigações, junto da Comissão Nacional de Proteção de Dados (CNPD) e perante os titulares dos dados.

3 - Tendo em consideração a categoria de dados tratados, dados pessoais de saúde no âmbito do combate a pandemia da COVID-19, o Ministério da Saúde e da Segurança Social é a entidade responsável pelo tratamento dos dados pessoais, concretamente através da Direção Nacional da Saúde e do Instituto Nacional de Saúde Pública.

4 - As atribuições e as responsabilidades das entidades referidas nos termos do número anterior devem ser claramente estabelecidas desde o início e explicados aos utilizadores.

5 - O Núcleo Operacional da Sociedade de Informação (NOSI) coopera com a entidade responsável pelo tratamento de dados, enquanto subcontratante, para efeitos do cumprimento do nº 2 e de realização de auditorias e inspeções, desde que devidamente mandatado.

6 - A subcontratação referida no número anterior deve ser formalizada sob a forma de um contrato ou outro ato jurídico que o vincule ao responsável pelo tratamento de dados, nos termos do nº 4 do artigo 15º do regime jurídico geral de proteção de dados pessoais das pessoas singulares e do parecer da CNPD.

Artigo 14º

Obrigações do responsável pelo tratamento de dados

1 - O responsável pelo tratamento de dados tem, pelo menos, as seguintes obrigações:

a) Pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizado, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito;

b) Dar instruções ao subcontratante, informar e aconselhar os técnicos que tratam os dados a respeito das suas obrigações nos termos do presente regulamento e do regime jurídico geral de proteção de dados pessoais das pessoas singulares;

c) Controlar a conformidade com o presente regulamento, com outras disposições e políticas relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados e às auditorias correspondentes;

d) Prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto do aplicativo sobre a proteção de dados e controlar a sua realização;

e) Cooperar com a autoridade de fiscalização;

f) Ser ponto de contacto para qualquer assunto relativo à aplicação, nomeadamente, junto à autoridade de fiscalização, sobre questões relacionadas com o tratamento e consulta de dados.

2 - No desempenho das suas funções, o responsável pelo tratamento de dados, tendo em devida consideração os riscos associados às operações de tratamento, bem como a natureza, o âmbito, o contexto e as finalidades do presente tratamento, deve tomar as medidas adequadas e acrescidas de segurança da informação de modo a evitar a reidentificação dos titulares a quem os dados pseudonimizados objeto de tratamento se referem.

3 - Sempre que tenha conhecimento de uma violação de dados pessoais, o responsável pelo tratamento deve notificá-la à autoridade de fiscalização, sem demora injustificada.

Artigo 15º

Procedimentos de envio de lista de contactos ao servidor de *backend*

Quando o dispositivo móvel envia para o servidor de *backend* uma lista de contactos:

a) O servidor só pode recolher o histórico de contactos dos portadores de vírus, na sequência de ações voluntárias destes portadores;

b) Os históricos de contactos armazenados no servidor devem ser apagados no prazo de 72 (setenta e duas) horas depois dos utilizadores serem notificados da sua proximidade com um portador de vírus;

c) Nenhuma informação deve sair do equipamento do utilizador, salvo quando um portador de vírus partilha com o servidor o histórico dos seus contactos ou quando um utilizador pede ao servidor informação sobre sua potencial exposição ao vírus;

d) Qualquer identificador incluído no histórico do dispositivo móvel deve ser apagado após 21 (vinte e um) dias contados da data da sua recolha;

e) Os históricos de contacto enviados por utilizadores diferentes não devem ser tratados, nomeadamente, para construir mapas de proximidade globais.

Artigo 16º

Funcionalidades

1 - O aplicativo deve dispor de uma funcionalidade que permita aos utilizadores saber se foram potencialmente expostos ao vírus, sendo esta informação baseada na proximidade de um portador do vírus, infetado dentro de uma janela de um número determinado de dias, antes da confirmação do diagnóstico positivo.

2 - O aplicativo deve fornecer recomendações aos utilizadores identificados como tendo estado potencialmente expostos ao vírus.

3 - O aplicativo deve transmitir instruções sobre as medidas que devem seguir, nomeadamente, recomendar o contacto com a linha de informação gratuita 800 11 12, destinada à prestação de informação e assistência aos cidadãos sobre a doença ou que se dirijam a um determinado local para fazerem testes à COVID-19.

4 - O conteúdo das recomendações e instruções referidas nos números anteriores deve ser aprovado pelas autoridades de saúde.

5 - O algoritmo que mede o risco de infeção tendo em conta fatores de distância e tempo, determinando quando uma interação tem de ser registada na lista de contactos, deve ser sujeito a permanente atualização, tendo em conta os conhecimentos mais recentes sobre a propagação do vírus.

6 - Os utilizadores devem ser notificados caso tenham sido expostos ao vírus ou devem poder obter regularmente informação sobre se foram ou não expostos ao vírus, durante o período de incubação.

7 - O aplicativo deve ser interoperável com outras aplicações desenvolvidas em outros países, de modo a que os utilizadores que viajam por diferentes países, passam ser notificados de forma eficiente.

8 - A interoperabilidade referida no número anterior depende de autorização prévia da CNPD e da adequação do aplicativo estrangeiro com este regulamento e com o regime jurídico geral de proteção de dados pessoais.

Artigo 17º

Segurança

1 - A comunicação da condição de infetado com SARS-CoV-2 no aplicativo implica o consentimento da pessoa, enquanto titular dos dados, ou do seu representante legal, caso seja menor de 16 (dezasseis) anos

2 - O aplicativo integra um mecanismo de confirmação dos utilizadores que consentem reportar-se positivos, através de um código em 12 dígitos ou em *QR code*, único, pseudonimizado, intransmissível, gerado no portal de gestão de permissões e formalmente entregue ao titular dos dados pelas autoridades de saúde.

3 - Os dados enviados para o servidor de *backend* devem ser transmitidos através de um canal seguro.

4 - Técnicas criptográficas de última geração devem ser implementadas para garantir trocas entre o aplicativo e o servidor, entre dispositivos e para proteger as informações armazenadas nos dispositivos e no servidor de *backend*.

5 - Podem ser usadas técnicas que incluem criptografia simétrica e assimétrica, criptografia homomórfica, funções de *hashing*, testes de pertença a base de dados, cálculo privado da interseção de bases de dados e *bloom filters*.

6 - O servidor de *backend* não deve manter identificadores de conexão de rede (p.ex., endereços IP) de qualquer utilizador, incluindo aqueles que foram diagnosticados positivamente e que transmitiram o seu histórico de contactos ou os seus próprios identificadores.

7 - A fim de evitar a representação ou a criação de utilizadores falsos, o servidor de *backend* deve autenticar o aplicativo e vice-versa.

8 - As funcionalidades do servidor devem ser protegidas de contra-ataques de repetição.

9 - A comunicação com o servidor de *backend* deve ser certificada digitalmente.

10 - Ao responsável pelo tratamento de dados incumbe o dever de informar, de forma clara e explícita, sobre como e onde deve ser descarregado o aplicativo nacional de rastreamento de contactos, a fim de diminuir o risco de utilização de aplicações de terceiros.

Artigo 18º

Equipa técnica de execução

1 - A equipa técnica multidisciplinar para a execução do processo de implementação do aplicativo, nas suas diferentes fases, é constituída por representantes do:

a) Grupo de cidadãos promotor da iniciativa, enquanto responsável pela solução tecnológica;

b) NOSI, enquanto parceiro e o garante do *compliance* tecnológico;

c) Instituto Nacional de Saúde Pública; e da

d) Direção Nacional da Saúde.

2 - Atribuições da equipa técnica:

a) Coordenar a execução do processo de implementação do aplicativo;

b) Gerir o ciclo de vida e garantir o suporte e a manutenção;

c) Garantir o cumprimento da desativação global e/ou da desinstalação automática, quando se justificar;

d) Definir os indicadores de avaliação de eficácia;

e) Validar a eficácia do aplicativo, do ponto de vista da saúde pública, com base em indicadores pré-estabelecidos;

f) Definir as etapas de ativação gradual, por municípios e ilhas;

g) Manter atualizado o algoritmo utilizado na medição do risco de infeção;

h) Propor iniciativas de comunicação.

Artigo 19º

Fases de execução

1 - A execução do processo de implementação do aplicativo obedece às seguintes fases:

a) Prova de conceito;

b) Teste piloto;

c) Ativação geral.

2 - A prova de conceito identifica erros ou vulnerabilidades na arquitetura do *software*, sem que hajam impactos na proteção de dados.

3 - A prova de conceito determina a viabilidade técnica do modelo do aplicativo e a conformidade com o presente regulamento e com o regime jurídico geral de proteção de dados pessoais.

4 - O teste piloto valida as condições técnicas, metodológicas e administrativas, inerentes ao projeto e avalia o funcionamento do aplicativo em ambiente real controlado.

5 - O teste piloto compreende as etapas de:

a) Aprovação pelas autoridades de saúde do conteúdo das recomendações, instruções e notificações geradas pelo aplicativo;

b) Definição do código único, pseudonimizado, para envio de dados ao servidor de *backend;*

c) Aprovação do protocolo de entrega do código único e do respetivo modelo de termo de entrega;

d) Definição e calibragem do algoritmo de medição do risco de contágio;

e) Formação dos Delegados de Saúde na utilização do portal de gestão de permissões;

f) Inventariação dos indicadores de avaliação de eficácia;

g) Disponibilização do aplicativo na *play store da Google e na app store da Apple*;

h) Testes de integração da infraestrutura (dispositivo móvel, portal de gestão de permissões e servidor de *backend*);

i) Testes de performance, qualidade, segurança e de conformidade da arquitetura do sistema.

6 - A ativação geral compreende as diferentes etapas de ativação do aplicativo, de forma gradual, por municípios e ilhas, de modo a reduzir ao mínimo o impacto na proteção de dados.

Artigo 20º

Transparência e comunicação

1 - A informação e comunicação destinada ao público ou aos titulares dos dados, relativa ao aplicativo e o seu funcionamento deve ser concisa, de fácil acesso e compreensão, formulada numa linguagem clara e simples e, na medida do possível, com recurso aos meios audiovisuais, para que o utilizador e titular dos dados saiba e compreenda, como e para que fins os seus dados pessoais são recolhidos.

2 - Essas informações podem ser fornecidas por via eletrónica, nomeadamente num sítio da internet, quando se destinarem ao público.

3 - Compete à entidade responsável pelo tratamento de dados, definir e implementar planos e campanhas de informação e comunicação ao público, relativamente à utilização do aplicativo e prestar as informações que couberem sobre o seu funcionamento.

4 - Nos termos do número anterior, cabe à entidade responsável pelo tratamento de dados promover todas as ações de comunicação relativas ao aplicativo.

Artigo 21º

Código-fonte

O código-fonte do aplicativo deve ser aberto e as especificações técnicas devem ser tornadas públicas, para que seja auditável e se for caso disso, se possa contribuir para melhorar o código, corrigir possíveis erros e garantir a transparência no tratamento dos dados pessoais.

Artigo 22º

Direito de acesso

O titular dos dados tem o direito de obter do responsável pelo tratamento, livremente e sem restrições, com periodicidade razoável e sem demoras ou custos excessivos, o acesso aos mesmos e à retificação, nos termos do regime jurídico geral de proteção de dados pessoais das pessoas singulares.

Artigo 23º

Direito de oposição e de apagamento

1 - O titular dos dados pode opor-se, a qualquer momento, ao tratamento dos seus dados desinstalando o aplicativo.

2 - A desinstalação do aplicativo leva à eliminação dos dados alojados localmente no *smartphone* e no *backend*, bem como à cessação imediata do rastreio.

Artigo 24º

Obrigação de notificação

A entidade responsável pelo tratamento dos dados pessoais deve notificar a CNPD, antes da realização do tratamento ou conjunto de tratamentos, enviando para o efeito o modelo do aplicativo customizado e adaptado à realidade nacional, bem como os protocolos de implementação, avaliação, comunicação e o relatório da prova de conceito, nos termos do parecer nº 11/2020, de 26 de maio, da CNPD.

———

Resolução nº 87/2020

de 20 de junho

A empreitada de expansão e modernização do Porto Inglês na Ilha do Maio, enquadra-se no programa de modernização das infraestruturas portuárias do país, lançado pelo governo e atualmente em curso, com vista a assegurar serviços de melhor qualidade, conforto e segurança.

O contrato de prestação de serviços de fiscalização adjudicado ao consórcio de empresas SCET-TUNISIE/NORVIA CV tem por objetivo assegurar, junto do Ministério das Infraestruturas, Ordenamento do Território e Habitação, os serviços de controlo de qualidade e custos financeiros e do cumprimento das regras de segurança e higiene, das obras da empreitada de expansão e modernização do Porto Inglês, financiada pelo Estado de Cabo Verde e pelo Banco Africano de Desenvolvimento.

Assim:

Ao abrigo do disposto na alínea *e*) do n.º 1 do artigo 42º do Decreto-lei n.º 1/2009, de 5 de janeiro, a aplicar por força do disposto no n.º 2 do artigo 3º da Lei n.º 88/VIII/2015, de 14 de abril; e

Nos termos do n.º 2 do artigo 265º da Constituição, o Governo aprova a seguinte Resolução:

Artigo 1º

Autorização

É autorizado ao Ministério das Infraestruturas, do Ordenamento do Território e Habitação a realizar as despesas com a celebração do contrato de prestação de serviços no âmbito de "*SURVEILLANCE ET CONTRÔLE DES TRAVAUX D'EXTENSION ET MODERNISATION DU PORT INGLÊS*", no montante de EUR 1.000.550 (um milhão e quinhentos e cinquenta euros), excluindo Imposto sobre o Valor Acrescentado.

Artigo 2º

Entrada em vigor

A presente Resolução entra em vigor no dia seguinte ao da sua publicação.

Aprovada em Concelho de Ministros, aos 18 de junho de 2020. — O Primeiro-Ministro, *José Ulisses de Pina Correia e Silva.*

I SÉRIE

BOLETIM OFICIAL

Registo legal, nº 2/2001, de 21 de Dezembro de 2001

Endereço Electronico: *www.incv.cv*

IMPRENSA NACIONAL DE CABO VERDE

Av. da Macaronésia,cidade da Praia - Achada Grande Frente, República Cabo Verde
C.P. 113 • Tel. (238) 612145, 4150 • Fax 61 42 09
Email: kioske.incv@incv.cv / incv@incv.cv

I.N.C.V., S.A. informa que a transmissão de actos sujeitos a publicação na I e II Série do *Boletim Oficial* devem obedecer as normas constantes no artigo 28º e 29º do Decreto-Lei nº 8/2011, de 31 de Janeiro.