STAYAWAY COVID APP: Estaremos realmente (ciber)seguros?

dinheirovivo.pt/opiniao/stayaway-covid-app-estaremos-realmente-ciberseguros-12893065.html

29 de julho de 2020

A STAYAWAY COVID APP é uma aplicação portuguesa que pretende ser uma ferramenta auxiliar de combate à pandemia de COVID-19 e que, para tal, pressupõe a monitorização de cidadãos infetados e o envio de um alerta às autoridades ou outras pessoas em situação de proximidade, no sentido de diminuir o número de contágios. A aplicação está já a ser testada, embora o Centro Nacional de Proteção de Dados tenha levantado questões relacionadas com o tratamento de dados e com a cibersegurança e divulgado que vai, juntamente com o Centro Nacional de Cibersegurança, conduzir avaliações técnicas e procedimentais.

Não me vou debruçar sobre a decisão política de implementar a STAYAWAY COVID APP, contudo há, a meu ver, dois pontos fundamentais que devem ser discutidos pela comunidade onde me insiro e pelos quais me tenho batido nos últimos 15 anos: privacidade e cibersegurança.

No plano da privacidade é essencial, desde logo, que:

- estes dados sejam efetivamente tratados como dados especiais que são, sendo imprescindível que sejam cedidos de forma voluntária e anónima – o que implica, por um lado, recuos, à posteriori, no consentimento e, por outro, que não seja possível identificar, de maneira nenhuma, os utilizadores;

- os princípios de tratamento de dados constantes do RGPD sejam respeitados, com destaque para a transparência, a limitação das finalidades, a minimização e a limitação da conservação, desde o desenvolvimento à implementação da aplicação e sucessivas

atualizações;

- o responsável pelo tratamento de dados, no caso, a DGS, esteja capacitado para o fazer;

- as partes terceiras – no caso, Google e Apple, respeitem estas mesmas exigências de privacidade.

Por outro lado, no plano da cibersegurança é fundamental garantir que:

- no plano do desenvolvimento, o código seja aberto na sua totalidade à comunidade para que esta possa testar a aplicação, na consciência de que essa partilha gerará também riscos;

- no plano das pessoas, as partes envolvidas sejam formadas para a cibersegurança, estando conscientes dos riscos e das boas práticas que os mitigam;

- no plano dos processos, sejam asseguradas as medidas técnico-organizativas capazes de promover a segurança da infraestrutura, nomeadamente dos servidores do Ministério da Saúde e da Casa da Moeda, que são críticos, já que a app também poderá ser usada com más intenções, para furar estas instituições.

A este propósito recordamos o recente incidente de segurança de que foi alvo a aplicação de rastreamento da Coreia do Sul, país pioneiro na chamada Saúde Pública Digital, que expôs dados pessoais e, mais ainda, a urgência de aplicações com este grau de sensibilidade terem de ser devidamente auditadas antes de saírem para o mercado.

Para que se tenha uma ideia, dados pessoais tão sensíveis como os de saúde, caindo nas mãos erradas, podem ser usados indevidamente como critério de exclusão na atribuição de um seguro de saúde ou de vida. Além disso, aplicações como estas, vulneráveis, permitem acesso direto de criminosos ao Ministério da Saúde, interrompendo os seus serviços com consequências devastadoras para a saúde pública, já que a maioria dos processos assentam em base tecnológica (recorde-se, aliás, que, ainda este mês, o Ministério da Saúde foi alvo de ciberataque). Imagine-se agora o que seria uma operação de urgência não poder ser realizada porque o sistema estava bloqueado, impedindo qualquer procedimento? Este é alias um assunto que me preocupa e sobre o qual tive oportunidade de falar no Dinheiro Vivo, no ano passado e do qual apenas recupero dois casos: o do Hospital do Barreiro, multado em 400 mil euros por má política e acesso indevido a dados de pacientes e o dos Hospitais CUF José de Mello Saúde, que sofreram um ataque de ransomware, paralisando o serviço e obrigando ao cancelamento de várias consultas e tratamentos até ao pagamento de 10 milhões de euros.

Há uma certa leviandade perante ciberataques ou violações de dados deste tipo e por isso procuro sempre socorrer-me de exemplos simples, para explicar esta realidade complexa que é a da cibersegurança e da privacidade. Esta realidade virtual, onde se encontram as tecnologias, tem consequências bem reais na vida dos cidadãos e é fundamental que todas as medidas sejam tomadas para garantir a sua segurança. Assim, para darmos o passo tecnológico de implementar uma aplicação como a STAYAWAY COVID é essencial que a mesma seja tão útil ou ética quanto segura.

Bruno Castro, CEO da Visionware