COVID-19

PROTEÇÃO DE DADOS PESSOAIS

AS MEDIDAS DE RASTREAMENTO SERÃO DEPOIS REVERSÍVEIS?

Cláudia Fernandes Martins

Não é um exagero dizer que o COVID-19 mudou a perspetiva de ver o Mundo e que esta, provavelmente, não mais será a mesma, tendo em conta os acontecimentos e medidas extraordinárias dos últimos meses.

Quanto aos "dados pessoais e privacidade" poderá não ser diferente. A recolha e utilização de dados pessoais de saúde, dados de geolocalização ou outros meta dados já se revelam e vão, sem dúvida, revelar-se, cada vez mais, essenciais no atual contexto, em particular, para a mitigação da propagação e contenção do COVID-19.

Têm surgido várias iniciativas com vista à implementação de aplicações de rastreio de contactos e de alerta na luta contra o COVID-19, tendo-se falado, inclusivamente, na criação de uma aplicação pan-europeia.

Em alguns países, essas medidas já estão, inclusivamente, a ser aplicadas. Por exemplo, na China, foi implementada uma aplicação para classificação de pessoas consoante o seu risco de contágio, informação, essa, que é partilhada com as autoridades públicas competentes, para além do recurso ao uso de "drones", tecnologia de reconhecimento facial, "scanners" infravermelhos. Na Coreia do Sul, rastreiam-se os telemóveis dos utilizadores, criando-se um mapa que fica disponível publicamente para consulta por todos os cidadãos e que permite saber por onde passaram as pessoas infetadas. Outras medidas também já foram adotadas em alguns países da União Europeia como na Áustria, Polónia, Bélgica, Alemanha e Itália.

Face ao atual contexto, é defensável que tais medidas de rastreamento e alertas se possam justificar, desde que sejam concebidas e implementadas em conformidade com as regras de proteção de dados pessoais em vigor na União Europeia, nomeadamente, o Regulamento Geral de Proteção de Dados (RGPD) e a Diretiva da Privacidade Eletrónica e respetiva legislação nacional.

Encontramo-nos numa situação de exceção, que justifica a adoção de medidas de exceção. Mas, mesmo numa situação excecional, tem de imperar a proporcionalidade, nomeadamente quanto à necessidade das medidas, os seus limites, duração, entre outros aspetos, que não podem ser ignorados agora e, inclusivamente, depois.

E uma das questões que se deve levantar com maior acuidade é precisamente esta: serão depois reversíveis as medidas adotadas e que vierem a ser adotadas no atual contexto?

Os nossos dados pessoais representam um potencial de utilização que, diria, inimaginável e que, quando indevidamente utilizados, constituem um risco para a privacidade e, não querendo ser alarmista, para a própria Humanidade, atendendo ao que com eles se poderá fazer em termos de restrições aos direitos, liberdades e garantias dos indivíduos.

É, por isso, importante que as medidas de rastreamento que venham a ser adotadas dependam de um prévio consentimento do seu titular, que deve ser cabalmente informado da utilização que será feita aos seus dados. Neste âmbito, o dever de informar e o dever de ser informado devem andar lado a lado. Se, por um lado, é necessário informar quanto à utilização dos dados pessoais, por outro lado, cada um de nós não se pode bastar com um simples "aceito os termos de privacidade", muitas vezes, nem sequer lidos.

Mais ainda, os dados pessoais recolhidos devem limitar-se ao estritamente indispensável às finalidades que visam prosseguir, bem como devem ser, na medida do possível, anonimizados (o que pressupõe a

irreversibilidade da identificação dos seus titulares) e deve ser assegurado o exercício cabal dos direitos de acesso, exatidão, oposição e apagamento dos dados pelos seus titulares.

Quando estejam em causa dados de saúde, os quais são considerados dados sensíveis (integrados nas chamadas categorias especiais de dados), é necessário que as autoridades de saúde pública sejam responsáveis pelo respetivo tratamento e que se verifique a necessária interação entre essas autoridades e as autoridades nacionais de proteção de dados pessoais. É fundamental que exista uma cooperação estreita entre essas autoridades e que os cidadãos fiquem cientes que podem confiar que os seus dados apenas serão recolhidos e utilizados para finalidades específicas face ao atual contexto e que, uma vez findo o período de exceção, os dados serão, de imediato, apagados.

Como se consegue isso? Não há uma resposta unívoca. Podem ser várias as soluções, desde que as regras de proteção de dados pessoais sejam respeitadas, nomeadamente, como defendeu recentemente o *European Data Protection Supervisor* (EDPS), através da utilização de identificadores de transmissão e de tecnologia "Bluetooth" para o rastreamento de utilizadores, de modo o menos intrusivo possível.

Por forma a assegurar um maior e mais eficaz controlo no cumprimento das regras de proteção de dados pessoais, parece-nos ser, todavia, preferível uma solução à escala europeia (como é o caso do "Pan-European Privacy Preserving Proximity Tracing – PEPP-PT", que junta mais de um centena de investigadores de oito países e que segue o exemplo da aplicação de rastreio "TraceTogether" de Singapura) do que várias soluções com recurso a diferentes tecnologias pelos Estados-membros, procurando-se, assim, uma resposta também ela mais eficaz no controlo da epidemia.

Um coisa é certa: a solução que vier a ser adotada deverá, sem dúvida, assentar num quadro de proteção de dados sólido e coerente, que tem de ser apoiado por uma aplicação rigorosa das regras de proteção de dados pessoais, pois é importante gerar a confiança necessária à utilização dessas aplicações pelos cidadãos, sendo, por isso, fundamental que cada indivíduo consiga controlar a utilização que é feita dos seus dados pessoais, não só agora, em que se justificam medidas excecionais, mas, sobretudo, depois do COVID-19.

Lisboa, 19 de abril de 2020