Jornal Oficial da União Europeia

C 124 I

Edição em língua portuguesa

Comunicações e Informações

63.º ano

17 de abril de 2020

Índice

PT

II

(Comunicações)

COMUNICAÇÕES DAS INSTITUIÇÕES, ÓRGÃOS E ORGANISMOS DA UNIÃO EUROPEIA

COMISSÃO EUROPEIA

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)

1 CONTEXTO

O desafio lançado pela pandemia de COVID-19 é sem precedentes para a União e para os Estados-Membros, assim como para os seus sistemas de saúde, modo de vida, estabilidade económica e sistema de valores. As tecnologias e os dados digitais têm um importante papel a desempenhar na luta contra a crise do coronavírus. As aplicações móveis geralmente instaladas nos telemóveis inteligentes podem apoiar as autoridades de saúde pública, a nível nacional e da UE, na monitorização e contenção da pandemia de COVID-19, sendo particularmente relevantes na fase de levantamento das medidas de contenção. Além de poderem orientar diretamente os cidadãos, podem também apoiar o esforço de rastreio de contactos. Há já vários países, na UE e a nível mundial, em que as autoridades nacionais ou regionais e os programadores anunciaram o lançamento de aplicações móveis com diferentes funcionalidades para apoiar a luta contra o vírus.

Em 8 de abril de 2020, a Comissão adotou uma recomendação relativa a um conjunto de instrumentos comuns a nível da União com vista à utilização de tecnologias e dados para combater a COVID-19 e sair da crise, nomeadamente no respeitante às aplicações móveis e à utilização de dados de mobilidade anonimizados (a «recomendação») ([1]). A recomendação visa, nomeadamente, a adoção de uma abordagem comum para a utilização das aplicações móveis («conjunto de instrumentos»), coordenada ao nível da UE, de modo a permitir aos cidadãos tomarem medidas eficazes de distanciamento social e servindo também para alertar, prevenir e rastrear os contactos, a fim de limitar a propagação da COVID-19. A recomendação estabelece os princípios gerais que devem nortear o desenvolvimento desse conjunto de instrumentos e indica que a Comissão publicará orientações mais pormenorizadas, nomeadamente sobre a proteção dos dados pessoais e as implicações da utilização deste tipo de aplicações em matéria de privacidade.

A Comissão, em cooperação com o Presidente do Conselho Europeu, definiu, a partir do roteiro europeu comum para o levantamento das medidas de contenção ligadas ao COVID-19, um conjunto de princípios para orientar a eliminação progressiva das medidas de contenção tomadas para fazer face ao surto de coronavírus. As aplicações móveis, incluindo as funcionalidades de rastreio de contactos, podem desempenhar um papel importante neste contexto. Dependendo das suas características e do seu nível de utilização pela população, estas aplicações podem ter um impacto significativo no diagnóstico, tratamento e gestão da doença do coronavírus 2019, dentro e fora do meio hospitalar. Estas aplicações são particularmente relevantes quando são levantadas as medidas de contenção e o risco de infeção aumenta, à medida que cada vez mais pessoas entram em contacto umas com as outras. Podem ajudar a interromper as cadeias de infeção, de forma mais rápida e eficaz do que as medidas gerais de contenção, e contribuir para reduzir significativamente o risco de propagação do vírus. Devem, por conseguinte, constituir um elemento importante da estratégia de saída, complementando outras medidas como o aumento da capacidade de realização de testes de diagnóstico ([2]). A confiança nelas depositadas é uma importante condição prévia do desenvolvimento, aceitação e utilização destas aplicações pelos cidadãos. As pessoas precisam de ter a certeza de que estas aplicações respeitam os direitos fundamentais e de que serão utilizadas apenas para os fins especificamente definidos, que não serão usadas para vigilância em larga escala e que os cidadãos manterão o

([1]) Recomendação C(2020) 2296 final de 8 de abril de 2020. https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf.

([2]) https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

controlo sobre os seus dados. Esta é a base para a exatidão e a eficácia destas aplicações na contenção da propagação do vírus. Por conseguinte, é essencial identificar as soluções que sejam menos intrusivas e plenamente conformes com os requisitos em matéria de proteção dos dados pessoais e da privacidade definidos no direito da UE. Além disso, as aplicações móveis devem ser desativadas, o mais tardar quando a pandemia for declarada sob controlo. Estas aplicações devem também incluir as proteções de segurança da informação mais avançadas.

As presentes orientações têm em conta a contribuição do Comité Europeu para a Proteção de Dados (CEPD) ([3]) e os debates no âmbito da rede de saúde em linha (e-Saúde) e do CEPD. O CEPD planeia publicar orientações nos próximos dias sobre a geolocalização e outros instrumentos de rastreio no contexto do surto de COVID-19.

Âmbito das orientações

Para garantir uma abordagem coerente em toda a UE e fornecer orientações aos Estados-Membros e aos criadores de aplicações móveis, este documento define as características e os requisitos que as aplicações devem satisfazer para garantir o cumprimento da legislação da UE em matéria de proteção da privacidade e dos dados pessoais, em especial o Regulamento Geral sobre a Proteção de Dados ([4]) (RGPD) e a Diretiva Privacidade Eletrónica ([5]). As presentes orientações não tratam de quaisquer outras condições, incluindo as limitações que os Estados-Membros possam ter incluído nas suas legislações nacionais no que respeita ao tratamento dos dados relativos à saúde.

Estas orientações não são juridicamente vinculativas. São sem prejuízo do papel desempenhado pelo Tribunal de Justiça da UE, única instituição que pode fazer uma interpretação vinculativa do direito da União.

As presentes orientações incidem apenas nas aplicações móveis de utilização voluntária para apoio na luta contra a pandemia de COVID-19 (aplicações descarregadas, instaladas e utilizadas voluntariamente pelos cidadãos) com uma ou várias das seguintes funcionalidades:

— fornecimento de informações exatas aos cidadãos sobre a pandemia de COVID-19;

— fornecimento de questionários para autoavaliação e orientação dos cidadãos (funcionalidade de controlo de sintomas) ([6]);

— alerta das pessoas que tenham estado na proximidade de uma pessoa infetada durante determinado período de tempo, de modo a fornecer informações como a recomendação de autoquarentena ou a indicação dos locais de realização de testes de diagnóstico (funcionalidades de rastreio de contactos e alerta);

— criação de um fórum de comunicação para médicos e pacientes em situação de autoisolamento e para os casos em que é prestado aconselhamento ulterior em matéria de diagnóstico e de tratamento (maior utilização da telemedicina).

De acordo com a Diretiva Privacidade e Comunicações Eletrónicas, a imposição da utilização de uma aplicação móvel que atinja o direito à confidencialidade das comunicações previsto no artigo 5.º só é possível através de uma medida legislativa que seja necessária, adequada e proporcionada, para proteger determinados objetivos específicos. Tendo em conta o elevado grau de ingerência de uma tal abordagem e os desafios em causa, nomeadamente no que se refere à adoção das salvaguardas adequadas, a Comissão considera que será necessário realizar uma análise cuidada antes de recorrer a esta opção. Por estas razões, a Comissão recomenda que essas aplicações sejam de utilização voluntária.

As presentes orientações não abrangem as aplicações móveis que visam fazer cumprir os requisitos em caso de quarentena (incluindo os requisitos de cumprimento obrigatório).

2 CONTRIBUIÇÃO DAS APLICAÇÕES MOVEIS NA LUTA CONTRA A COVID-19

A funcionalidade de controlo de sintomas é um instrumento que servirá para as autoridades de saúde pública orientarem os cidadãos para a realização de testes ao coronavírus e fornecerem informações sobre o autoisolamento, sobre como evitar a transmissão a terceiros e quando procurar ajuda médica. Pode também complementar as medidas de vigilância no quadro dos cuidados de saúde primários e informar melhor sobre as taxas de transmissão da COVID-19 na população.

([3]) https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

([4]) 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) (JO L 119 de 4.5.2016, p. 1).

([5]) Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37).

([6]) Se as aplicações móveis fornecerem informações relacionadas com o diagnóstico, a prevenção, a monitorização, a previsão ou o prognóstico, deverá ser avaliada a sua potencial qualificação como dispositivos médicos de acordo com o quadro regulamentar nesta matéria. No respeitante a esse quadro, remete-se para a Diretiva 93/42/CEE do Conselho, de 14 de junho de 1993, relativa aos dispositivos médicos (JO L 169 de 12.7.1993, p. 1) e para o Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos (JO L 117 de 5.5.2017, p. 1).

As funcionalidades de rastreio de contactos e de alerta são instrumentos que servirão para identificar as pessoas que tenham estado em contacto com uma pessoa infetada com COVID-19 e para as informar sobre os passos seguintes adequados, tais como a autoquarentena e a realização de testes de diagnóstico ou para as aconselhar sobre o que fazer em caso de sintomas. Esta funcionalidade é, por conseguinte, útil para os cidadãos e para as autoridades de saúde pública. Além disso, pode desempenhar um papel importante na gestão das medidas de contenção no contexto dos cenários de saída. O seu impacto pode ser reforçado com uma estratégia apoiada na realização de um maior número de testes de diagnóstico às pessoas com sintomas ligeiros.

mbas as funcionalidades podem também ser uma fonte de dados relevantes para as autoridades de saúde pública, além de facilitarem a sua comunicação às autoridades epidemiológicas nacionais e ao Centro Europeu de Prevenção e Controlo das Doenças (ECDC). Tal ajudaria a compreender os padrões de transmissão e, em combinação com os resultados dos testes, estimar o valor preditivo positivo dos sintomas respiratórios numa dada comunidade, bem como fornecer informações sobre o nível de circulação do vírus.

O grau de fiabilidade das estimativas está diretamente relacionado com a quantidade e com a fiabilidade dos dados comunicados.

Por conseguinte, se conjugadas com estratégias de diagnóstico adequadas, as funcionalidades de controlo de sintomas e de rastreio de contactos podem fornecer informações sobre o nível de circulação do vírus e ajudar a avaliar a eficácia das medidas de distanciamento físico e de confinamento. Conforme indicado na recomendação, para permitir a cooperação transfronteiras e garantir a deteção dos contactos entre utilizadores de diferentes aplicações (particularmente importante nos movimentos transfronteiriços de cidadãos), será necessário assegurar a interoperabilidade entre soluções informáticas de diferentes Estados-Membros. Nos casos em que uma pessoa infetada entra em contacto com um utilizador de uma aplicação de outro Estado-Membro, deverá ser possível, na medida do estritamente necessário, a comunicação transfronteiriça dos dados pessoais desse utilizador às autoridades de saúde do seu Estado-Membro. Os trabalhos sobre esta questão farão parte do conjunto de instrumentos anunciado na recomendação. A interoperabilidade deverá ser assegurada por meio de requisitos técnicos e através do reforço da comunicação e cooperação entre autoridades de saúde nacionais. Poderá também ser usado um modelo de cooperação especial ([7]), enquanto modelo de governação das aplicações móveis de rastreio de contactos durante a pandemia de COVID-19.

3 ELEMENTOS PARA UMA UTILIZAÇÃO RESPONSAVEL E EM CONFIANÇA DAS APLICAÇÕES

As funcionalidades incluídas nas aplicações podem ter um impacto diferente num vasto conjunto de direitos consagrados na Carta dos Direitos Fundamentais da UE, como a dignidade do ser humano, o respeito pela vida privada e familiar, a proteção dos dados pessoais, a liberdade de circulação, a não discriminação, a liberdade de empresa e a liberdade de reunião e de associação. A ingerência na privacidade e no direito à proteção dos dados pessoais pode assumir uma relevância especial, uma vez que algumas das funcionalidades assentam num modelo com um uso intensivo de dados.

Os elementos apresentados adiante visam dar orientações sobre a forma de limitar o caráter intrusivo das funcionalidades das aplicações, a fim de assegurar o cumprimento da legislação da UE em matéria de proteção dos dados pessoais e da privacidade.

3.1 As autoridades nacionais de saúde (ou entidades que desempenham funções de interesse público na área da saúde) como responsáveis pelo tratamento

É essencial identificar quem decide dos meios e das finalidades do tratamento de dados (ou seja, o responsável pelo tratamento) para determinar o responsável pelo cumprimento das regras da UE em matéria de proteção de dados pessoais, nomeadamente quem deve informar as pessoas que descarregam a aplicação sobre o que vai acontecer com os respetivos dados pessoais (já existentes ou que serão gerados através do dispositivo, por exemplo, o telemóvel, onde a aplicação está a ser instalada), os direitos que lhes assistirão, quem será responsável em caso de violação de dados, etc.

Dada a sensibilidade dos dados em questão e a finalidade do tratamento de dados abaixo descrito, a Comissão considera que as aplicações devem ser concebidas de modo a que os responsáveis pelo tratamento ([8]) sejam as autoridades nacionais de saúde (ou entidades que desempenham funções de interesse público na área da saúde). Os responsáveis pelo tratamento são responsáveis por assegurar a conformidade com o RGPD (princípio da responsabilidade). O âmbito desse acesso deve ser limitado com base nos princípios descritos adiante, no ponto 3.5.

([7]) Esta cooperação já existe no que respeita ao projeto MyHealth@EU para intercâmbio de processos de doentes e de receitas eletrónicas. Ver também o artigo 5.º, n.º 5, e o considerando 17, da Decisão de Execução 2019/1765 da Comissão.

([8]) Ver o considerando 45 do RGPD.

Tal contribuirá igualmente para um maior confiança da população e, por conseguinte, para uma maior aceitação das aplicações (e dos sistemas de informação sobre cadeias de transmissão da infeção subjacentes) e garantirá que estas cumprem a finalidade prevista de proteção da saúde pública. As políticas subjacentes, os requisitos e os controlos devem ser harmonizados e aplicados de forma coordenada pelas autoridades nacionais de saúde.

3.2 **Assegurar que as pessoas mantêm o controlo**

Para que as pessoas confiem nas aplicações, é fundamental demonstrar-lhes que mantêm o controlo dos seus dados pessoais. Para o efeito, a Comissão considera particularmente importante satisfazer as seguintes condições:

— a instalação da aplicação nos dispositivos deve ser voluntária e não devem existir consequências negativas para a pessoa que decida não a descarregar ou utilizar;

— as diferentes funcionalidades das aplicações (por exemplo, funcionalidades de informação, controlo de sintomas, rastreio de contactos e alerta) não devem ser agrupadas, de modo a permitir que as pessoas possam dar o seu consentimento separado para cada uma das funcionalidades. Tal não deverá impedir o utilizador de combinar diferentes funcionalidades da aplicação, se o fornecedor oferecer essa opção;

— se forem utilizados dados de proximidade (dados gerados pelo intercâmbio de sinais de baixo consumo energético do Bluetooth (BLE) entre dispositivos a uma distância epidemiologicamente relevante e durante um período epidemiologicamente relevante), os dados devem ser armazenados no dispositivo da pessoa. Se esses dados se destinarem a ser partilhados com as autoridades de saúde, só o devem ser depois da confirmação de que a pessoa em causa está infetada com a COVID-19 e na condição de esta escolher fazê-lo;

— as autoridades de saúde devem fornecer às pessoas todas as informações necessárias relacionadas com o tratamento dos seus dados pessoais (em conformidade com os artigos 12.º e 13.º do RGPD e com o artigo 5.º da Diretiva Privacidade Eletrónica);

— a pessoa deve poder exercer os direitos que lhe assistem ao abrigo do RGPD (em particular, acesso, retificação e apagamento). Qualquer restrição dos direitos ao abrigo do RGPD ou da Diretiva Privacidade Eletrónica deve, em conformidade com estes atos, ser necessária, proporcionada e estar prevista na legislação;

— as aplicações devem ser desativadas o mais tardar quando a pandemia for declarada sob controlo; a desativação não deve depender da desinstalação pelo utilizador.

3.3 **Fundamento jurídico para o tratamento**

Instalação das aplicações e armazenamento de informações no dispositivo do utilizador

Como referido acima, ao abrigo da Diretiva Privacidade Eletrónica (artigo 5.º), o armazenamento de informações no dispositivo do utilizador ou a possibilidade de acesso a informações já armazenadas no mesmo são permitidos se i) o utilizador tiver dado o seu consentimento prévio ou ii) o armazenamento e/ou o acesso forem estritamente necessários para fornecer um serviço da sociedade da informação (por exemplo, a aplicação) expressamente solicitado (ou seja, instalado e ativado) pelo utilizador.

Regra geral, o armazenamento de informações no dispositivo da pessoa e a possibilidade de acesso a informações já armazenadas no mesmo são necessários para que as aplicações possam funcionar. As funcionalidades de rastreio de contactos e de alerta requerem igualmente o armazenamento de outras informações (como o nome alternativo, efémero e mudado regularmente, do ID de utilizador dos utilizadores desta funcionalidade na proximidade) no dispositivo da pessoa. Além disso, estas funcionalidades exigem que o utilizador (infetado ou provavelmente infetado) carregue dados de proximidade. Este carregamento não é necessário ao funcionamento da aplicação. Por conseguinte, os requisitos da opção ii) mencionada no parágrafo anterior não são satisfeitos, sendo portanto o consentimento (opção i)) a base mais adequada às atividades relevantes. Este consentimento deve ser «dado de livre vontade», «específico», «explícito» e «informado» na aceção do RGPD. Além disso, deve ser expresso mediante um ato positivo da pessoa, o que exclui formas de consentimento tácito (por exemplo, o silêncio ou a inatividade) ([9]).

([9]) Ver as orientações do Comité Europeu para a Proteção de Dados sobre o consentimento: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Fundamento jurídico para o tratamento pelas autoridades nacionais de saúde – direito europeu ou direito nacional

Habitualmente, as autoridades nacionais de saúde tratam dados pessoais quando existe uma obrigação legal estabelecida no direito da UE ou do Estado-Membro que prevê esse tratamento e que satisfaz as condições previstas no artigo 6.º, n.º 1, alínea c), e no artigo 9.º, n.º 2, alínea i), do RGPD, ou quando esse tratamento é necessário ao exercício de funções de interesse público reconhecido pelo direito da UE ou do Estado-Membro ([10]).

O direito nacional tem de prever medidas específicas e adequadas para salvaguardar os direitos e liberdades dos titulares dos dados. Em princípio, quanto mais forte for o impacto nas liberdades individuais, mais fortes deverão ser as garantias correspondentes previstas no direito aplicável.

As leis da UE e dos Estados-Membros anteriores ao surto de COVID-19 e as leis adotadas pelos Estados-Membros especificamente para combater a propagação da epidemia podem, em princípio, ser usadas como fundamento jurídico para o tratamento de dados pessoais, desde que prevejam medidas que permitam monitorizar a epidemia e satisfaçam os requisitos estabelecidos no artigo 6.º, n.º 3, do RGPD.

Tendo em conta a natureza dos dados pessoais em causa (em especial os dados relativos à saúde que constituem uma categoria especial de dados pessoais), bem como as circunstâncias da atual pandemia de COVID-19, usar uma lei como fundamento jurídico contribuiria para a segurança jurídica, uma vez que i) preveria em pormenor o tratamento de dados relativos à saúde específicos e indicaria claramente as finalidades desse tratamento; ii) determinaria claramente quem é o responsável pelo tratamento, ou seja, a entidade que trata os dados, e quem, para além do responsável pelo tratamento, pode ter acesso a esses dados; iii) excluiria a possibilidade de tratar esses dados com finalidades diferentes das enumeradas na legislação e (iv) preveria salvaguardas específicas. A fim de não comprometer a utilidade pública e a aceitação das aplicações, o legislador nacional deve estar especialmente atento para que a solução escolhida seja o mais inclusiva possível do ponto de vista dos cidadãos.

O tratamento pelas autoridades de saúde com base na lei não altera o facto de as pessoas continuarem a ser livres de instalarem ou não a aplicação e de partilharem ou não os seus dados com as autoridades de saúde. Por conseguinte, a desinstalação da aplicação não deve ter consequências negativas para os utilizadores.

As aplicações de rastreio de contactos e de alerta permitem alertar as pessoas. Nos casos em que o alerta for diretamente emitido pela aplicação, a Comissão chama a atenção para a proibição de submeter as pessoas a uma decisão tomada exclusivamente com base no tratamento automatizado que produza efeitos na sua esfera jurídica ou que a afete significativamente de forma similar (artigo 22.º do RGPD).

3.4 **Minimização dos dados**

Os dados produzidos através de dispositivos e já armazenados anteriormente nesses dispositivos estão protegidos do seguinte modo:

— A título de «dados pessoais», ou seja, qualquer informação relativa a uma pessoa singular identificada ou identificável (artigo 4.º, n.º 1, do RGPD), é protegida ao abrigo do referido regulamento. Os dados relativos à saúde beneficiam de proteção adicional (artigo 9.º do RGPD).

— A título de «dados de localização», ou seja, dados tratados numa rede de comunicações eletrónicas ou por um serviço de comunicações eletrónicas, que indiquem a posição geográfica do equipamento terminal do utilizador, estão protegidos ao abrigo da Diretiva Privacidade Eletrónica (artigo 5.º, n.º 1, artigo 6.º e artigo 9.º) ([11]),

— As informações armazenadas e acessíveis a partir dos equipamentos terminais do utilizador são protegidas ao abrigo do artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica.

Os dados não pessoais (como os dados irreversivelmente anonimizados) não são protegidos ao abrigo do RGPD.

A Comissão recorda que o princípio da minimização dos dados exige que só os dados pessoais que sejam adequados, pertinentes e limitados ao que é necessário em relação à finalidade ([12]), podem ser tratados. Deverá ser efetuada uma avaliação da necessidade de tratar os dados pessoais e a pertinência desses dados pessoais em função da ou das finalidades prosseguidas.

A Comissão observa que, por exemplo, se a finalidade da funcionalidade for o controlo de sintomas ou a telemedicina, tais finalidades não exigem o acesso à lista de contactos da pessoa que é proprietária do dispositivo.

([10]) Artigo 6.º, n.º 1, alínea e), do RGPD.

([11]) O Código das Comunicações Eletrónicas prevê que sejam também abrangidos os serviços funcionalmente equivalentes aos serviços de comunicações eletrónicas.

([12]) Princípio da minimização dos dados.

A produção e o tratamento de menos dados limitam os riscos de segurança. Por conseguinte, a conformidade com as medidas de minimização dos dados confere também garantias de segurança.

— Funcionalidade de informação:

Uma aplicação apenas com esta funcionalidade não precisa de tratar quaisquer dados relativos à saúde das pessoas. Limita-se a fornecer-lhes informações. Para cumprir esta finalidade, não pode ser processada qualquer informação armazenada e acessível a partir do equipamento terminal além do necessário para fornecer as informações.

— Funcionalidades de controlo de sintomas e telemedicina:

Se a aplicação incluir uma ou duas destas funcionalidades, tratará os dados pessoais em matéria de saúde. Por conseguinte, deve ser especificada uma lista de dados que podem ser tratados na legislação subjacente aplicável às autoridades de saúde.

Além disso, as autoridades de saúde podem necessitar dos números de telefone das pessoas que utilizaram a verificação de sintomas e carregado os resultados. As informações armazenadas e acessíveis a partir de equipamentos terminais só podem ser tratadas na medida em que sejam necessárias para permitir à aplicação cumprir a sua finalidade e permitir o seu funcionamento.

— Funcionalidade de rastreio de contactos e de alerta:

A maioria das infeções por COVID-19 ocorre através de gotículas que atingem uma distância limitada. Identificar, tão rapidamente quanto possível, as pessoas que se encontram na proximidade de uma pessoa infetada é um fator essencial para interromper a cadeia de infeção. A determinação da proximidade é função da distância e da duração de um contacto e deve ser estabelecida de um ponto de vista epidemiológico. A interrupção da cadeia de infeção é particularmente importante para evitar o ressurgimento de infeções na fase de saída da crise.

Para tal, poderão ser necessários dados de proximidade. Para a medição da proximidade e dos contactos estreitos, as comunicações via Bluetooth de baixo consumo (*Bluetooth Low Energy* - BLE) entre dispositivos afigura-se mais precisa e, por conseguinte, mais adequada do que a utilização de dados de geolocalização (dados GNSS/GPS ou dados de localização celular). A tecnologia BLE evita a possibilidade de rastreio (ao contrário dos dados de geolocalização). Por conseguinte, a Comissão recomenda a utilização de dados comunicados por BLE (ou dados gerados por uma tecnologia equivalente) para determinar a proximidade.

Os dados de localização não são necessários para as funcionalidades com a finalidade de rastreio de contactos, uma vez que o seu objetivo não é acompanhar os movimentos de pessoas ou fazer cumprir prescrições. Além disso, o tratamento de dados de localização no contexto do rastreio de contactos seria difícil de justificar à luz do princípio da minimização dos dados e pode levantar questões de segurança e privacidade. Por esta razão, a Comissão aconselha a não utilização de dados de localização neste contexto.

Independentemente dos meios técnicos utilizados para determinar a proximidade, não se afigura necessário armazenar a hora exata do contacto ou o local (se disponível). No entanto, poderá ser útil armazenar o dia do contacto para saber se o contacto ocorreu quando a pessoa desenvolveu sintomas (ou 48 horas antes ([13])) e para orientar a mensagem de seguimento com o conselho, por exemplo, sobre o tempo de autoquarentena.

Os dados de proximidade só devem ser gerados e tratados se existir um risco real de infeção (consoante a proximidade e a duração do contacto).

Deve observar-se que a necessidade e a proporcionalidade da recolha de dados dependerá assim de fatores como a medida em que as instalações de testagem estão disponíveis, em especial quando já tiverem sido ordenadas medidas como o confinamento. O alerta de pessoas que tenham estado em contacto estreito com uma pessoa infetada pode ser feito de duas formas:

De acordo com a primeira abordagem, um alerta é automaticamente emitido através da aplicação para os contactos estreitos quando um utilizador notifica a aplicação - com a aprovação ou confirmação pela autoridade sanitária através, por exemplo, de um código QR ou TAN - de que o resultado do seu teste foi positivo (tratamento descentralizado). O conteúdo da mensagem de alerta deve, de preferência, ser determinado pela autoridade de saúde. De acordo com a segunda abordagem, os identificadores temporários arbitrários são armazenados num servidor de suporte na posse da autoridade de saúde (solução com servidor de suporte). Os utilizadores não podem ser diretamente identificados através destes dados. Através dos identificadores, os utilizadores que tenham estado em contacto estreito com um utilizador testado positivo, recebem um alerta no seu dispositivo. Se as autoridades de saúde desejarem contactar os utilizadores que tenham estado em contacto estreito com uma pessoa infetada também por telefone ou por SMS, necessitam do consentimento desses utilizadores para fornecerem os seus números de telefone.

([13]) A pessoa infetada é contagiosa 48 horas antes do início dos sintomas.

3.5 **Limitar a divulgação/acesso aos dados**

— Funcionalidade de informação:

Nenhuma informação armazenada e acessível a partir dos equipamentos terminais, que não seja necessária para assegurar a funcionalidade de informação, pode ser partilhada com autoridades de saúde. Uma vez que esta funcionalidade fornece apenas os meios de comunicação, as autoridades de saúde não terão acesso a quaisquer outros dados.

— Funcionalidades de controlo de sintomas e telemedicina:

A funcionalidade de controlo de sintomas pode ser útil para os Estados-Membros orientarem os cidadãos no sentido de saberem se devem ser testados e para prestarem informações sobre o isolamento e sobre o momento e a forma de acesso aos cuidados de saúde, em especial para os grupos de risco. Esta funcionalidade pode igualmente complementar a vigilância sindromática de cuidados primários e ajudar a calcular as taxas de infeção da COVID-19 na população. Por conseguinte, pode decidir-se que as autoridades de saúde responsáveis e as autoridades epidemiológicas nacionais devem ter acesso às informações fornecidas pelo paciente. O ECDC poderia receber dados agregados das autoridades nacionais para a vigilância epidemiológica.

Se for adotada a opção que permita um contacto com os serviços de saúde e não através da própria aplicação, também é necessário divulgar às autoridades de saúde nacionais o número de telefone dos utilizadores de aplicações.

— Funcionalidade de rastreio de contactos e de alerta:

— Dados da pessoa infetada

As aplicações geram pseudo-aleatoriamente identificadores efémeros e periodicamente cambiantes dos telefones que estão em contacto com o utilizador. Uma opção pode ser a de os identificadores serem armazenados no dispositivo do utilizador (designada por «tratamento descentralizado»). Outra opção pode estabelecer que estes identificadores arbitrários sejam armazenados no servidor a que as autoridades de saúde têm acesso (designada por «solução com servidor de suporte» (*backend server solution*). A solução descentralizada é mais consentânea com o princípio da minimização. As autoridades de saúde só devem ter acesso a dados de proximidade provenientes do dispositivo de uma pessoa infetada para poder contactar as pessoas em risco de infeção.

Tais dados serão disponibilizados às autoridades de saúde apenas depois de a pessoa infetada (após ter sido testada) partilhar proativamente estes dados com estas autoridades.

A pessoa infetada não deve ser informada da identidade das pessoas com as quais esteve potencialmente em contacto epidemiológico relevante e que serão alertadas.

— Dados das pessoas que estiveram em contacto (epidemiológico) com a pessoa infetada

A identidade da pessoa infetada não deve ser divulgada às pessoas com as quais tenha estado em contacto epidemiológico. É suficiente comunicar-lhes o facto de terem estado em contacto epidemiológico com uma pessoa infetada nos últimos 16 dias. Tal como acima referido, os dados relativos à data e ao local de tais contactos não devem ser armazenados. Por conseguinte, não é necessário nem possível comunicar esses dados.

Para rastrear os contactos epidemiológicos de um utilizador da aplicação que tenha sido considerado infetado, as autoridades de saúde nacionais devem ser informadas apenas sobre o identificador da pessoa com quem a pessoa infetada esteve em contacto epidemiológico desde 48 horas antes do início dos sintomas até 14 dias após o início dos sintomas, com base na proximidade e na duração do contacto.

O ECDC poderá receber dados agregados de rastreio de contactos das autoridades nacionais para a vigilância epidemiológica sobre indicadores definidos em colaboração com os Estados-Membros.

3.6 **Estabelecimento das finalidades exatas do tratamento**

A base jurídica (legislação da União ou dos Estados-Membros) deve estabelecer a finalidade do tratamento. A finalidade deve ser específica, de modo a que não haja dúvidas sobre o tipo de dados pessoais necessários para alcançar o objetivo pretendido, e explícita. .

A(s) finalidade(s) exatas dependerão das funcionalidades da aplicação. Cada funcionalidade de uma aplicação poderá ter várias finalidades. A fim de permitir que as pessoas tenham pleno controlo dos seus dados, a Comissão recomenda que não se agrupem diferentes funcionalidades. Em qualquer caso, o utilizador deve ter a possibilidade de escolher entre diferentes funcionalidades, cada uma com finalidades distintas.

A Comissão desaconselha a utilização dos dados recolhidos para finalidades diferentes da luta contra a COVID-19. Caso sejam necessárias finalidades como a investigação científica e as estatísticas, estas devem ser incluídas na lista inicial de finalidades e comunicadas claramente aos utilizadores.

— Funcionalidade de informação:

A finalidade desta funcionalidade é fornecer informações que sejam pertinentes do ponto de vista das autoridades de saúde no contexto da crise.

— Finalidades de controlo de sintomas e de telemedicina:

A funcionalidade de controlo de sintomas pode fornecer uma indicação da percentagem de indivíduos que apresentam sintomas compatíveis com a COVID-19 e que estão efetivamente infetados (por exemplo, submetendo todas ou um número aleatório de pessoas com sintomas desta natureza a esfregaços e testes, se houver capacidade para o fazer). Esta identificação da finalidade deve indicar claramente que os dados pessoais de saúde serão tratados para permitir que o utilizador i) avalie, com base num conjunto de perguntas colocadas, se desenvolveu sintomas de COVID-19, ou ii) obtenha aconselhamento médico se tiver desenvolvido sintomas do COVID19.

— Funcionalidades de rastreio de contactos e de alerta:

A mera indicação da finalidade «prevenir novas infeções com COVID-19» não é suficientemente específica. Neste caso, a Comissão recomenda que se especifique mais pormenorizadamente a(s) finalidade(s) nos seguintes moldes: «conservar os contactos das pessoas que utilizam a aplicação e que podem ter sido expostas à infeção com COVID-19, a fim de alertar as pessoas suscetíveis de terem sido infetadas».

3.7 **Estabelecer limites estritos de conservação de dados**

O princípio da limitação da conservação exige que os dados pessoais sejam conservados apenas durante o período necessário. O horizonte temporal deve ser determinado com base na pertinência em termos médicos (em função da finalidade da aplicação: o período de incubação, etc.), bem como na vigência realista das medidas administrativas que se revelem necessárias.

— Funcionalidade de informação:

Se forem recolhidos dados durante a instalação desta funcionalidade, estes devem ser imediatamente apagados. Não há qualquer justificação para conservar estes dados.

— Funcionalidades de controlo de sintomas e telemedicina:

Estes dados devem ser suprimidos pelas autoridades de saúde após um período máximo de um mês (período de incubação mais margem) ou depois de a pessoa ter sido testada e o resultado ter sido negativo. As autoridades de saúde podem conservar os dados durante períodos mais longos para elaborar relatórios de vigilância e para fins de investigação, desde que estes sejam anonimizados.

— Funcionalidades de rastreio de contactos e de alerta:

Os dados de proximidade devem ser apagados logo que deixem de ser necessários para a finalidade de alertar as pessoas. Tal deve acontecer após um período máximo de um mês (período de incubação mais margem) ou depois de a pessoa ter sido testada e o resultado ter sido negativo. As autoridades de saúde podem conservar os dados de proximidade durante períodos mais longos para elaborar relatórios de vigilância e para fins de investigação, desde que estes sejam anonimizados.

Os dados devem ser conservados no dispositivo do utilizador. Só os dados que tenham sido comunicados pelos utilizadores e que sejam necessários para cumprir a finalidade devem ser carregados para o servidor à disposição das autoridades de saúde, caso essa opção seja escolhida (ou seja, apenas os dados de quem tenha estado em «contacto estreito» com pessoas que tenham tido um teste positivo para a COVID-19).

3.8 **Garantir a segurança dos dados**

A Comissão recomenda que os dados sejam conservados no dispositivo terminal do indivíduo, em formato encriptado, utilizando técnicas de encriptação avançadas. Caso os dados sejam conservados num servidor central, o acesso ao mesmo, incluindo o acesso administrativo, deve ser registado.

Os dados de proximidade só devem ser gerados e conservados no dispositivo terminal do utilizador em formato encriptado e pseudonomizado. A fim de assegurar que o rastreio por terceiros é excluído, deve ser possível ativar o *Bluetooth* sem ter de ativar outros serviços de localização.

Durante a recolha de dados de proximidade por BLE, é preferível criar e conservar identificadores de utilizador temporários que sejam regularmente modificados, em vez de conservar o identificador real do dispositivo. Esta medida proporciona uma proteção adicional contra escutas e localização por parte de piratas informáticos, dificultando, por conseguinte, a identificação das pessoas.

A Comissão recomenda que o código fonte da aplicação seja tornado público e disponibilizado para análise.

Podem ser previstas medidas adicionais para garantir a segurança dos dados tratados, nomeadamente a supressão ou a anonimização automáticas dos dados a partir de um determinado momento. Em geral, o grau de segurança deve corresponder à quantidade e ao grau de sensibilidade dos dados pessoais tratados.

Todas as transmissões do dispositivo pessoal às autoridades nacionais de saúde devem ser encriptadas.

Sempre que a legislação nacional preveja que os dados pessoais recolhidos possam também ser tratados para fins de investigação científica, a pseudonimização deve, em princípio, ser utilizada.

3.9 **Garantir a exatidão dos dados**

Garantir a exatidão dos dados pessoais tratados não é apenas uma condição indispensável para a eficiência da aplicação, mas também um requisito ao abrigo da legislação em matéria de proteção de dados pessoais.

Neste contexto, é essencial garantir a exatidão das informações relativas à ocorrência de um contacto com uma pessoa infetada (distância epidemiológica e duração), a fim de minimizar o risco de obter falsos positivos. Tal deverá equacionar cenários em que dois utilizadores da aplicação estão em contacto na rua, nos transportes públicos ou num edifício. É pouco provável que a utilização de dados de localização baseados em redes de telemóveis seja suficientemente exata para tal.

Por conseguinte, é aconselhável recorrer a tecnologias que permitam uma avaliação mais exata do contacto (como o *Bluetooth*).

3.10 **Papel das autoridades de proteção de dados**

As autoridades de proteção de dados devem ser plenamente associadas ao desenvolvimento de uma aplicação e consultadas durante este processo, devendo também avaliar a implantação das aplicações. Dado que o tratamento de dados no contexto da aplicação pode ser considerado um tratamento em grande escala de categorias especiais de dados (dados de saúde), a Comissão chama a atenção para o artigo 35.º do RGPD relativo à avaliação de impacto sobre a proteção de dados.

ISSN 1977-1010 (edição eletrónica)
ISSN 1725-2482 (edição em papel)

Serviço das Publicações da União Europeia
2985 Luxemburgo
LUXEMBURGO

PT