Comité Europeu para a Proteção de Dados

Diretrizes

Diretrizes n.º 4/2020 sobre a utilização de dados de localização e ferramentas de *contact tracing* no contexto do surto de COVID-19

Adotado em 21 de abril de 2020

ÍNDICE

ÍNDICE 2
1 INTRODUÇÃO E CONTEXTO 3
2 UTILIZAÇÃO DOS DADOS DE LOCALIZAÇÃO 5
3 APLICAÇÕES DE RASTREAMENTO DE CONTACTO 7
4 CONCLUSÃO 11
ANEXO - GUIA DE ANÁLISE DAS APLICAÇÕES DE RASTREAMENTO DE CONTACTO 12

O Comité Europeu para a Proteção de Dados

Tendo em conta o artigo 70.º, n. º1, alínea e), do 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 (a seguir designado como «RGPD»);

Tendo em conta o Acordo EEE, nomeadamente o anexo XI e o Protocolo n.º 37, com a redação que lhe foi dada pela Decisão do Comité Misto do EEE n. º 154/2018, de 6 de julho de 2018[1];

Tendo em conta os artigos 12.º e 22.º do seu Regulamento Interno.

ADOTOU AS SEGUINTES DIRETRIZES:

1 INTRODUÇÃO E CONTEXTO

1 Governos e atores privados estão a voltar-se para o uso de soluções baseadas em dados como parte da resposta à pandemia COVID-19, levantando inúmeras preocupações com a privacidade.

2 O CEPD sublinha que o quadro jurídico de proteção de dados foi concebido para ser flexível e, como tal, é capaz de obter uma resposta eficaz na limitação da pandemia e na proteção dos direitos humanos e das liberdades fundamentais.

3 O CEPD acredita firmemente que, quando o tratamento de dados pessoais é necessário para a gestão da pandemia COVID-19, a proteção de dados é indispensável para construir confiança, criar as condições de aceitação social de qualquer solução e, assim, garantir a eficácia dessas medidas. Uma vez que o vírus não conhece fronteiras, parece preferível desenvolver uma abordagem europeia comum em resposta à atual crise ou, pelo menos, criar um quadro interoperável.

4 No geral, o CEPD considera que dados e tecnologias usadas para ajudar a combater a COVID-19 devem ser usados para capacitar, em vez de controlar, estigmatizar ou reprimir indivíduos. Além disso, embora os dados e a tecnologia possam ser ferramentas importantes, eles têm limitações intrínsecas e podem apenas alavancar a eficácia de outras medidas de saúde pública. Os princípios gerais de eficácia, necessidade e proporcionalidade devem orientar qualquer medida adotada pelos Estados-Membros ou pelas instituições da UE que envolvam o tratamento de dados pessoais para combater a COVID-19.

5 Estas orientações clarificam as condições e princípios para a utilização proporcionada dos dados de localização e dos instrumentos de localização, para dois fins específicos:

- utilizar dados de localização para apoiar a resposta à pandemia, modelando a propagação do vírus, de modo a avaliar a eficácia global das medidas de confinamento;
- rastreamento de contactos, que visa notificar os indivíduos de que estiveram próximos de alguém que foi confirmado como portador do vírus, a fim de, rapidamente, quebrar as cadeias de contaminação.

[1] As referências aos « Estados-Membros » feitas ao longo do presente documento devem ser entendidas como referências aos « Estados-Membros do EEE ».

6 A eficiência da contribuição das aplicações de rastreio de contacto para a gestão da pandemia depende de muitos fatores (por exemplo, percentagem de pessoas que a instalariam; definição de «contacto» em termos de proximidade e duração). Além disso, essas aplicações têm de fazer parte de uma estratégia global de saúde pública para combater a pandemia, incluindo, nomeadamente, os testes e subsequentes estabelecimentos de contacto para efeito de confirmação. 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. Caso contrário, estas aplicações podem não atingir o seu objectivo.

7 O CEPD salienta que o RGPD e a Diretiva 2002/58/CE (Diretiva «ePrivacy») contêm regras específicas que permitem a utilização de dados anónimos ou pessoais para apoiar as autoridades públicas e outros intervenientes a nível nacional e da UE na monitorização e na disseminação do vírus SARS-CoV2.[2]

8 A este respeito, o CEPD já tomou posição sobre a utilização de tais aplicações de rastreamento de contacto dever ser voluntária e não dever depender do rastreamento de movimentos individuais, mas sim de informações de proximidade sobre os utilizadores.[3]

[2]Ver a declaração anterior do CEPD sobre o surto de COVID 19.
[3] https://EDPB.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance final.pdf

2 UTILIZAÇÃO DOS DADOS DE LOCALIZAÇÃO

2.1 Fontes de dados de localização

9 Existem duas principais fontes de dados de localização disponíveis para modelar a propagação do vírus e a eficácia global das medidas de confinamento:

- dados de localização recolhidos pelos prestadores de serviços de comunicações eletrónicas (como os operadores de telecomunicações móveis) durante a prestação do seu serviço; bem como
- dados de localização recolhidos pelas aplicações dos prestadores de serviços da sociedade da informação cuja funcionalidade exige a utilização desses dados (por exemplo, navegação, serviços de transporte, etc.).

10 O CEPD recorda que os dados de localização recolhidos junto dos fornecedores de comunicações eletrónicas[4] só podem ser tratados no âmbito das atribuições dos artigos 6.º e 9.º da Diretiva «ePrivacy». Isto significa que estes dados só podem ser transmitidos às autoridades ou a terceiros se tiverem sido anonimizados pelo fornecedor ou, relativamente a dados que indiquem a posição geográfica do equipamento terminal de um utilizador, que não sejam dados de tráfego, com o consentimento prévio dos utilizadores.[5]

11 No que se refere às informações, incluindo dados de localização, recolhidas diretamente do equipamento terminal, aplica-se o n.º 3 do artigo 5.º da Diretiva «ePrivacy». Assim, o armazenamento de informações no dispositivo do utilizador ou o acesso às informações já armazenadas só é permitido se (i) o utilizador tiver dado consentimento[6] ou (ii) o armazenamento e/ou acesso for estritamente necessário para o serviço da sociedade da informação explicitamente solicitado pelo utilizador.

12 No entanto, são possíveis derrogações aos direitos e obrigações previstos na Diretiva «ePrivacy» nos termos do artigo 15.º, quando constituem uma medida necessária, adequada e proporcionada no seio de uma sociedade democrática para determinados objetivos.[7]

13 No que se refere à reutilização dos dados de localização recolhidos por um prestador de serviços da sociedade da informação para efeitos de modelização (por exemplo, através do sistema operativo ou de alguma aplicação previamente instalada), devem ser satisfeitas condições adicionais. Com efeito, quando os dados tiverem sido recolhidos em conformidade com o n.º 3 do artigo 5.º da Diretiva «ePrivacy», só poderão ser tratados posteriormente com o consentimento adicional do titular dos dados ou com base em legislação da União ou dos Estados-Membros que constitua uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no n.º 1 do artigo 23.º do RGPD.[8]

2.2 Foco no uso de dados de localização anonimizados

14 O CEPD salienta que, quando se trata de utilizar dados de localização, deve ser dada preferência ao tratamento de dados anonimizados em vez de dados pessoais.

15 Anonimização refere-se ao uso de um conjunto de técnicas a fim de remover a capacidade de associar os dados a uma pessoa singular identificada ou identificável contra qualquer esforço «razoável». Este «teste de razoabilidade» deve ter em conta os aspetos objetivos (tempo, meios técnicos) e elementos contextuais que podem variar caso a caso (raridade de um fenómeno, considerando a densidade populacional, a natureza e o volume de dados). Se os dados não passarem neste teste, então não foram anonimizados e, portanto, permanecem no âmbito do

[4] Ver artigo 2.º, alínea c), da Diretiva «ePrivacy».
[5] Ver artigos 6.º e 9.º da Diretiva «ePrivacy».
[6] A noção de consentimento na Diretiva «ePrivacy» continua a ser a noção de consentimento no RGPD e deve atender a todos os requisitos do consentimento conforme previsto nos artigos 4.º(11) e 7.º do RGPD.
[7] Para a interpretação do artigo 15.º da Diretiva « ePrivacy », ver também o acórdão TJUE de 29 de janeiro de 2008 no processo C-275/06, Productores de Musica de España (Promusicae) contra Telefonica de España SAU.
[8] Ver secção 1.5.3 das Diretrizes 1/2020 sobre o tratamento de dados pessoais no contexto de veículos conectados.

RGPD.

16 A avaliação da robustez do anonimato depende de três critérios: i) individualização (isolando um indivíduo de um grupo; ii) suscetibilidade de associação – «*linkability*»(ligação entre dois registos relativos a um mesmo indivíduo); e (iii) inferência (deduzindo, com probabilidade significativa, informação desconhecida sobre um indivíduo).

17 O conceito de anonimização é propenso a ser mal compreendido e muitas vezes é confundido com pseudonimização. Enquanto a anonimização permite usar os dados sem qualquer restrição, os dados pseudonimizados ainda estão no âmbito do RGPD.

18 Existem muitas opções para anonimização eficaz,[9] mas sempre com uma ressalva. Os dados não podem ser anonimizados por si próprios, o que significa que apenas conjuntos de dados como um todo podem ser tornados anónimos. Neste sentido, qualquer intervenção num único padrão de dados (por meio de criptografia, ou qualquer outra transformação matemática) pode, na melhor das hipóteses, ser considerada uma pseudonimização.

19 Processos de anonimização e ataques de reidentificação são campos ativos de pesquisa. É fundamental que todos os responsáveis implementem soluções de anonimização para acompanhar os recentes desenvolvimentos neste domínio, especialmente no que diz respeito aos dados de localização (originários de operadores de telecomunicações e/ou serviços da sociedade da informação) que são conhecidos por serem notoriamente difíceis de anonimizar.

20 Na verdade, um grande número de pesquisas mostrou que os dados de localização[10] que se *pensa serem anonimizados podem, de facto, não ser*. Os traços de mobilidade dos indivíduos são, por inerência, altamente correlacionados e únicos. Portanto, são vulneráveis a tentativas de reidentificação em determinadas circunstâncias.

21 Um único padrão de dados que rastreie a localização de um indivíduo durante um período significativo de tempo não pode ser totalmente anonimizado. Esta conclusão continua válida se a precisão das coordenadas geográficas registadas não for suficientemente reduzida, ou se partes do rastreio forem retiradas, mesmo que apenas se mantenham os locais em que se tenha estado durante um período considerável de tempo. Isso também vale para dados de localização que sejam deficientemente agregados.

22 Para alcançar a anonimização, os dados de localização devem ser cuidadosamente processados para atender ao teste de razoabilidade. Nesse sentido, tal processamento inclui considerar conjuntos de dados de localização como um todo, bem como o processamento de dados de um conjunto grande de indivíduos usando técnicas disponíveis de anonimização robustas, desde que sejam adequadas e efetivamente implementadas.

23 Por fim, dada a complexidade dos processos de anonimização, é altamente incentivada a transparência quanto à metodologia de anonimização utilizada.

[9] (de Montjoye et al., 2018) "On the privacy-conscientious use of mobile phone data" .

[10] (de Montjoye et al., 2013) "Unique in the Crowd: The privacy bounds of human mobility" and (Pyrgelis et al., 2017) "Knock Knock, Who's There? Membership Inference on Aggregate Location Data".

3 APLICAÇÕES DE RASTREAMENTO DE CONTACTO

3.1 Análise jurídica geral

24 O acompanhamento sistemático e em larga escala da localização e/ou dos contactos entre pessoas singulares constitui uma grave intrusão na sua privacidade. Tal só pode ser legitimado se contar com uma adoção voluntária pelos utilizadores para cada uma das finalidades respetivas. Isto implicaria, em particular, que os indivíduos que decidem não utilizar ou não podem utilizar tais aplicações não devem sofrer qualquer desvantagem.

25 Para garantir a responsabilização, deve estar claramente definido quem é o o responsável por qualquer aplicação de rastreamento de contacto. O CEPD considera que as autoridades de saúde nacionais podem ser as responsáveis[11] pelo tratamento dessa aplicação, admitindo-se poderem ser previstos outros responsáveis. Em todo o caso, se a implementação de aplicações de rastreamento de contacto envolver diferentes atores, os seus papéis e responsabilidades devem ser claramente estabelecidos desde o início e explicados aos utilizadores.

26 Além disso, no que se refere ao princípio da limitação da finalidade, os objetivos devem ser suficientemente específicos e excluir o tratamento posterior para fins não relacionados com a gestão da crise sanitária COVID-19 (por exemplo, fins comerciais ou de segurança pública). Uma vez definido claramente o objetivo, será necessário assegurar que a utilização dos dados pessoais seja adequada, necessária e proporcionada.

27 No contexto de uma aplicação de rastreio de contacto, deve dar-se atenção redobrada ao princípio da minimização dos dados e à proteção de dados desde a conceção e por defeito:

- as aplicações de rastreamento de contacto não exigem o rastreamento da localização de utilizadores individuais. Em vez disso, devem ser utilizados dados de proximidade;
- uma vez que estas aplicações podem funcionar sem identificação direta dos indivíduos, devem ser tomadas medidas adequadas para evitar a reidentificação;
- as informações recolhidas devem residir no equipamento terminal do utilizador e apenas as informações relevantes devem ser recolhidas quando tal for absolutamente necessário.

28 No que diz respeito à legalidade do tratamento, o CEPD observa que as aplicações de rastreamento de contacto envolvem armazenamento e/ou acesso a informações já armazenadas no terminal, que estão abrangidas pelo disposto no n.º 3 do artigo 5.º da Diretiva «ePrivacy». Se essas operações fossem estritamente necessárias para a prestação de um serviço expressamente solicitado pelo utilizador, não seria exigível o seu consentimento. Para operações não estritamente necessárias, o fornecedor precisaria de obter o consentimento do utilizador.

29 Além disso, o CEPD dá nota que o facto de a utilização de aplicações de localização de contacto ser voluntária, não significa que o tratamento de dados pessoais se baseie necessariamente no consentimento. Quando as autoridades públicas prestam um serviço com base num mandato atribuído por e em conformidade com os requisitos legais, afigura-se que a base jurídica relevante para o tratamento é a necessidade de desempenhar uma tarefa de interesse público, ou seja, o artigo 6.º, n.º 1, alínea e), do RGPD.

30 O artigo 6.º, n.º 3, do RGPD determina que o fundamento para o tratamento referido na alínea e) do n.º 1 do artigo 6.º deve ser estabelecido pela legislação da União ou dos Estados-Membros. A finalidade do tratamento é determinada por essa legislação e tem de ser necessária ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento.[12]

31 A medida legislativa que fornece a base legal para a utilização de aplicações de rastreio de contactos terá de incorporar salvaguardas significativas, incluindo uma referência ao caráter

[11] Ver também a Comissão Europeia «Orientação sobre aplicações que apoiam a luta contra a pandemia do COVID 19 em matéria de proteção de dados» Bruxelas, 16.4.2020 C(2020) 2523 final.
[12] Ver considerando (41).

voluntário da aplicação. Deverá ser incluída uma especificação clara da finalidade e limitações explícitas relativas à utilização posterior de dados pessoais, bem como uma identificação clara do(s) responsável(ais) envolvido(s). As categorias de dados, bem como as entidades (e as finalidades) para as quais os dados pessoais podem ser divulgados também devem ser identificadas. Dependendo do nível de interferência, devem ser incorporadas salvaguardas adicionais, tendo em conta a natureza, o âmbito e os objetivos do tratamento. Por último, o CEPD recomenda igualmente a inclusão, logo que possível, dos critérios para determinar quando a aplicação deve ser desinstalada e que entidade deve ser responsável por essa determinação.

32 No entanto, se o tratamento de dados assentar noutra base jurídica, como, por exemplo, o consentimento (alínea a) n.º 1 do artigo 6.º),[13] o responsável pelo tratamento terá de assegurar o cumprimento dos específicos requisitos para que essa base jurídica seja válida.

33 Além disso, a utilização da aplicação para combater a pandemia de COVID-19 pode levar à recolha de dados de saúde (por exemplo, o estado de uma pessoa infetada). O processamento desses dados é apenas permitido quando é necessário por razões de interesse público na área da saúde pública, satisfazendo as condições do art. 9.º, n.º 2, alínea i), do RGPD[14] ou para fins de saúde, conforme descrito no artigo 9.º, n.º 2, alínea h), do RGPD.[15] Dependendo do fundamento legal, pode também basear-se no consentimento explícito (artigo 9.º, n.º 2, alínea a), do RGPD).

34 De acordo com o objetivo inicial, o artigo 9.º, n.º 2, alínea j), do GDPR também permite que os dados de saúde sejam processados quando necessários para fins de pesquisa científica ou para fins estatísticos.

35 A atual crise sanitária não deve ser utilizada como uma oportunidade para estabelecer mandatos de retenção de dados desproporcionados. A limitação do armazenamento deve considerar as verdadeiras necessidades e a relevância médica (o pode incluir razões de epidemiologia como, p. ex., o período de incubação) e os dados pessoais devem ser mantidos apenas durante a crise da COVID-19. Posteriormente, como regra geral, todos os dados pessoais devem ser apagados ou anonimizados.

36 É entendimento do CEPD que tais aplicações não podem substituir, mas apenas servir de base para o contacto realizado por profissionais de saúde pública qualificado, que pode determinar se contactos próximos são suscetíveis de resultar em transmissão de vírus ou não (p. ex., quando interagem com alguém protegido por equipamentos adequados). O CEPD sublinha que procedimentos e processos, incluindo os respetivos algoritmos implementados pelas aplicações de rastreamento de contactos, devem funcionar sob a estrita supervisão de pessoal qualificado, a fim de limitar a ocorrência de falsos positivos e negativos. Em especial, a tarefa de aconselhamento sobre as próximas etapas não deve basear-se unicamente no processamento automatizado.

37 A fim de garantir a sua equidade, responsabilidade e, de um modo mais geral, a conformidade com a lei, os algoritmos devem ser auditáveis e devem ser regularmente revistos por peritos independentes. O código-fonte da aplicação deve ser tornado público para o mais amplo controlo possível.

38 Prevê-se a ocorrência de falsos positivos. Na medida em que a identificação de um risco de infeção pode ter um alto impacto sobre os indivíduos, como p. ex. permanecer em isolamento até o teste ser negativo, a capacidade de corrigir dados e/ou resultados subsequentes de análise é uma necessidade. É evidente que tal só se deverá aplicar aos cenários e implementações em que os dados são tratados e/ou armazenados de uma forma que tal correção seja tecnicamente

[13] Os responsáveis pelo tratamento (especialmente as autoridades públicas) devem prestar especial atenção ao facto de que o consentimento não deve ser considerado como dado livremente se o indivíduo não tiver uma escolha genuína de recusar ou retirar o seu consentimento sem consequências negativas.

[14] O tratamento deve basear-se na legislação da União ou dos Estados-Membros que preveja medidas adequadas e específicas para salvaguardar os direitos e liberdades da pessoa em causa, em especial o sigilo profissional.

[15] Ver artigo 9.º, n.º 2, alínea h), do RGPD.

exequível e que os efeitos adversos acima mencionados sejam suscetíveis de ocorrer.

39 Por último, o CEPD considera que deve ser efetuada uma avaliação do impacto na proteção de dados (AIPD) antes de implementar esse instrumento, dado que o tratamento é considerado de elevado risco (dados de saúde, adoção antecipada em larga escala, monitorização sistemática, utilização de novas tecnológicas soluções[16]). O CEPD recomenda fortemente a publicação das AIPDs.

3.2 Recomendações e requisitos funcionais

40 De acordo com o princípio da minimização de dados, entre outras medidas de proteção de dados desde a conceção e por defeito,[17] os dados tratados devem ser reduzidos ao estritamente necessário. A aplicação não deve recolher informações não relacionadas ou não necessárias para a finalidade, designadamente estado civil, identificadores de comunicação, itens de diretório de equipamentos, mensagens, registos de chamadas, dados de localização, identificadores de dispositivo.

41 Os dados transmitidos por aplicações devem incluir apenas alguns identificadores únicos e pseudonimizados, gerados pela, e específicos da aplicação. Esses identificadores devem ser renovados regularmente, com uma frequência compatível e suficiente com o objetivo de conter a propagação do vírus, limitando o risco de identificação e de rastreio físico dos indivíduos.

42 Implementações para rastreamento podem seguir uma abordagem centralizada ou descentralizada.[18] Ambas devem ser consideradas opções viáveis, desde que estejam em vigor medidas de segurança adequadas, cada uma acompanhada de um conjunto de vantagens e desvantagens. Assim, a fase conceitual de desenvolvimento de aplicações deve incluir sempre uma análise minuciosa de ambos os conceitos, pesando cuidadosamente os respetivos efeitos sobre a proteção de dados e a privacidade e os possíveis impactos sobre os direitos dos indivíduos.

43 Qualquer servidor envolvido no sistema de rastreamento de contactos só deve recolher o histórico de contactos ou os identificadores pseudonimizados dos utilizadores infetados na sequência de uma avaliação de confirmação das autoridades de saúde e sempre decorrente de uma ação voluntária do utilizador. Em alternativa, o servidor pode manter uma lista de identificadores pseudonimizados de utilizadores infetados ou seu histórico de contactos apenas durante o tempo necessário para informar os outros utilizadores da sua exposição, e não deve tentar identificar utilizadores potencialmente infetados.

44 A adoção de uma metodologia global de rastreamento, que inclua aplicações e interações com profissionais de saúde, pode exigir, em alguns casos, o processamento de informações adicionais. Neste contexto, essas informações adicionais devem permanecer no terminal do utilizador e só devem ser objeto de tratamento quando seja estritamente necessário e com consentimento prévio e específico do titular dos dados.

45 As técnicas criptográficas de última geração devem ser as utilizadas para proteger os dados armazenados em servidores e em aplicações e nas trocas entre aplicações e o servidor remoto. Também se exige a mútua autenticação entre a aplicação e o servidor.

46 O reporte de um utilizador infetado com COVID-19 na aplicação deve estar sujeita a um consentimento específico e adequado, por exemplo através de um código de utilização único ligado a uma identidade pseudonimizada da pessoa infetada e a um laboratório de testes ou profissional de saúde que valide a informação. Se a confirmação da infeção não puder ser obtida de forma segura, não pode haver tratamento de dados com base em presunções do estado de saúde do utilizador.

---

[16] Ver orientações do WP29 (adotadas pelo CEPD) sobre a avaliação do impacto na proteção de dados (DPIA) e determinar se o tratamento pode « resultar num risco elevado » para efeitos do Regulamento 2016/679.

[17] Ver Diretrizes CEPD 4/2019 sobre o artigo 25.º Proteção de dados desde a conceção e pordefeito.

[18] Em geral, a solução descentralizada está mais de acordo com o princípio da minimização.

47 O responsável, em colaboração com as autoridades públicas, tem de informar clara e explicitamente sobre o *link* que deve ser descarregado para a aplicação de rastreamento de contacto nacional, a fim de diminuir o risco de os titulares dos dados estarem erradamente a usar aplicações de terceiros.

4 CONCLUSÃO

48 O mundo enfrenta uma importante crise de saúde pública que requer respostas fortes, as quais terão impacto para além desta emergência. O processamento automatizado de dados e as tecnologias digitais podem ser componentes-chave na luta contra a COVID-19. No entanto, deve ter-se consciência do «efeito *ratchet*» na utilização destas tecnologias. É responsabilidade de todos assegurar que as medidas tomadas nestas circunstâncias extraordinárias são necessárias, limitadas no tempo, respeitadoras do princípio da minimização e sujeitas a uma revisão periódica e genuína, bem como a uma avaliação científica.

49 O CEPD sublinha que não se deve escolher entre uma resposta eficaz à atual crise e a proteção dos nossos direitos fundamentais: podemos alcançar ambos e, além disso, os princípios de proteção de dados podem desempenhar um papel muito importante na luta contra o vírus. A legislação europeia em matéria de proteção de dados permite a utilização responsável de dados pessoais para fins de gestão da saúde, assegurando simultaneamente que os direitos e liberdades individuais não sejam afectados no processo.

Pelo Comité Europeu de Proteção de Dados

A Presidente

(Andrea Jelinek)

ANEXO - GUIA DE ANÁLISE DAS APLICAÇÕES DE RASTREAMENTO DE CONTACTO

Declaração de Isenção de Responsabilidade

A seguinte orientação não é nem prescritiva nem exaustiva, e o seu único objetivo é fornecer orientações gerais a quem desenvolve e implementa aplicações de rastreamento de contacto. Outras soluções que não as aqui descritas podem ser usadas e podem ser lícitas desde que cumpram o quadro legal relevante (ou seja, o RGPD e a Diretiva «ePrivacy»).

Note-se também que este guia é de natureza geral. Por conseguinte, as recomendações e obrigações nele contidas não devem ser consideradas exaustivas. Qualquer avaliação deve ser efetuada caso a caso e cada aplicação pode exigir medidas adicionais não incluídas no presente guia.

1. Resumo

Em muitos Estados-Membros, está a ser ponderada a utilização de aplicações de rastreamento de contacto para ajudar a população a descobrir se esteve em contacto com uma pessoa infetada com SARS-Cov2.

As condições sob as quais essas aplicações contribuirão eficazmente para a gestão da pandemia ainda não estão fixadas. E essas condições deveriam ser estabelecidas antes de qualquer implementação de tal aplicação. No entanto, é pertinente fornecer orientações que deem informação a quem as está a desenvolver, de modo que a proteção dos dados pessoais possa ser garantida desde a fase inicial da conceção.

Note-se que este guia é de natureza geral. Por conseguinte, as recomendações e obrigações contidas no presente documento não devem ser consideradas exaustivas. Qualquer avaliação deve ser efetuada caso a caso e cada aplicação pode exigir medidas adicionais não incluídas no presente guia. O objetivo deste guia é fornecer orientação geral a quem está a desenvolver e a quem vai implementar aplicações de rastreamento de contacto.

Alguns critérios podem ultrapassar os requisitos decorrentes do quadro de proteção de dados. Tal, tem por objetivo garantir o mais elevado nível de transparência, a fim de favorecer a aceitação social de tais aplicações.

Para o efeito, quem disponibilize aplicações de rastreamento de contacto deve ter em conta os seguintes critérios:

- A utilização de tal aplicação deve ser estritamente voluntária. O seu uso não pode condicionar o acesso a quaisquer direitos garantidos por lei. Os indivíduos devem ter o controlo total sobre seus dados pessoais, em todos os momentos, e ser capazes de escolher livremente a utilização de uma tal aplicação.
- As aplicações de deteção de contactos são suscetíveis de gerar um risco elevado para os direitos e liberdades das pessoas singulares e, por isso, exije-se que seja efetuada uma avaliação do impacto na proteção de dados antes da sua implementação.
- Informações sobre a proximidade entre os utilizadores da aplicação podem ser obtidas sem os localizar. Este tipo de aplicação não precisa e, portanto, não deve envolver o uso de dados de localização.

- Quando um utilizador é diagnosticado como infetado com o vírus SARS-Cov2, só as pessoas com as quais o utilizador tenha estado em contacto próximo, e apenas dentro do período de tempo epidemiologicamente relevante, devem ser informadas.
- Dependendo da arquitetura escolhida, este tipo de aplicações pode exigir a utilização de um servidor centralizado. Nesse caso, e em conformidade com os princípios da minimização dos dados e da proteção de dados desde a conceção, os dados tratados pelo servidor centralizado devem ser limitados ao mínimo:
    - o Quando um utilizador é diagnosticado como infetado, informações sobre seus anteriores contactos próximos ou os identificadores transmitidos pela aplicação do utilizador só podem ser recolhidoscom o seu consentimento. Tem de ser definida uma metodologia para a confirmação de que a pessoa está efetivamente infetada, sem a utilização da sua identidade. Tecnicamente, isso é possível, por exemplo, apenas alertando os contactos próximos depois da intervenção de um profissional de saúde que confirme que aquele utilizador está efetivcamente infetado, utilizando um código único específico;
    - o As informações armazenadas no servidor central não devem permitir que o responsável identifique utilizadores diagnosticados como infetados ou que tenham estado em contacto com eles, nem deve permitir a inferência de padrões de contacto não necessários para a determinação dos contactos relevantes.
- Estas aplicações requerem a transmissão de dados que são lidos por dispositivos de outros utilizadores:
    - o A troca de identificadores pseudonimizados entre os equipamentos móveis dos utilizadores (computadores, tablets, relógios conectados, etc.), por exemplo, transmitindo-os através da tecnologia Bluetooth Low Energy;
    - o Identificadores devem ser gerados usando processos criptográficos de última geração.
    - o Os identificadores devem ser renovados regularmente para reduzir o risco de ataques de rastreio físico e de ligação.

  Estas medidas devem ser asseguradas para garantir processos técnicos seguros. Em particular, a aplicação não deve transmitir aos utilizadores informações que lhes permitam inferir a identidade ou o diagnóstico de outros. O servidor central não deve nunca identificar os utilizadores, nem sobre eles inferir informações.

Declaração de responsabilidade: os princípios supramencionados são exigíveis para a implementação de aplicações de rastreamento de contactos para a exclusiva finalidade de informar as pessoas potencialmente expostas ao vírus, sem necessidade de as identificar. Os responsáveis pela aplicação e pela sua infraestrutura devem ser controlados pela autoridade supervisora competente. Contudo, o cumprimento das presentes orientações não é necessariamente suficiente para garantir o pleno cumprimento do quadro legal de proteção de dados.

2. Definições

Contacto	Um contacto é 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 pelo vírus. Os parâmetros de duração da exposição e distância entre pessoas devem ser estimados pelas autoridades de saúde e devem ser definidos na aplicação.
Dados de localização	Refere-se a todos os dados tratados numa rede de comunicações eletrónicas ou por um serviço de comunicações eletrónicas que indique a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas publicamente disponível (conforme definido na Diretiva «ePrivacy»), bem como dados de outras potenciais fontes, relativos a: • latitude, longitude ou altitude do equipamento terminal; • a direção da viagem do utilizador; ou • o momento em que as informações de localização foram registradas.
Interação	No contexto da aplicação de rastreamento de contacto, uma interação é definida como a 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 a localização dos dois utilizadores da interação.
Portador do vírus	Neste documento, consideramos portadores de vírus os utilizadores que foram testados positivos para o vírus e que receberam um diagnóstico oficial de médicos ou centros de saúde.
Localização do contacto	Pessoas que por terem estado em contacto próximo (de acordo com critérios a serem definidos pelos epidemiologistas) com um portador do vírus correm um risco significativo de também serem infetados e, por sua vez, de infetar outros. O rastreamento de contactos é uma metodologia de controlo de doenças 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.

3. Gerais

GEN -1	A aplicação deve ser uma ferramenta complementar às técnicas tradicionais de rastreamento de contacto (nomeadamente entrevistas com pessoas infetadas), ou seja, fazer parte de um programa de saúde pública mais amplo. Deve ser usado apenas até que as técnicas de rastreamento de contacto por intervenção humana possam gerir a quantidade de novas infeções.
GEN -2	O mais tardar, no fim da situação excecional de pandemia, as autoridades públicas competentes devem instituir um procedimento para interromper a recolha de identificadores (*v.g.*, desativação global da aplicação, instruções para os utilizadores desinstalarem a aplicação, desinstalação automática) e eliminar todos os dados recolhidos de todas as bases de dados (aplicações móveis e servidores).

GEN-3	O código-fonte da aplicação e do seu servidor deve ser aberto e as especificações técnicas devem ser tornadas públicas, para que seja auditável o código e, se for caso disso, contribuir para melhorar o código, corrigir possíveis erros e garantir a transparência no tratamento dos dados pessoais.
GEN-4	**As fases de implementação da aplicação devem permitir validar progressivamente a sua eficácia do ponto de vista da saúde pública. Para o efeito, deve ser definido um protocolo de avaliação que especifique indicadores que permitam medir a eficácia da aplicação.**

4. Finalidades

FIN-1	A aplicação deve prosseguir a única finalidade de rastreamento de contacto para que as pessoas potencialmente expostas ao vírus SARS-Cov2 possam ser alertadas e cuidadas. Não pode ser utilizado para outro fim.
FIN-2	A aplicação não deve ser desviada da sua utilização primária para efeitos de controlo do cumprimento das medidas de quarentena ou confinamento ou do distanciamento social.
FIN-3	A aplicação não deve ser utilizada para tirar conclusões sobre a localização dos utilizadores com base na sua interação e/ou com base em quaisquer outros meios.

5. Considerações de ordem funcional

FUNC-1	A aplicação deve dispor de uma funcionalidade que permita aos utilizadores saber que foram potencialmente expostos ao vírus, sendo esta informação baseada na proximidade de um portador de vírus, infetado dentro de uma janela de um n.º determinado de dias antes do teste de rastreio positivo (o n.º de dias deve ser definido pelas autoridades de saúde).
FUNC-2	A aplicação deve fornecer recomendações aos utilizadores identificados como tendo estado potencialmente expostos ao vírus. Deve transmitir instruções sobre as medidas que devem seguir, e deve permitir que o utilizador solicite conselhos. Nesses casos, uma intervenção humana será obrigatória.
FUNC-3	O algoritmo que mede o risco de infeção tendo em conta fatores de distância e tempo, e, assim, determinando quando um contacto tem de ser registado na lista de contactos, deve ser sujeito a permanente atualização, de forma segura, tendo em conta os conhecimentos mais recentes sobre a propagação do vírus.
FUNC-4	**Os utilizadores devem ser notificados caso tenham sido expostos ao vírus** ou devem obter regularmente informação sobre se foram ou não expostos ao vírus, durante o período de incubação.
FUNC-5	A aplicação deverá ser interoperável com outras aplicações desenvolvidas em todos os Estados-Membros da UE, de modo a que os utilizadores que viajam por diferentes Estados-Membros possam ser notificados de forma eficiente.

6. Dados

DADOS 1	A aplicação deve ser capaz de transmitir e receber dados através de tecnologias de comunicação de proximidade (como Bluetooth Low Energy), para que o rastreamento de contacto possa ser realizado.
DADOS 2	Os dados de transmissão devem incluir identificadores pseudo-aleatórios criptograficamente fortes, gerados por e específicos da aplicação.
DADOS 3	O risco de colisão entre identificadores pseudo-aleatórios deve ser suficientemente baixo.
DADOS 4	Os identificadores pseudo-aleatórios devem ser renovados regularmente, com uma frequência suficiente para limitar o risco de reidentificação, acompanhamento físico ou ligação de indivíduos, por qualquer pessoa, incluindo quem tenha acesso aos servidores de suporte à aplicação, outros utilizadores de aplicações ou terceiros maliciosos. Esses identificadores devem ser gerados pela aplicação do utilizador, possivelmente com base numa *seed* fornecida pelo servidor central.
DADOS 5	De acordo com o princípio da minimização dos dados, a aplicação não deve recolher dados que não sejam estritamente necessários para efeitos de rastreamento de contacto
DADOS 6	A aplicação não deve recolher dados de localização para fins de rastreamento de contacto. Os dados de localização podem ser processados com o único propósito de permitir que a aplicação interaja com aplicações semelhantes em outros países e a precisão da localização deve ser limitada ao estritamente necessário para esta exclusiva finalidade.
DADOS 7	A aplicação não deve recolher dados de saúde para além dos que são estritamente necessários, exceto numa base facultativa e com o único objetivo de auxiliar no processo de tomada de decisão de informar o utilizador.
DADOS 8	Os utilizadores devem ser informados de todos os dados pessoais que serão recolhidos. Estes dados devem ser recolhidos apenas com a sua autorização.

7. Propriedades técnicas

TECNOLOGIA-1	A aplicação deverá utilizar da tecnologia de comunicação de proximidade (v.g., Bluetooth Low Energy) para detetar os utilizadores nas proximidades do dispositivo que executa a aplicação.
TECNOLOGIA-2	A aplicação deve manter o histórico dos contactos de um utilizador no equipamento do utlizador, por um período de tempo limitado predefinido.
TECNOLOGIA-3	A aplicação pode depender de um servidor central para implementar algumas das suas funcionalidades.
TECNOLOGIA-4	A aplicação deve ser baseada numa arquitetura que confie, na medida do possível, nos dispositivos dos utilizadores.
TECNOLOGIA-5	Por iniciativa dos utilizadores notificados como infetados pelo vírus e após confirmação do seu estado por um profissional de saúde devidamente certificado, o seu histórico de contacto ou seus próprios identificadores devem ser transmitidos ao servidor central.

8. Segurança

SEC-1	A aplicação deve ter um mecanismo de confirmação dos utilizadores que reportam estar positivos ao SARS-CoV2, designadamente fornecendo um código único ligado a um laboratório de teste ou profissional de saúde. Se a confirmação não puder ser obtida de forma segura, os dados não devem ser processados.
SEC-2	Os dados enviados para o servidor central devem ser transmitidos através de um canal seguro.
SEC-3	A utilização dos serviços de notificação prestados pelos fornecedores de plataformas OS deve ser cuidadosamente avaliada e não deve conduzir à divulgação de quaisquer dados a terceiros.
SEC-4	As solicitações não devem ser vulneráveis a adulteração por um utilizador malicioso
SEC-5	Técnicas criptográficas de última geração devem ser implementadas para garantir trocas entre a aplicação e o servidor, entre aplicações e para proteger as informações armazenadas nas aplicações e no servidor. Exemplos de técnicas que podem ser usadas incluem criptografia simétrica e assimétrica, funções de hashing, testes de pertença a uma base de dados sem que o responsável fique a saber qual o indivíduo testado, cálculo privado da interseção de bases de dados, Bloom filters, selecionar um indivíduo de uma base de dados, sem que o responsável fique a saber qual o indivíduo selecionado, criptografia homomórfica.
SEC-6	
SEC-7	O servidor central não deve manter identificadores de conexão de rede (p.ex., endereços IP) de qualquer utilizador, incluindo aqueles que foram diagnosticados positivamente e que transmitiram seu histórico de contactos ou seus próprios identificadores.
SEC-8	A fim de evitar a representação ou a criação de utilizadores falsos, o servidor deve autenticar a aplicação.
SEC-9	A aplicação deve autenticar o servidor central.
SEC-10	As funcionalidades do servidor devem ser protegidas contra ataques de repetição.
SEC-11	As informações transmitidas pelo servidor central devem ser assinadas para autenticar a sua origem e integridade.

9. Proteção dos dados pessoais e privacidade

— Lembrem-se: as seguintes orientações dizem respeito a uma aplicação cuja única finalidade é o rastreamento de contacto.

PRIVI - 1	O intercâmbio de dados deve respeitar a privacidade dos utilizadores , e, especialmente, respeitar o princípio da minimização dos dados.
PRIVI - 2	A aplicação não deve permitir que os utilizadores, ao usá-la, sejam identificados diretamente.
PRIVI - 3	A aplicação não deve permitir que os movimentos dos utilizadores sejam rastreados.
PRIVI - 4	O uso da aplicação não deve permitir que os utilizadores infiram qualquer informação sobre outros utilizadores, especialmente se são portadores de vírus.
PRIVI - 5	A confiança no servidor central deve ser limitada. A gestão do servidor central deve seguir regras de gestão claramente definidas e incluir todas as medidas necessárias para garantir a sua segurança. A localização do servidor central deverá permitir uma supervisão eficaz por parte da autoridade de controlo competente.
PRIVI - 6	Uma Avaliação de Impacto na Proteção de Dados deve ser realizada e deve ser tornada pública.
PRIVI - 7	A aplicação só deve revelar ao utilizador se foi exposto ao vírus e, se possível, o número de horas e datas de exposição, sem revelar informações sobre outros utilizadores.
PRIVI - 8	As informações transmitidas pela aplicação não devem permitir que os utilizadores identifiquem os portadores do vírus, nem os seus movimentos.
PRIVI - 9	As informações veiculadas pela aplicação só devem permitir que as autoridades de saúde identifiquem utilizadores potencialmente expostos com seu consentimento.
PRIVI - 10	Os pedidos feitos pelas aplicações ao servidor central não devem revelar nada sobre o portador do vírus.
PRIVI - 11	Os pedidos das aplicações ao servidor central não devem revelar qualquer informação desnecessária sobre o utilizador, exceto, e somente quando necessário, para os seus identificadores pseudonimizados e a sua lista de contactos.
PRIVI - 12	Os *linkage attacks* não devem ser possíveis.
PRIVI - 13	Os utilizadores devem poder exercer os seus direitos através da aplicação.
PRIVI - 14	A desintalação da aplicação deve resultar na eliminação de todos os dados recolhidos localmente.
PRIVI - 15	A aplicação só deve recolher dados transmitidos por instâncias da aplicação ou aplicações equivalentes interoperáveis. Não devem ser recolhidos dados de outras aplicações ou de dispositivos de comunicação de proximidade.
PRIVI - 16	Para evitar a reidentificação pelo servidor central, devem ser implementados os servidores *proxy*. O objetivo destes *non-colluding servers* é misturar os identificadores de vários utilizadores (sejam identificadores dos portadores de vírus ou de contactos) antes de partilhá-los com o servidor central, de modo a evitar que o servidor central conheça os identificadores (*v.g.,* IP) dos utilizadores.
PRIVI - 17	Quer a aplicação quer o servidor devem ser cuidadosamente desenvolvidos e configurados para só recolher os dados necessários (*v.g.*, nenhum identificador deve ser incluído nos *logs* do servidor) e para impedir que qualquer *SDK* de terceiros recolha dados para outras finalidades.

A maioria das aplicações de rastreamento de contacto que estão em discusão seguem duas abordagens quando um utilizador é declarado infetado: o utilizador envia para um servidor o histórico de contactos de proximidade obtidos por *scanning*, ou pode enviar a lista dos seus próprios identificadores transmitidos. Os princípios em seguida elencados são aplicados de acordo com estas duas abordagens. Embora sejam estas as abordagens aqui discutidas, tal não significa que não existam outras possíveis ou mesmo preferíveis, por exemplo abordagens que implementem alguma forma de criptografia E2E ou que utilizem outras tecnologias de reforço da segurança e da privacidade.

9.1. Princípios aplicáveis quando a aplicação envia para o servidor uma lista de contactos:

COM-1	O servidor central deve recolher o histórico de contacto dos portadores de vírus apenas na sequência de ações voluntárias destes portadores.
COM-2	O servidor central não deve manter nem circular uma lista dos identificadores pseudonimizados dos portadores de vírus .
COM-3	O histórico de contacto armazenado no servidor central deve ser apagado depois de os utilizadores serem notificados da sua proximidade com um portador de vírus.
COM-4	Nenhuma informação deve sair do equipamento do utilizador, salvo quando um portador de vírus partilha com o servidor central o histórico dos seuscontactos ou quando um utilizador pede ao servidor informação sobre sua potencial exposição ao vírus.
COM-5	Qualquer identificador incluído no histórico local deve ser apagado após um n.º determinado de dias contado da data da sua recolha (o n.º de dias deve ser definido pelas autoridades de saúde).
COM-6	Os históricos de contacto enviados por utilizadores diferentes não devem ser tratados, por exemplo, para construir mapas de proximidade globais.
COM-7	Os dados nos registos do servidor devem ser minimizados e devem cumprir os requisitos de proteção de dados.

9.2. Princípios aplicáveis quando a aplicação envia a lista de seus próprios identificadores para o servidor central:

ID-1	O servidor central deve recolher o histórico de contacto dos portadores de vírus apenas na sequência de ações voluntárias destes portadores.
ID-2	O servidor central não deve manter nem circular uma lista dos identificadores pseudonimizados dos portadores de vírus.
ID-3	O histórico de contacto armazenado no servidor central deve ser apagado depois de os utilizadores serem notificados de sua proximidade com um portador de vírus.
ID-4	Nenhuma informação deve sair do equipamento do utilizador, salvo quando um portador de vírus partilha o histórico dos seus contactos com o servidor central ou quando um utilizador pede ao servidor informação sobre sua potencial exposição ao vírus.
ID-5	Os dados nos registos do servidor devem ser minimizados e cumprir os requisitos de proteção de dados.