Translations proofread by EDPB Members.
This language version has not yet been proofread.

Olivier Micol

Bruxelas, 14 de abril de 2020

Chefe de Unidade - Comissão Europeia
Direção-Geral da Justiça e dos Consumidores
Unidade C.3 – Proteção dos dados
Bélgica

Referência: OUT2020-0028

Ex.mo Senhor Micol,

Muito agradeço que tenha contactado e solicitado o parecer do Comité Europeu para a Proteção de Dados (CEPD) sobre o projeto de Orientações respeitantes a aplicações móveis de apoio à luta contra a pandemia de COVID-19 na perspetiva da proteção de dados. Com efeito, o CEPD tem-se empenhado em avançar rapidamente nesta matéria, tendo publicado uma declaração em 19 de março, e planeia emitir orientações adicionais sobre rastreio, investigação científica e teletrabalho na próxima semana. Algumas autoridades nacionais de supervisão estão também a desenvolver orientações a nível nacional para aconselhar os respetivos governos e operadores de telecomunicações sobre a melhor forma de cumprir as regras de proteção de dados. O CEPD congratula-se com a iniciativa da Comissão de desenvolver uma abordagem pan-europeia coordenada, no âmbito da qual as aplicações móveis podem tornar-se uma das medidas propostas para capacitar as pessoas na resposta de luta contra a pandemia. O CEPD afirmou repetidamente que a aplicação dos princípios de proteção de dados e o respeito pelos direitos e liberdades fundamentais não são apenas uma obrigação legal, mas também um requisito para reforçar a eficácia de quaisquer iniciativas baseadas em dados para combater a propagação da COVID-19 e para apoiar as estratégias de desconfinamento.

O CEPD está ciente de que não existe uma solução única nesta matéria e que as opções disponíveis exigem que sejam tidos em conta muitos fatores, incluindo o facto de a saúde das pessoas poder ser afetada. É por esta razão que as soluções técnicas previstas devem ser analisadas em pormenor, numa base casuística. Por outro lado, o CEPD considera que é um passo na direção certa com o objetivo de salientar a necessidade essencial de consultar as autoridades de proteção de dados a fim de garantir que os dados pessoais são tratados de forma lícita, respeitando os direitos das pessoas, em conformidade com a legislação em matéria de proteção de dados.

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

O desenvolvimento das aplicações deve ser efetuado de forma responsável, documentando com uma avaliação de impacto sobre a proteção de dados toda a privacidade implementada desde a conceção e a privacidade por meio de mecanismos por defeito, e o código-fonte deve ser disponibilizado publicamente para um controlo tão amplo quanto possível por parte da comunidade científica.

Nesta fase, e com base nas informações fornecidas pela Comissão, o CEPD só se pode concentrar no objetivo global das aplicações previstas, a fim de verificar se estão em conformidade com os princípios da proteção de dados, e nos mecanismos previstos para o exercício dos direitos e liberdades da população. Ao fazê-lo, o CEPD considera que a Comissão irá estabelecer elementos para uma reflexão mais aprofundada, a fim de ajustar, quando necessário, as escolhas indicadas no documento, ou de explorar novas opções técnicas. Em qualquer caso, o CEPD irá investigar mais aprofundadamente esta questão nas suas próximas orientações.

Nesta resposta, o CEPD gostaria de abordar especificamente a utilização de aplicações para a funcionalidade de rastreio de contactos e de alerta, uma vez que este é o aspeto que requer mais atenção a fim de minimizar as interferências com a vida privada, permitindo simultaneamente o tratamento de dados com o objetivo de preservar a saúde pública.

Caso essas aplicações se revelem pertinentes para a aplicação de uma política de saúde pública, só podem atingir a sua eficiência máxima se forem utilizadas pela maior percentagem possível da população, num esforço coletivo de luta contra o vírus. Qualquer heterogeneidade funcional, falta de interoperabilidade ou mesmo diferença individual na utilização da aplicação podem criar externalidades negativas noutras pessoas, resultando num efeito sanitário reduzido. O CEPD apoia firmemente a proposta da Comissão de adoção voluntária deste tipo de aplicações, uma escolha que deve ser feita pelas pessoas como um compromisso de responsabilidade coletiva. Há que salientar que a adoção voluntária está associada à confiança individual, o que ilustra a importância dos princípios da proteção de dados.

O CEPD observa que o simples facto de a utilização do rastreio de contactos ocorrer numa base voluntária não significa que o tratamento de dados pessoais pelas autoridades públicas se baseie necessariamente no consentimento. Quando as autoridades públicas prestam um serviço, com base num mandato atribuído e em conformidade com os requisitos estabelecidos na lei, afigura-se que a base jurídica mais pertinente para o tratamento dos dados é a necessidade de execução de uma tarefa de interesse público. A adoção de leis nacionais que promovam a utilização voluntária da aplicação sem quaisquer consequências negativas para as pessoas que não a utilizam poderia constituir uma base jurídica para a utilização das aplicações. Tais intervenções legislativas não devem, por conseguinte, ser concebidas como um meio de incentivo à adoção obrigatória, devendo as pessoas ser livres de instalar e desinstalar a aplicação. Estas leis podem ser acompanhadas de atividades de comunicação adequadas a nível nacional para promover esses instrumentos, através de campanhas de sensibilização e assistência aos menores, aos deficientes, ou a partes da população menos qualificadas ou com menores níveis de instrução, a fim de evitar a adoção dispersa, ou de conhecimento inexato da evolução das epidemias e eventuais clivagens no domínio da saúde. Com

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

efeito, qualquer falta de dados, devido ao uso indevido da aplicação, ou mesmo à falha da bateria do dispositivo, pode comprometer seriamente a utilidade pública global destes instrumentos.

As aplicações de rastreio de contactos não requerem a localização dos utilizadores individuais. O seu objetivo não é acompanhar os movimentos de pessoas ou fazer cumprir prescrições. A principal função de tais aplicações é a descoberta de eventos (contactos com pessoas portadoras do vírus), que são meramente prováveis e que, no caso da maioria dos utilizadores, podem nem sequer ocorrer, especialmente na fase de desconfinamento. A recolha de dados sobre os movimentos de um indivíduo no contexto de aplicações de rastreio de contactos violaria o princípio da minimização dos dados. Além disso, criaria enormes riscos em matéria de segurança e privacidade.

As autoridades de saúde e os cientistas estão bem colocados para identificar aquilo que constitui um evento a partilhar se, onde e quando ele ocorrer, desde que seja estritamente necessário como exigido na lei, e devem definir alguns dos requisitos funcionais da aplicação. Uma outra questão que deve ser debatida é o armazenamento desses eventos. Estão previstas duas grandes opções: armazenamento local de dados nos dispositivos individuais ou armazenamento centralizado. O CEPD considera que ambas podem ser alternativas válidas, desde que estejam em vigor medidas de segurança adequadas e que as diferentes entidades também possam ser consideradas responsáveis pelo tratamento dos dados em função do objetivo final da aplicação (por exemplo, o responsável pelo tratamento dos dados e os dados tratados podem ser diferentes se o objetivo for fornecer informações numa aplicação ou contactar a pessoa por telefone, por exemplo). Em qualquer caso, o CEPD pretende sublinhar que a solução descentralizada é mais consentânea com o princípio da minimização.

Por último, estas aplicações não são plataformas sociais para divulgar o alarme social ou dar origem a qualquer tipo de estigmatização. Com efeito, devem ser instrumentos que permitam capacitar as pessoas para darem o seu contributo. Citando o projeto de orientações, o seu único objetivo consiste em permitir às «*autoridades de saúde pública identificarem as pessoas que tenham estado em contacto com pessoas infetadas com COVID-19 e convidarem essas pessoas a observarem um período de autoquarentena, realizarem rapidamente testes e apresentarem recomendações sobre as etapas seguintes, se for caso disso, incluindo as medidas a tomar em caso de sintomas*». A qualidade dos dados tratados é extremamente importante neste esforço. As medidas que devem ser tomadas «*para identificarem as pessoas que tenham estado em contacto com pessoas infetadas com COVID-19*» não são fáceis nem simples. Informar uma pessoa, através de uma notificação numa aplicação, pode ser feito de modo a que a aplicação processe apenas pseudónimos aleatórios. Além disso, um mecanismo deve assegurar que, sempre que uma pessoa é declarada como positiva à COVID, as informações introduzidas na aplicação são corretas, uma vez que tal pode desencadear notificações a outras pessoas quanto ao facto de terem estado expostas. Esse mecanismo poderá basear-se, por exemplo, num código de utilização única que possa ser digitalizado pela pessoa quando o resultado de um teste lhe for comunicado. Cada contacto deve ser efetuado apenas pelas autoridades sanitárias, após uma avaliação da prova de dados sólidos, com a menor interferência possível. Além disso, a Comissão deverá clarificar o papel da «*lista de contactos da pessoa que é proprietária do dispositivo*», tal como previsto nas orientações.

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

Os algoritmos utilizados em aplicações de rastreio de contactos devem funcionar sob a supervisão rigorosa de pessoal qualificado, a fim de limitar a ocorrência de falsos positivos e negativos e a tarefa de «*apresentarem recomendações sobre as etapas seguintes*» não deve de modo algum ser totalmente automatizada. É aconselhável instaurar um mecanismo de retorno de chamada (*call-back mechanism*) em que a pessoa recebe um número de telefone ou um canal de contacto para obter mais informações junto de um agente humano. Além disso, a fim de evitar a estigmatização, nenhum elemento de identificação potencial de qualquer outro titular de dados deve fazer parte desta «*recomendação*», e a utilização da aplicação, ou parte dela (como quadros de bordo, parâmetros de configuração, etc.), não deve permitir a reidentificação de quaisquer outras pessoas, infetadas ou não pela COVID-19. O CEPD sugere vivamente que não sejam armazenados quaisquer dados de identificação direta no dispositivo dos utilizadores e que esses dados sejam, em qualquer caso, apagados o mais rapidamente possível.

O CEPD apoia firmemente o conceito indicado nas recomendações de que, uma vez terminada esta crise, esse sistema de emergência não deve continuar em uso e, regra geral, os dados recolhidos devem ser apagados ou anonimizados.

Por último, o CEPD e os seus membros, responsáveis por aconselhar e assegurar a correta aplicação do RGPD e da Diretiva Privacidade Eletrónica, devem ser plenamente associados a todo o processo de elaboração e aplicação dessas medidas. O CEPD recorda que tenciona publicar orientações nos próximos dias sobre a geolocalização e outros instrumentos de rastreio no contexto do surto de COVID-19.

Em todas as circunstâncias, o CEPD continua disponível para fornecer orientações adicionais às instituições da UE e a todas as partes interessadas envolvidas no desenvolvimento e utilização dessas aplicações móveis na luta contra a COVID-19.

Com os meus melhores cumprimentos,

Andrea Jelinek

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels