COMITÊ CIENTÍFICO DE APOIO AO ENFRENTAMENTO À PANDEMIA COVID-19
GOVERNO DO ESTADO DO RIO GRANDE DO SUL

# Nota Técnica Sobre o Rastreamento Digital de Contatos com *Smartphones*
# EM 16 DE MAIO DE 2020

## Sobre o Rastreamento Digital de Contatos com *Smartphones*

O distanciamento social tem sido uma das principais medidas adotadas para reduzir o espalhamento da COVID-19 na população, com variados graus de sucesso pelo mundo. Esta abordagem remove ou reduz o contato de indivíduos potencialmente infectados com outros membros da sociedade, algo particularmente importante quando a transmissão, como é o caso da COVID-19, ocorre com frequência de forma assintomática.

No entanto, o distanciamento apenas pode ser insuficiente quando não adotado de forma expressiva pela sociedade. Assim, uma possibilidade alternativa, ou complementar, é procurar e isolar de forma pró-ativa os indivíduos com alta probabilidade de estarem infectados, permitindo maior mobilidade de indivíduos com menor probabilidade de carregarem o vetor.

Esta abordagem é conhecida como **rastreamento de contatos** e é amplamente utilizada no controle de doenças contagiosas. O rastreamento de contatos tradicional envolve uma equipe que, ao identificar um indivíduo infectado, obtém uma lista de locais e pessoas com as quais este indivíduo teve contato recentemente (o tempo depende da duração do período infeccioso da doença e pode ser de até 14 dias para a COVID-19). Então, estas pessoas são procuradas e testadas, isolando as infectadas e repetindo o processo para cada caso positivo.

Uma limitação desta abordagem é que os indivíduos infectados dificilmente lembrarão da totalidade, ou mesmo da maioria, dos seus contatos recentes. Muitos destes contatos podem ter sido absolutamente passivos -- desconhecidos que compartilharam um espaço com o infectado sem maiores interações (como em um supermercado, por exemplo).

O **rastreamento digital de contatos** é uma variação desta abordagem tradicional. Ela é viabilizada devido a ampla circulação de *smartphones* na população e tem o potencial de tornar o processo mais efetivo ao automatizar o rastreamento. Já existem diversos países utilizando aplicativos com este propósito. A maioria utiliza-se da tecnologia *bluetooth*, uma forma de comunicação de rádio de curto alcance, a mesma utilizada em fones sem fio. Esses aplicativos operam, tipicamente, da seguinte forma: cada celular emite um sinal *bluetooth* que o identifica e, ao mesmo tempo, registra a presença de dispositivos próximos (tipicamente menos de 2 metros), mantendo uma lista de identificadores de aparelhos que estiveram em proximidade ao longo do tempo. Quando o usuário indica que testou positivo (sendo usualmente necessária a confirmação oficial de médico ou laboratório), a lista de identificadores é utilizada para enviar notificações aos aparelhos que estiveram em proximidade do usuário infectado.

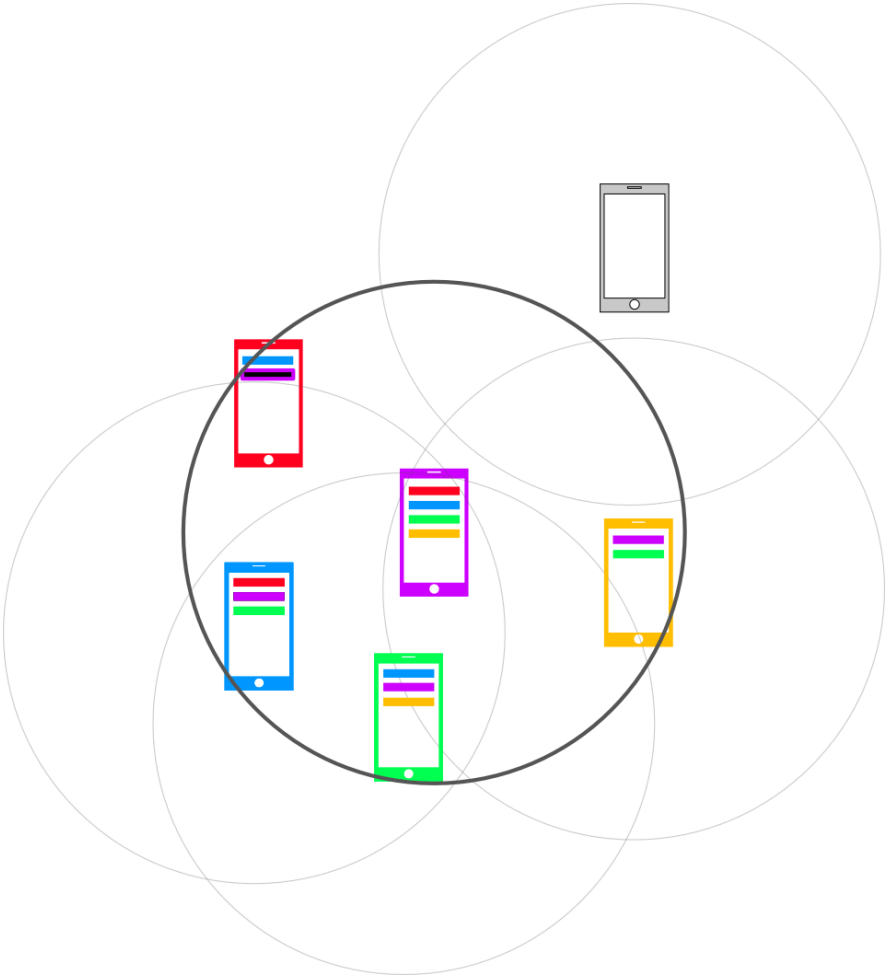

***Figura 1. Cada celular mantém uma lista de identificadores de outros celulares que se encontram em proximidade.***

Os detalhes da implementação deste fluxo variam entre implementações, e em particular com relação ao que é feito após um usuário testar positivo e informar o aplicativo. Essencialmente, há duas variantes: **sistemas centralizados** e **sistemas descentralizados**. Nos centralizados, os aplicativos mantém suas listas de contatos em um servidor central na nuvem, pertencente a uma empresa ou governo; quando o usuário testa positivo, é este servidor que se responsabiliza por decidir quem e como notificar. Nos descentralizados, a lista de contatos permanece apenas no celular de cada usuário e, quando este testa positivo, apenas o seu identificador é informado a um servidor central; neste caso, são os outros celulares que constantemente verificam no servidor se há algum identificador marcado como positivo que esteja em suas listas e alertam apenas seus usuários se necessário.

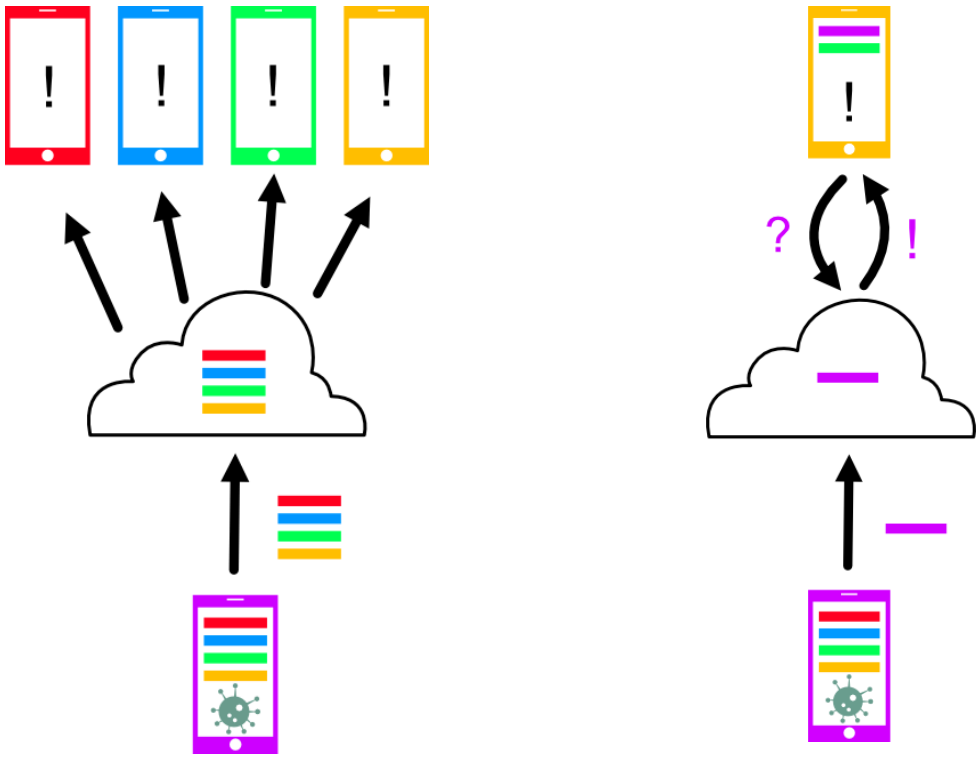


***Figura 2. Usuários que testaram positivo informam o aplicativo que inicia o processo de notificar outros celulares que estiveram próximos. No modo centralizado (esquerda) um servidor na nuvem recebe a lista completa de identificadores de todos celulares usando o aplicativo e dispara as notificações. No descentralizado (direita), o servidor apenas recebe identificadores dos celulares de usuários que testaram positivo; cada celular é responsável por perguntar ao servidor se algum identificador na sua lista testou positivo, para então notificar o usuário.***

Estas duas variantes diferem principalmente no grau de privacidade oferecida aos usuários e funcionalidades oferecidas a gestores. Sistemas centralizados fornecem a terceiros uma grande quantidade de informações, permitindo que estes recuperem

essencialmente toda a rede de contatos da totalidade de usuários do aplicativo. Ainda que os identificadores possam ser anônimos, este método torna mais fácil a aplicação de técnicas de de-anonimização (quando o uso de meta-dados é utilizado para recuperar a identidade) e há o risco de os dados serem utilizados para outros fins, especialmente se o aplicativo coleta também outras informações, como localização geográfica.

Por outro lado, o maior volume também permite que o detentor dos dados faça análises mais ricas que podem beneficiar políticas públicas. Países que adotaram o modelo centralizado incluem França, Noruega, Austrália e Singapura. No entanto, estes países têm observado baixa adoção do aplicativo, tornando sua eficácia limitada, o que pode ser parcialmente atribuído a preocupações com privacidade.

Já o modelo descentralizado reduz a exposição de dados privados a terceiros e pode incluir mecanismos para tornar impraticável tentativas de de-anonimização (como rotação de identificadores). A redução da exposição de dados privados reduz preocupações de violação de privacidade mas, correspondentemente, limita análises aprofundadas uma vez que ninguém possui a totalidade dos dados. É importante observar que estas aplicações, centralizadas ou descentralizadas, não precisam coletar informações de localização ou de identidade do usuário para funcionarem -- são diferentes de aplicações que permitem medir índices de mobilidade, que necessitam da localização exata do aparelho.

A preocupação com privacidade fez com que diversos países passassem a exigir que aplicações de rastreamento garantam a privacidade do usuário. É o caso da União Europeia, que está estabelecendo regras específicas para aplicações deste tipo, além das estipuladas na *General Data Protection Regulation* (GDPR) -- o arcabouço europeu de regulações de proteção de dados pessoais. Da mesma forma, aplicativos em uso no território brasileiro deverão respeitar a Lei Geral de Proteção de Dados Pessoais (LGPD), fortemente baseada na GDPR.

Vários países sinalizaram a adoção do modelo descentralizado, como Alemanha, Itália, Canadá, Finlândia e Estônia. No entanto, nenhum fez ainda implementação de forma massiva, em parte por estarem colaborando e aguardando os dois gigantes da tecnologia, Apple e Google, que recentemente se uniram para oferecer uma base descentralizada em seus sistemas operacionais para celulares (iOS e Android). As empresas fornecerão uma API (interface de acesso) em seus sistemas operacionais que permitirá um uso mais eficaz e seguro dos *smartphones* para este propósito, sobre a qual desenvolvedores construirão suas aplicações.

Com isso, funcionalidades básicas de coleta de dados estarão disponíveis por padrão na maioria dos *smartphones,* sem necessidade de instalar aplicativos específicos. Nesta caso, porém, o usuário terá que optar por ativar estas funcionalidades e instalar algum aplicativo para fazer uso dos dados coletados. Esta é a forma com que a maioria dos aplicativos de *fitness* operam atualmente - o sistema operacional é responsável por contar passos, calorias gastas e outras métricas de atividade do usuário, mantendo estas informações seguras no próprio *smartphone*, e aplicativos apenas solicitam estes dados sob autorização do usuário.

Uma alta adesão, esperada com a adoção de modelos descentralizados pré-instalados na maioria dos *smartphones*, é crucial para a eficácia do rastreamento digital de contatos. Em uma população com adesão de 20%, há apenas 4% de chance de duas pessoas aleatórias que se encontram estarem ambas utilizando a aplicação. Quando há a possibilidade de transmissão do vírus mas não há uma notificação correspondente pelo aplicativo, diz-se que ocorreu um falso negativo. A baixa adesão é a principal causa de falsos negativos.

Por outro lado, uma alta adesão leva ao aumento de falsos positivos. Estes ocorrem quando um usuário é notificado da possibilidade de estar infectado, quando não houve de fato esta possibilidade. Como o sistema opera por ondas de rádio, é possível que os celulares se comuniquem mesmo com barreiras físicas entre as pessoas, como vidros ou paredes. Neste caso, a transmissão do vírus não ocorre mas os usuários serão notificados se um deles testar positivo.

Falsos positivos são particularmente importantes quando se considera as ações a serem tomadas quando se recebe uma notificação do aplicativo, indicando a possibilidade de infecção. Uma possibilidade é a auto-quarentena. Porém, esta é uma solução particularmente custosa quando não há razoável certeza de infecção e grande quantidade de falsos positivos, levando usuários a ignorar notificações ou deixar de utilizar o aplicativo como um todo. Idealmente, o usuário que recebe uma notificação deve ter acesso a testes para verificar se de fato está infectado. Para tanto, é necessário uma infra-estrutura de testagem considerável, amplamente disponível e com baixo (ou nenhum) custo para o usuário. Acredita-se, portanto, que o rastreamento de contatos digital só é de fato viável se acompanhado de testagem massiva.

Com a progressão dramática do COVID-19 no Brasil, aplicativos de rastreamento digital de contatos poderão ser uma realidade no Brasil em breve, seja com soluções locais (por exemplo, o CovidApp da UFSC) ou adoção de aplicativos globais. O Brasil possui alta penetração de *smartphones*, uma das maiores do mundo, o que levaria a uma base expressiva inicial para adoção de uma aplicação deste tipo. É, no entanto,

ainda difícil de quantificar o tamanho do impacto deste método de combate, especialmente com relativa baixa adoção. Como no caso de quarentenas obrigatórias, há um balanço entre liberdade/privacidade e saúde pública. Diferentes países se posicionam em diferentes locais deste espectro e ainda é cedo para dizer onde o Brasil, ou o RS, se posicionará.

De toda forma, deve-se observar os seguintes aspectos de qualquer aplicativo de rastreamento digital de contatos antes de adotá-lo:

1) Os benefícios do uso do aplicativos são claros? Estão bem descritos e eu compreendo os potenciais riscos de falsos positivos e falsos negativos?
2) Qual a política de privacidade do aplicativo? Ela respeita a LGPD? Que dados são coletados e com quem são compartilhados? Quais os riscos para o usuário?
3) Como os casos positivos são informados ao aplicativo? É necessário uma confirmação oficial, ou basta a indicação do usuário? Como é feita essa confirmação?
4) Qual o real significado de uma notificação e quais ações são desencadeadas automaticamente por uma notificação? Quanto controle tenho sobre estas ações?
5) O que devo fazer ao receber uma notificação via aplicativo? Há ações concretas que posso tomar que me beneficiarão ou beneficiarão a saúde pública?

**Referências**


Crocker, A., Opsahl, K. e Cyphers, B. (2020, 10 de Abril). “The Challenge of Proximity Apps For COVID-19 Contact Tracing”. Disponível em: https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing

Romani, B. (2019, 6 de Fevereiro). “Penetração de smartphones no Brasil atinge 60%, mostra pesquisa. O Estado de São Paulo”. Disponível em: https://link.estadao.com.br/noticias/cultura-digital,brasil-lidera-uso-de-smartphones-entre-emergentes-mostra-pesquisa,70002710014

CovidApp. https://covidapp.ufsc.br/

EU General Data Protection Regulation (GDPR). https://gdpr-info.eu/

Lei Geral de Proteção aos Dados (LGPD). http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm