STAYAWAY COVID: QUE RISCOS PARA A PRIVACIDADE?

Cláudia Fernandes Martins

A aplicação STAYAWAY COVID, desenvolvida pelo Instituto de Engenharia de Sistemas de Computadores, Ciência e Tecnologia (INESC TEC), em parceria com o Instituto de Saúde Pública da Universidade do Porto e as empresas Keyruptive e Ubirider, foi recentemente lançada e já conta com mais de um milhão de "downloads" nos sistemas operativos Android e iOS.

Esta aplicação, que é de instalação e utilização voluntárias, permite alertar os utilizadores para o risco de eventual contágio da doença COVID-19 quando o telemóvel do utilizador tenha estado a uma distância inferior a dois metros durante mais de 15 minutos do telemóvel de outra pessoa (também ela utilizadora da aplicação) a quem tenha sido depois diagnosticada a doença COVID.

A STAYAWAY COVID é uma aplicação de notificação da exposição individual a fatores de risco de contágio que, enquanto instrumento de saúde pública, tem por objetivo interromper a cadeia de propagação da doença COVID-19. Para atingir este objetivo, é, porém, necessário que o maior número possível de pessoas descarregue e utilize a aplicação e que insira a informação necessária no sistema, pois isto aumentará a probabilidade de vir a ser diagnosticado um maior número de pessoas, mesmo que ainda não apresente sintomas.

Antes de uma prévia utilização da aplicação, é, assim, legítimo que os seus potenciais utilizadores se questionem quanto à segurança desta aplicação e de que forma é assegurada a sua privacidade.

Como qualquer aplicação informática não é obviamente possível assegurar que a STAYAWAY COVID constitui uma aplicação 100% segura. Esta garantia ninguém poderá dar. Esta circunstância (que, diga-se, não valerá apenas para a aplicação STAYAWAY, mas para as aplicações em geral) não mitiga, de forma alguma, um potencial utilizador de fazer uma escolha consciente (entre instalar ou não a aplicação) e de tomar uma decisão informada de acordo com os riscos.

Embora a aplicação STAYAWAY COVID não aceda aos dados de identificação do utilizador (por exemplo, nome, morada, números de identificação, aplicações de redes sociais, etc.), nem recolha dados de localização do utilizador ou de terceiros (por exemplo, o local onde ocorreu o risco de contágio), isto não significa que a sua utilização não implique um risco de identificabilidade e de localização do utilizador.

A aplicação só funciona com a interface "Bluetooth Low Energy" (BLE) ativa, o que permite, de forma precisa, saber a localização de telemóveis, que emitem sinais que podem ser lidos por recetores instalados em qualquer local (por exemplo, na via pública). Logo, não é possível afirmar que não existe um risco de rastreamento da localização e das deslocações do utilizador por terceiros.

Esse risco existe, mas pode ser minimizado, uma vez que a aplicação funciona sob o sistema fornecido pela Google e a Apple, designado "Google-Apple Exposure Notification" (Sistema de Notificação de Exposição Google-Apple, "GAEN"), que permite utilizar um endereço aleatório sujeito a alterações periódicas para a comunicação dos chamados códigos "RPI" ("Rolling Proximity Identifiers") e, deste modo, que não se estabeleça uma relação com um determinado telemóvel, impedindo o rastreamento.

Sucede que a Google e a Apple (dependendo do sistema utilizado para descarregar a aplicação, Android ou iOS) ficam com o verdadeiro endereço da interface de "Bluetooth" e não é verdadeiramente possível saber como estes colossos informáticos utilizam ou utilizarão a informação no futuro.

Neste âmbito, não há como negar que impera a opacidade do sistema. O código do sistema GAEN não é um código aberto, pelo que não se encontra sujeito a escrutínio, podendo, inclusive, ser alterado por livre iniciativa da Google ou da Apple. Os próprios criadores da aplicação STAYAWAY e o responsável pelo tratamento dos dados, que, no caso, é a Direção Geral da Saúde, tão-pouco detêm o controlo total dos dados dos utilizadores, uma vez que o tratamento é realizado pelo sistema operativo dos dispositivos móveis do utilizador.

O recurso à interface da Google e da Apple constitui, assim, um dos aspetos mais críticos desta aplicação. Isto não significa, porém, que não se deva instalar e utilizar a aplicação.

Em relação a outras aplicações que têm a informação agregada numa única base de dados, a aplicação STAYAWAY foi concebida para que a informação fique parcialmente descentralizada (o armazenamento das chaves e dos identificadores recebidos de terceiros com quem se teve um contacto de proximidade são remetidos para o telemóvel do utilizador), o que, do ponto de vista da proteção dos dados, permite mitigar o nível de afetação dos direitos dos utilizadores.

Um outro aspeto positivo a ter em conta é que a aplicação oferece garantias de não re-identificação dos dados através da pseudonimização (ou seja, os dados são tratados de forma a que deixem de poder ser atribuídos a um indivíduo específico, salvo através de informações suplementares que são mantidas separadamente e sujeitas a medidas técnicas específicas), o que dificulta a utilização de dados para outras finalidades e a sua interconexão com outros tratamentos de dados.

Além do mais, o apagamento automático dos dados e o seu curto prazo de conservação (14 dias) são também aspetos relevantes a considerar e que permitem mitigar, em caso de ocorrência de incidentes de segurança, o nível de afetação da privacidade dos seus utilizadores.

Dentro do atual contexto, é importante que cada utilizador possa fazer uma escolha informada e consciente antes de decidir instalar e utilizar a aplicação (mas isto não valerá apenas para a aplicação STAYAWAY, mas para as aplicações em geral), que tem, sem dúvida, os seus méritos e poderá vir a ser muito útil no combate à propagação da doença COVID, mas claro em conjunto com o cumprimento das restantes recomendações da Direção Geral da Saúde.

25 de setembro de 2020